Tatiana-Eleni Synodinou
Philippe Jougleux
Christiana Markou
Thalia Prastitou
Editors

EU Internet Law

Regulation and Enforcement

Springer

EU Internet Law

Tatiana-Eleni Synodinou • Philippe Jougleux •
Christiana Markou • Thalia Prastitou
Editors

EU Internet Law

Regulation and Enforcement

Springer

Editors
Tatiana-Eleni Synodinou
Department of Law
University of Cyprus
Nicosia, Cyprus

Philippe Jougleux
School of Law
European University Campus
Nicosia, Cyprus

Christiana Markou
School of Law
European University Campus
Nicosia, Cyprus

Thalia Prastitou
School of Law
European University Campus
Nicosia, Cyprus

ISBN 978-3-319-64954-2 ISBN 978-3-319-64955-9 (eBook)
DOI 10.1007/978-3-319-64955-9

Library of Congress Control Number: 2017956058

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Introduction

Internet law constitutes a huge challenge for jurists. On the one hand, legal changes and growing case law continuously add new valuable information and clarifications while on the other, technological revolutions and innovative behaviors often introduce legal uncertainty and even confusion. For the technology expert and the jurist interested in information technology law, this creates a constant pressure to keep up to date. In this respect, this collective work is essential, for crystallizing the debate around fundamental issues in areas affecting internet law, namely data protection, cyber-crime, consumer protection, copyright enforcement and freedom of expression. Therefore, it aims at shedding light on current relevant legal debates, conflicts and issues, as well as offering some answers and solutions. The ultimate aim of this collective work is to furnish the reader with the fundamental keys to decrypt the current state of the law of the internet and to be able to foresee its mutations.

More specifically, the first Part of this collective work focuses on the much-discussed new European General Data Protection Regulation 2016/679 (Regulation or GDPR). This important legal instrument has been intended to replace the 95/46/EC Data Protection Directive (DPD) which has been the European Union (EU)'s data protection regime for more than two decades mainly as a response to the emergence, and enormous success, of online social media networks. Therefore, it is only natural to start with the obvious question of whether the said Regulation is adequate. It is also important for the Regulation's main changes, from the pre-existing regime, to be highlighted, as well as for its specific provisions, which have gained particular attention because of either their innovative nature or the sensitivity of their subject matter, to be inquired into. These are the provisions referring to the now infamous right to be forgotten, as well as to the practice of profiling which poses acute risks to personal data and privacy. All of these issues or questions comprise the subject matter of the chapters in the first Part of this book.

In Chap. 1, Irene Loizidou, the Cyprus Commissioner for Personal Data Protection, and Constantinos Georgiades, officer from the Office of the Cyprus Commissioner for Personal Data Protection, aim to assist readers in making sense of the wealth of rules of the GDPR. According to the authors, unlike data protection

experts, the average person is mainly troubled by practical questions pertaining to the GDPR, particularly its impact on the way businesses and professionals qualifying as data controllers should perform tasks. Without attempting a thorough analysis of the GDPR, the chapter aims at giving answers to these practical questions, thereby assisting in the general understanding of the measure and the needs that its implementation gives rise to. It does so by highlighting the differences between the GDPR and the DPD. It lists the principal aims of the GDPR, including the remedying of the problems inherent in the DPD, and proceeds with emphasizing the uniformity of its rules achieved by the very nature of the measure as a Regulation rather than as a Directive. The authors observe that the GDPR builds upon rights and obligations existing in the DPD but takes an important step further introducing news rights and obligations, particularly aiming at responding to the challenges posed by the advent of the Internet including social networks. Additionally, unlike the DPD, the GDPR expressly provides the principles of 'privacy by default' and 'privacy by design' effectively rendering it a legal requirement that data protection is considered from the design stage of data processing systems which must also be privacy-friendly by default. The authors refer to the 'one stop shop' feature of the GDPR, which is capable of reducing red tape and reduce the administrative burden of compliance for data controllers with cross-border operations. Furthermore, they rightly place particular emphasis on the principle of accountability requiring controllers not only to operate in compliance with the GDPR but also to be able to prove such compliance. As they note the GDPR strengthens the role of Data Protection Authorities and additionally regulates transfers of personal data to third countries retaining the basic relevant model of the DPD. They finish their chapter by clarifying that despite its detailed rules, the GDPR does not intend to prevent the flow of data. Instead, it aims at regulating it so that the flow does not infringe upon the human right of privacy and data protection.

In Chap. 2, Lilian Mitrou engages in a more critical analysis of the suitability of the GDPR in the digital era. Specifically, she inquiries into whether the GDPR appears to be the appropriate law for the digital age and aims to shed light on the question of whether this new Regulation constitutes, in practice, a revision of the current framework or a legislative paradigm shift in data protection law, which enhances better protection of informational privacy rights of users. Lilian Mitrou commences her analysis by examining the material and territorial scope of the new EU data protection framework, and the extent to which this appears to be an internet jurisdiction. More specifically, within the first section of her chapter she discusses the narrowing down of the so-called household exception as a significant and controversial issue to the GDPR's material scope, as well as the uncertainties inherent in the "equipment" criterion utilized to define its territorial scope. In the next section, she proceeds with addressing the notion of consent and the way it is regulated as a legal ground of processing in the GDPR. The author moves on, *inter alia,* to an interesting analysis of the new features of valid consent and looks into whether the consent approach is adequate to address the challenges posed in the digital era. Furthermore, she focuses on the new rights that are introduced in the EU data protection framework, these being the right to be forgotten and the right to data

portability, and on the extent to which these appear to respond to new Internet-related challenges. The author concludes her in depth presentation and analysis of the GDPR by attempting to answer the interesting question of whether protecting personal data on the internet appears to be a Herculean or a Sisyphean task.

Chapter 3, by Andres Guadamuz, deals with the so-called right to be forgotten or more simply, the right to data erasure in the GDPR. The chapter explains how the particular right can prove useful to individuals, particularly those facing a situation whereby defamatory information about them exists on the internet and is accessible to the public through search engines. It then searches for the precursors of the right in earlier academic works, legislative instruments and relevant case law, particularly from the United Kingdom (UK). As the author explains, the right is premised on the right to data protection and has to be balanced against other rights and freedoms such as the freedom of expression. European courts strive to achieve a relevant balance according to the author, unlike courts in the United States of America (USA), which have showed a strong preference to the freedom of expression. The chapter proceeds with a thorough description and commentary of the notorious decision of the Court of Justice of the European Union (CJEU) in the *Google Spain* case, where the Court opined that search engines qualify as data controllers and should therefore remove links to data that is, amongst others, irrelevant or excessive from their search results if the data subject has made a relevant request. The author notes the controversy caused by the said CJEU decision and the fears repeatedly expressed that it can result in the relevant right being misused by criminals seeking to hide previous activity. The author refers to post-*Google Spain* national case law disproving these fears, in which the courts have refused to find an obligation to remove links to information. The chapter also looks into the practical implementation of the right by Google and observes that more than 50% of the removal requests submitted to Google have not been satisfied. Noting that Google has come to administer some sort of private justice, the author nevertheless defends the right against its detractors emphasizing that it is limited to cases where there is truly an unnecessary invasion to individual privacy. Article 17 of the GDPR, which contains the relevant right, serves as further proof that the right is not intended to operate as an inappropriate restriction to freedom of expression. The particular provision specifically refers to freedom of expression and contains exceptions capable of shielding the right against much of the criticism against it.

The last chapter of Part I, Chap. 4, is dedicated to Internet profiling. According to the authors, Isak Mendoza and Lee Bygrave, one of the most enigmatic, intriguing and forward-looking rights provided by EU law on the protection of personal data is a qualified right for a person not to be subjected to automated decisions based on profiling. The authors undertake a critical analysis of Article 22 of the GDPR that places limits on the making of fully automated decisions based on profiling when the decisions incur legal effects, or similarly significant consequences for the persons subject to them. More importantly, this analysis is enriched by comparisons with its predecessor, namely Article 15 of the DPD. More specifically, after describing this right as embodied in Article 15 of the DPD, the authors attempt to

answer two important questions regarding this reformulated right as found in the GDPR. At first, the two authors examine the issue of whether Article 22 signals a different set of concerns, or a different set of mechanisms and semantics than those pertaining to Article 15. Secondly, they proceed to an inquiry of whether this reformulated right provides stronger protection of the principle underlying Article 15(1), as well as whether this new right will have a greater impact on automated profiling. In answering these questions, they *inter alia*, engage in an interesting analysis of the Article 22(1) right and its four ingredients, as well as of the relevant derogations, namely contract, authorization by EU or national law and consent, provided in Articles 22(2)(a) and 22(3), Article 22(2)(b) and Articles 22(2)(c) and 22(3), respectively. Lastly, the authors also discuss the qualified prohibition of Article 22 on decisions based on sensitive data. Based on this interesting analysis, the authors draw important conclusions as to whether Article 22 bears a great deal of similarity with its predecessor, Article 15 of the DPD particularly in respect of the right and/or prohibition it provides.

The second Part is dedicated to online consumer protection, which again goes at the heart of Internet law given that the vast majority of online services are addressed to, and often heavily utilized by, consumers. Consumers face new risks on the internet and are in need of legal protection against them. It is for this reason that more recent consumer protection measures have a strong digital flavor. This is particular true regarding the two recently published proposals for Directives concentrating on contract law issues pertaining to online sales and contracts for digital content, presented by the European Commission in December 2015. These legislative proposals need to be critically assessed in an attempt to determine whether they fit for their purpose or whether they should undergo changes before they gain the status of EU law. Additionally their interrelationship with national corresponding legislative measures in this field, if any, is another interesting question that needs to be tackled. At the same time, the rise of the so-called Sharing Economy poses new challenges and calls for new regulations. However, older regulations too, such as the 85/374/EEC Product Liability Directive (PLD) which has been in place for three decades naturally, now, raises various digital related questions, particularly with regard to its applicability to intangible products such as software. Furthermore, it should not be forgotten that consumer protection is achieved also through criminal legislation, which tackles fraud; fraud comprises a major problem online as the Internet has furnished fraudsters with new opportunities and tools. All of these issues are discussed in the chapters of the second Part of this book.

In Chap. 5, Paula Giliker engages in a thorough examination of the main provisions of the 2015 Proposal of the European Commission for a directive on contracts for the supply of digital content. More specifically the author, in the first part of her chapter, evaluates the three main areas of contract law that are covered by the 2015 Proposal, these being rules on the conformity of digital content with the contract, remedies available for lack of conformity and lastly the right to modify and to terminate long term contracts. Based on her in depth analysis, she provides some general observations and conclusions relating to whether the 2015 Proposal is

likely to be successful commenting, *inter alia*, on the decision of the Commission to opt for a Directive rather than a Regulation, to choose maximum over minimum harmonization, as well as to divide the regulation of the sale of tangible goods and that of the supply of digital content between two distinct directives. In the second part of this chapter, the author engages in a very interesting comparison of the proposed European legislative measure with one of the few national corresponding legislative measures in this field, that has been enacted in the UK in Part 1 of the Consumer Rights Act (CRA) 2015. As the author explains, the CRA 2015 represents an ambitious attempt by the UK to consolidate its consumer law, undertaking at the same time the integration of a number of EU consumer directives into its law. Based on this interesting evaluation and comparison the author highlights the confinement of the CRA 2015 to contracts where a "price" is paid and questions whether the UK legislator should continue to ignore the growth of the market for digital contracts. She also inquires into a whether a 6-month presumption of conformity is sufficient. In the last part of her chapter, Paula Giliker evaluates the implications of the UK's decision to leave the EU on this area of law inquiring into whether the 2015 Proposal, if implemented, is likely, nevertheless, to have some influence on UK law and vice versa.

In Chap. 6, Thalia Prastitou Merdi brings forward a comparative analysis of the most important aspects of the two proposed new digital single market contact law Directives, *vis à vis*, their predecessor, the proposal for a Regulation on a Common European Sales Law (pCESL). More specifically, the proposed Directives for the supply of digital content and for the online and other distance sale of goods were presented as a "modified proposal" for the pCESL aiming to fully harmonize, in a targeted way, the key mandatory rights and obligations of the parties to a contract in this area of law. The author attempts to answer the question of whether these proposals as they currently stand form an adequate replacement for the rebirth of a truly digital European Contract Law. She performs this task by using a three perspective comparative analysis specifically examining the legal form of the two proposals, their scope of application, and more importantly, their substantive content. Throughout this process, the author sheds light on important and interesting matters such as the shift of the European Commission's approach from unification to total harmonization, the proposals' extended territorial, yet narrow personal scope of application, as well as their limited and, in places, complex substantive content. In relation to the latter, the author focuses on the conformity criteria and the remedies available to the buyer including the right to claim damages within the two proposals. Based on this thorough analysis, Thalia Prastitou Merdi draws conclusions as to whether substantial differences exist both between corresponding provisions of the two proposals, as well as between the proposals and the pCESL. More importantly, the author comments on whether possible theoretical asymmetries existing between the two proposals can be seen as inevitably leading to practical inconsistencies. In the last part of this chapter, the author puts forward certain conclusions as to whether there is still way to go for a truly digital European contract law.

In Chap. 7, Catherine Easton explores current key issues of EU internet and information technology law in relation to the growth of the so-called Sharing Economy. According to the author, the rise of the Sharing Economy is a global phenomenon and one that the EU, as a global economic entity, has recognized as one meriting attention in the form of strategically implemented law and policy. As the author explains, this was undertaken in September 2015 when the European Commission initiated a consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing, as well as the collaborative economy. The results were drawn upon, in June 2016, to produce the European Commission's Agenda for the Collaborative Economy. After explaining what the online sharing economy actually entails, the author proceeds with a practical analysis of the status of platforms such as AirBnb and Uber, as facilitators rather than as producers, in various legal areas such as data protection, intermediary liability, verification, reputational systems and the use of algorithms. The author interestingly employs this thematic approach in an attempt to evaluate the sharing economy from the perspective of the challenges these new forms of doing business create for EU Internet Law. Throughout her interesting analysis, Catherine Easton brings forward recent EU legislation, important CJEU case law, as well as relevant legal scholarship in a successful attempt to make her arguments clearer. Furthermore, she focuses on the position of the EU as a regulator in this specific online sphere and, in particular, she evaluates its stance as outlined in the European Commission's Agenda for the Collaborative Economy also attempting predictions in relation to future reforms and the evolving nature of this sector.

Chapter 8, by Geraint Howells, Christian Twigg-Flesner and Chris Willet looks into the issue of product liability with regard to intangible goods. These have become mainstream, as consumers now tend to prefer those to their traditional (physical) counterparts. The European Commission has recently announced an evaluation of the PLD posing three questions pertaining to whether intangible goods qualify as 'products' under the said Directive, whether unintended behaviors by robots could be considered as 'defects' and how strict liability can be allocated amongst the participants in the Internet of Things (IoT). The chapter proposes answers to each of these questions putting most of the emphasis on the first one. It starts by explaining the current law on whether intangible goods qualify as 'products' noting that that the answer very much depends on whether the digital content is supplied on a physical medium or not. This is a shaky distinction according to the authors who argue that the status of intangible goods as 'products' should not be affected by the involvement (or non-involvement) of a physical medium. The chapter notes that it is uncontroversial that producers are liable for defects in digital products when these are embedded into physical goods and that therefore the pressing question is whether the same should be true with regard to intangible goods in their own right. The authors draw a distinction between intangible goods that merely provide information and those which perform a task without human intervention arguing that only the latter should be considered as 'products' attracting strict liability within a product liability regime. They then look into the 'product' definition of the PLD, which does not explicitly answer the

question and search for a sound policy base for viewing intangible goods as products. They find it in their distinction between intangible goods of information provision and intangible goods of task performance. The authors also explain that unintended behaviors of robots can, in certain circumstances, comprise 'defects' and that strict liability in the world of the IoT can be developed along the lines of existing case law on product safety which makes specific provision for the requirement of safety when accessories are involved.

Chapter 9, by Rolf Weber and Dominic Staiger, concentrates on what has been a relatively overlooked issue in the EU Digital Single Market Strategy, namely liability in the digital environment. The authors look into new liability patterns by reference to particular new technologies such as the IoT, robotics and drones. IoT devices, which track fitness and movement patterns for example, pose significant challenges to data protection. As the authors note, certain businesses had to change their products to bring them in line with EU data protection laws. Autonomous robots qualify as 'machinery' or 'products', yet some of their provisions are not apt for robots. The question of liability of the producer is therefore difficult to answer particularly because the traditional notion of liability is based on the possibility to exert control whereas robots may act independently. The authors examine a number of possible solutions including the creation of legal personhood for robots noting that a main question pertains to the ability of existing legal frameworks to respond to the complex liability issues relating to robotics. Drones also pose legal challenges in the area of security and privacy, some of which have been responded to by regulatory action limiting their use by the public. The chapter proceeds looking into particular legal frameworks that can address issues raised in or by the digital environment. These are the EU legal framework on online sales, the proposed Directive for contracts for the supply of digital content, tortious liability and child protection laws that in the EU exist, partly, in the GDPR. As for tortious liability, the authors observe the relevance of data protection laws but opine that product liability law will need drastic reform to be able to address the issue of liability in the digital environment. The authors discuss future legal challenges including cross-device tracking and even the difficulty in identifying the regulator, which is responsible for each particular issue. They place particular emphasis on security breaches and explain the challenges for both data controllers and data subjects using the example of litigated US cases. Finally, the chapter lists and discusses possible liability mitigation strategies such as enterprise risk management and privacy impact assessments, the latter enabling the identification of potential privacy risks and thus, the proactive taking of measures to prevent their materialization.

In the third Part of this book, a portrait is drawn of the current developments effectively bringing about an intellectual property crisis in the digital society and of the attempted solutions given at legislative and jurisprudential level. One such solution is the so-called portability right, which is essentially a new right of legitimate use. Given that online violations of intellectual property rights often occur on the systems of some intermediary, the limitations of liability for intermediaries provided in the 2000/31/EC E-Commerce and in the 2004/48/EC Copyright

Enforcement Directives need to be revisited in an attempt to examine whether they shield relevant intermediaries from liability. Intellectual property is also inherent in domain names, something that raises interesting issues in relation to geographical indications that may form part of a domain name. These issues are analyzed in the chapters of the third Part of this book.

More specifically, Tatiana Synodinou in Chap. 10 analyzes the nascent concept of portability in European copyright law. Two facets of EU portability are explored, with the emphasis on their interaction with copyright law: the data portability right in the GDPR, and the proposal for a regulation on ensuring the cross-border portability of online content services in the internal market. As the author notes, the data portability right appears *prima facie* as a mechanism linked purely to personal data protection and with no relation with copyright law. Nonetheless, the new right slightly interferes with established copyright principles, and mainly with rules governing the control of use of copyright-protected works in social media. Overlaps arise, mainly in cases where copyright protection and the protection of a data subject's image as personal data concur. The controller's obligation to provide the data in a structured, commonly used and machine-readable format might be interpreted as an obligation to provide the data in interoperable open-standard formats. Nonetheless, as the author observes, a systematic interpretation of the relevant provisions of the Regulation does not support such a meaning of the technical standard of the data portability right. In this context, the author poses the question whether the data portability right is just an empty shell, whose application and enforcement is dependent on the goodwill of the copyright holders of online platforms. In the opinion of the author, this could be remedied by the introduction of a specific data portability exception in the 96/9/EC Database Directive. In the second part of the chapter, the analysis focuses on the emergence of portability in European copyright law. In the view of the author, the key issue is that of how the emerging portability privilege is challenging the principle of copyright territoriality. The author examines the legal nature of the proposed Regulation's portability formula, which appears to be an intriguing amalgam, inspired both by mainstream copyright law logic and by consumer law interests. As the author pinpoints, although not expressly qualified as a "lawful user's right" or a "consumer's or subscriber's right", the obligation of portability takes the form of a personal right in favor of a consumer.

Philippe Jougleux in Chap. 11, which is entitled "The role of Internet intermediaries in copyright law online enforcement", discusses the importance of copyright law enforcement as a prerequisite for the emergence of a digital single market. The author firstly analyzes the reasons behind the current crisis in copyright law enforcement and highlights the fact that online copyright law enforcement against the end user or against the first uploader agent is impractical and complicated, as it opposes to data protection principles. However, the CJEU jurisprudence has clearly stated that a fair balance has to be found protecting the rightholders' interests too. In this perspective, Internet intermediary's involvement is unavoidable. The question is examined of whether the Internet intermediary's liability should have been abandoned 15 years ago with the enactment of the E-commerce Directive, whereby

the intermediaries' safe harbor was established. However, the author shows that the law itself, together with an audacious jurisprudential interpretation, leads in practice to the application of a fault-based approach to Internet intermediaries' liability. Indeed, the safe harbor is linked to the application of some strict conditions, specifically in the case of hosting services. The intermediary needs to be in position to ignore the illegal character of the content and to offer a notice and take down system. This is well resumed in the "passive role" doctrine adopted by CJEU. However, the author presents a contemporary shift from the "passive role" doctrine towards an "active-preventative" approach, which is even stricter for the intermediaries. As this evolution is obviously not sufficient to resolve the issue of online enforcement of copyright law, this analysis is supplemented by the emerging topic of gag orders. The author presents the dynamic combination of safe harbor and injunctions. In the light of the principles provided by the CJEU in the *Telekabel* case, injunctions against intermediaries have to be seen as the last and most efficient tool towards copyright law enforcement in the online environment. The author concludes that this method, combined with the trends in case law related to pan-European judicial orders, despite being incomplete with some questions regarding its practical application persisting, nowadays offers the most promising solution.

The heated question of intermediaries' liability is also explored in Chap. 12. Gerald Spindler focuses on the contemporaries' evolutions of the Internet Service Providers (ISPs) safe harbor. The author first presents the safe harbor mechanism and then explains that the use of injunctions severely limits the scope of the system. Indeed, right holders have asked blocking injunctions against access providers for a long time, with, at first, mixed results. However, the *Telekabel* CJEU's decision opened the door to a wild practice of blocking injunction, while at the same time, protecting and safeguarding the balance of interests. The author then refers to the *McFadden* case about WiFi hotspots and provides an in depth analysis of the CJEU's reasoning. Furthermore, the impact of this evolution on national court decisions is evoked. The issue of injunction against host providers is also examined with reference to the *Loreal vs Ebay* and *Google adwords* CJEU's cases. The chapter also adopts a *de legeferenda* approach and the author discusses the potential reforms of the system. One central element of the safe harbor legal framework resides in the practical operation of the notice-and-take-down procedure. However, the notice-and-take-down procedure has many flaws including the uncertainty with regard to the procedural part and the time reaction and a burden on the intermediary. The author states that two extremes should be excluded, namely the mere reliance upon official notifications by authorities and assuming actual knowledge following simple notification on the other. Instead, he proposes a modified notice procedure combined with a counter-notice and put back option inspired by the model of Finnish legal system. This system should be accompanied by rapid preliminary review proceedings. Furthermore, the safe harbor's system should be complemented by a clearer definition of the intermediary's duty of care when the provider is voluntarily monitoring content. In addition, a 'follow the money' approach that would focus on advertising placement on illegal websites would

clearly help intellectual property enforcement. Finally, the author considers that one-size-fits-all criteria for the qualification of an active role of a provider may not be the best solution and that for example, a legal framework tailored to search engines may have to be provided.

The last chapter of Part III is dedicated to the question of the protection of geographical indications (and designations of origin) against cybersquatting and other misuses and forms of exploitation of their reputation. In Chap. 13, Theodore Georgopoulos examines the issues inherent in domain names referring to geographical indications and discusses the new legal challenges posed by the program for generic top-level domains (gTLD). EU law seems to offer enhanced protection for protected geographical terms both against "commercial use" by domain names and against misuse of geographical indications in the frame of comparative and misleading advertising. However, as the author emphasizes, it appears that the challenges posed by cyberspace to the legal principle of territoriality call for the regulation of the question at international level. The author undertakes a detailed analysis of relevant jurisprudence (with emphasis on the World Intellectual Property Organization system) and concludes that ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) is inadequate to sufficiently protect geographical indications. As trademark law, both at international and national level, is not well-equipped to regulate the question of geographical indications with regard to domain name registration and use, the author argues that adequate protection of geographical indications can be based on the principle of distributive justice, as well as on the acknowledgement of an (international) right to local identity. Indeed, specific legal protection is justified on the frame of the particularities of geographical indications. This specific legal framework would not exclude trademark protection but add a new layer of protection, which, according to the author, can be governed by the principles of distributive justice and human rights. This legal framework would be characterized by the involvement of the groups of producers. Even if the author recognizes the difficulty inherent in such an evolution, the affirmation of a right to local identity in the field of cyberspace, with regard to the registration and use of domain names would nonetheless facilitate the revision of the existing mechanisms for dispute settlement of conflicts between protected geographical indications and domain names.

The final Part of the book focuses on the freedom of speech, the limits of which are tested in the digital environment. The issue is multi-facet and has various different aspects. The internet, and the so-called new media it enables, challenges the concept of journalism and thus, requires a re-examination of the journalist's privilege. A different aspect relates to hate speech and terrorist content. On the internet, such harmful content, which nevertheless constitute 'speech' can easily be communicated and reach millions without any effort or cost, something that exasperates the problem and forces a careful look into whether criminal law is well-equipped to respond to these new challenges. Online fraud is also conducted through speech, yet it jeopardizes the rights and interests of the internet users and it is thus clear that such speech should not be protected under the veil of the protection

of freedom of speech. The chapters of the final Part of this book look into these delicate issues.

In Chap. 14, Costas Stratilatis explores the issue of whether the right of journalists not to disclose their sources should be extended to cover various 'citizen journalists' of the New Media. The author starts with a review of some jurisprudential attempts to deal with this problem in the USA. Apart from referring to important legal scholarship on this matter in general, special attention is particularly given to Wikileaks, the well-known website which has been publishing classified government documents and whose inclusion or exclusion from the protection afforded by the privilege has occupied a significant space in legal scholarship in the USA in recent years. In the next section, the same issue is explored in the context of various Council of Europe's Recommendations. Although, as the author exemplifies, this problem has not arisen in the jurisprudence of the European Court of Human Rights (ECtHR), these instruments still indicate a restrictive approach regarding a possible extension of the right of journalists not to disclose their sources in the field of New Media 'citizen journalism'. Interestingly, Costas Stratilatis explains how these restrictive tendencies can be connected with the famous 'chilling effect' doctrine, which underpins the traditional, functional-utilitarian and institutional justification of the right of journalists not to disclose their sources under the fundamental right of freedom of speech and of the press. Furthermore, in the next section of this chapter, a recent attempt to escape the traditional approach by focusing on the 'source' rather than on the 'journalist' is brought forward. At this stage, the author undertakes interesting discussion on the main advantages of the source-oriented approach, as well as on the difficulties and problems currently existing regarding this alternative approach. Finally, in the last section of his chapter the author, returning to the traditional context of the debate, proposes an enlargement of the traditional concept of 'journalist', subject to certain conditions, so that the relevant privilege can provide protection to all persons who disseminate information to the public using the New Media.

In Chap. 15, Ioannis Iglezakis deals with another complex issue, namely that of the regulation of online hate speech. As the author notes, the Internet with its unique ability of communication of one-to-many and many-to-many and its potential for anonymous and mobile interaction has become the new frontier for the dissemination of hate speech. To deal with this issue, many countries have enacted legislation criminalizing hate speech and additionally, international legal acts have been introduced for the harmonization of national legislations. In this chapter, the regulatory instruments with regard to hate speech on the Internet at an international level are presented and its conflict with the right to freedom of expression is explored. The chapter first explores the characteristics and the definition of online speech, thereby highlighting the fact that hate speech presents some distinguishing features in the online environment, specifically anonymity. To define hate speech, Ioannis Iglezakis uses a comparative and an international approach with a focus on the Council of Europe's definition. Then, he analyzes the international and EU legal framework against hate speech on the Internet to focus again on the Additional Protocol to the Convention of Cybercrime whose main principles are discussed.

Furthermore, the chapter comments upon the relevant EU legislation and offers a discussion about the enforcement of the Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law. Following this presentation of the relevant frameworks, the author judiciously adds an analysis of the potential conflict with the right to freedom of expression. A rich jurisprudence from the ECtHR is cited about the limits of the freedom of expression on the internet, with additional references to the intermediary's liability (the "*Delfi's* case"). The author concludes that legal measures against hate speech may not prove sufficient to restrain the flood of hate speech online publications and proposes better cooperation with the private sector for a more efficient approach.

In Chap. 16, Céline Castet-Renard discusses the issue of online surveillance in the fight against terrorism in France. The chapter provides a critical analysis of recent French legislative measures aiming at strengthening online surveillance as part of the fight against terrorism. The author presents in detail the complex French legislative arsenal and questions seriously its efficacy from the point of view of state security, while she also points to the possible dangers emerging for the protection of the fundamental rights of individuals. As the author emphasizes the balance of interests most probably tilts in favor of protecting state security and safeguarding citizens' fundamental rights is put at risk. First, Céline Castet-Renard notes that the targeted surveillance measures may endanger human rights (in particular, the right to respect for private and family life, and personal data protection) because it is indeed a question of watching one or several individuals in real time; not only the suspected person or people themselves are watched but also his or their circle of acquaintances and this simply based on "serious reasons". Furthermore, in the context of the "state of emergency", the substitution of the judicial judge, who is the natural guardian of the public liberties, by the administrative judge, who is solely in control of the administrative searches and seizures, is also questionable. The shift from targeted surveillance to massive blind surveillance is a source of additional problems. The author presents the regimes covering the massive collection of Passenger Name Record (PNR) data and of other data ("black box", IMSI-Catchers). As she argues, it is not enough to be able to collect and store a great wealth of information. It is also necessary to have the ability to process it and to make connections to recognize the real threat, even when faced with increasingly unpredictable individual profiles. In this context, the legislator has to establish a relevant balance of interest. As the author concludes, even if the threat of terrorism is real and strong, respect for important values should prevail.

The last chapter of the book, Chap. 17, is dedicated to the regulation of economic fraud crimes in the Internet. Specifically, it focuses on certain important economic fraud crimes, such as identity-related crimes, phishing and pharming and hacking, under the presupposition that they are perpetrated for financial gain. Thereafter, a section is devoted to international legislative instruments by the Council of Europe, with an emphasis on the Convention on cybercrime, which is considered one of the most important initiatives to date, has been embraced by so many Member States. However, as Margarita Papantoniou observes, the Convention has undergone no

amendments so far and no decisive steps have been taken by Member States to harmonize and modernize their laws to better respond to this phenomenon of increasing incidents of cyber fraud crimes. The EU, on the other hand, has taken up a number of initiatives, such as the enactment of policies, strategies, communications and decisions, all not directly enforceable, something that highlights the fact that it is for the Member States to deal with challenges in cyberspace. The recent Directives 2013/40 and 2016/1148, concentrate on the matter of security of information systems and networks and only tackle one specific area of fraud, namely hacking by fraudsters to obtain or gain money. The challenges identified in this area of law are numerous. Most of them revolve around the debate regarding whether existing laws should be re-drafted or new specific legislation should be enacted instead, the non-reporting of such crimes and the consequent lack of cooperation between the private and public sector, and prosecutorial and evidential issues that appear during criminal procedures. The author concludes that it is clear and widely acknowledged that all measures taken up to now represent piecemeal regulatory attempts and by no means form a coherent plan to 'annihilate the danger'.

Contents

Part I
Personal Data Protection: What Perspectives?

Chapter 1
The GDPR: New Horizons

Irene Loizidou Nicolaidou and Constantinos Georgiades

Abstract This article purports to be an introductory "easy reading" tool assisting non-experts in the field of data protection to comprehend the complex legalities of the General Data Protection Regulation (GDPR), which replaces Directive 95/46/EC (the Directive). The article explores what the GDPR is expected to deliver and how it is envisaged to remedy some of the shortcomings of the Directive. The article does not go into an in-depth legal analysis of the GDPR. Instead, it attempts to explain how the expectations relating to the GDPR are reflected in some of its core provisions. Understanding the "spirit of the law" may assist the reader to comprehend its letter.

1 Introduction

In the Greek language, and this may be true for other languages too, the word "horizon" is often used metaphorically to describe an expectation or a set expectations stemming from an event that lays ahead in the nearby or distant future. On 24 May 2016, the long debated Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereafter "the GDPR", came into force and shall apply as of 25 May 2018. The GDPR replaces Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereafter "the Directive", which served as the EU's main data protection legal instrument for 21 years.

The GDPR provides the rules for the processing of personal data of natural persons, stipulates that some of these data should be treated as sensitive and sets out the rights of citizens and the obligations of organizations that process their personal

I.L. Nicolaidou (✉) • C. Georgiades
Office of the Commissioner for Personal Data Protection, 1082 Nicosia, Cyprus
e-mail: commissioner@dataprotection.gov.cy; cgeorgiades@dataprotection.gov.cy

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_1

data. Furthermore, it assigns the monitoring of its application by entities in the public and the private sector to national independent supervisory authorities, the Data Protection Authorities (DPAs) and sets out the rules for these authorities' cooperation, particularly where enforcement is required. While the Directive served its purposes well for more than 21 years, it had some shortcomings that needed to be remedied. The Lisbon Treaty, globalization and emerging technological developments also called for the need to review the Directive. To understand the GDPR, one has to have a basic insight to what this legislation aims to achieve and how it attempts to remedy the shortcomings of the Directive.

Introducing the GDPR to persons with limited or no experience in the field of data protection is not an easy task. DPAs that are entrusted with this task are often faced with the following questions: Why was it deemed necessary to replace the Directive? What does the GDPR aim to achieve? How is the GDPR expected to fulfill these aspirations? An experienced reader may seek the answers to these questions, with ease, in the Commissions' Communication or the Impact Assessment accompanying the Proposal for the GDPR or in GDPR's own Preamble. It is reasonable to assume that an experienced reader may need to understand, for example, that the basis for the GDPR's Proposal was Article 16 of the Treaty for the Functioning of the European Union (TFEU), the new legal basis for data protection measures introduced by the Lisbon Treaty, whereas the Directive was based on the 'internal market' legal basis, specifically on Article 114 (as it is now) of the TFEU.

The average person however, who is called upon to implement the GDPR, is concerned with questions that are more practical such as "what has changed?" "How do these changes affect my day to day work?" and "what should I look for?" Therefore, this article will attempt to answer this type of questions by focusing on the differences between the GDPR and the Directive and leaving aside their similarities. To this end, core provisions of the Directive that roughly remain unaffected in the GDPR, such as the basic data protection principles set out in GDPR Article 5 and the conditions for the lawful processing of personal data set out in Articles 6 and 9, shall be overlooked in this article, without devaluating their importance. After all, these Articles deserve a thorough legal analysis, but this is neither the subject nor the purpose of this article.

This article aims to be an introductory "easy reading" tool for assisting newcomers in the field of data protection to understand the complex legalities of the GDPR. It explores what the GDPR is expected to deliver and how it is envisaged to remedy some of the shortcomings of the Directive. The article does not go into an in-depth legal analysis of the GDPR. In lieu, it attempts to explain how the expectations relating to the GDPR are reflected in some of its core provisions. Understanding the "spirit of the law" can assist readers with limited or no legal expert knowledge in better comprehending the "letter of the law". The article hopes to familiarize readers with some or little experience in national data protection legislation, with some of the core provisions they will come across in the GDPR.

2 Principal Aims of the GDPR

The GDPR aims at improving the existing legislation and in particular at achieving the following:

(a) To remedy some of the problems that occurred because of the defragmented transposition and implementation of the Directive by introducing uniform relevant rules,
(b) To strengthen the existing rights of the citizens,
(c) To introduce new rights and obligations, particularly with regard to citizens' activities in the digital environment,
(d) To reduce administrative burdens and to cut red-tape procedures, both for DPAs and for enterprises that operate in more than one Member States,
(e) To consider the impact of the costs inherent in compliance with data protection rules on micro, small and medium size enterprises (SMEs),
(f) To enhance the principles of transparency, accountability and self-regulation,
(g) To enhance the supervisory role of the DPAs and to strengthen their cooperation, particularly, in cross-border cases where persons are affected in more than one Member States,
(h) To better regulate the responsibilities of controllers and processors and their liability and to introduce more stringent sanctions and penalties,
(i) To better regulate transfers of personal data to (third) countries outside the EU and,
(j) To promote research, innovation and technology and to contribute to EU's social integration and economic development, particularly in the field of e-commerce while, at the same time, ensuring sufficient respect to the rights to privacy and personal data protection.

3 Understanding the GDPR

3.1 Uniform Rules

A Directive is a legal instrument that allows Member States (MS) a degree of flexibility, as to how to transpose it into their national legal order. A Regulation on the other hand, is a more rigid legal instrument that allows no or little flexibility in its transposition. The non-uniform implementation of the 1995 Directive had resulted to the fragmentation of the data protection rules, to legal uncertainty and to the perception that the legislation does not offer substantial protection, in particular with regard to online activities. By replacing the Directive with a

Regulation, the legislator clearly wishes to ensure a more uniform[1] application of the enshrined data protection rules.

When the Directive was adopted in 1995, the internet, particularly the WWW, was still at its earliest stages. Today, DPAs are called to deal with complaints against enterprises, which operate online in more than one MSs, and it is not always easy to determine which DPA has competency to examine them, according to the applicable law of the Directive. The *territorial scope*[2]of the GDPR is enshrined to resolve some of the shortcomings of the Directive pertaining to the applicable law. For example, the Directive applies where the processing is carried out in the context of activities of an establishment of the controller on the territory of a Member State, but it does not define these activities nor it explains adequately what can be considered as an "establishment". The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not and it provides definitions for the establishment the main establishment of the controller, for undertakings and for cross-border activities.

For the better handling of cross-border cases, the GDPR provides separate definitions[3] for the *establishment* and the *main establishment* of an enterprise (the controller) and for a *group of undertakings*. In addition, it defines the role of each DPA in such cases, distinguishing them into *lead*, *competent* and *concerned* authority.

3.2 Existing Rights and Obligations

The Directive also provided for several of the rights foreseen by the GDPR. The GDPR however elaborates on these rights and stipulates how these can be applied in practice. For example, in practice, only few people read or understand the lengthy, complex privacy policies posted on various websites they visit. The right to be *informed* obliges enterprises to use clear and plain language, in particular when addressing children.[4] The right of *access* to personal data stipulates that a person can request and receive from a controller, information relating to the processing of his own data. This means that the controller cannot disclose to this person information relating to other persons. In many cases, requests of access submitted by email were declined because the controller did not bother to verify the identity of

[1]Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135/53 (GDPR) Preamble par. 9.

[2]GDPR Article 3.

[3]GDPR Article 4.

[4]GDPR Article 12.

the data subject. The GDPR makes it clear that the controller can provide to the right person the requested information in a commonly used electronic form when the request is made by electronic means.[5] It also provides rules for the processing of data that does not require the *identification*[6] of the data subject.

One of the core elements of the Directive was the processing of personal data based on *consent*. However, it was not always clear how the person gives his consent in the digital environment. The GDPR sets out certain *conditions*[7] obliging the controller to demonstrate that the data subject has given his consent. It also provides special rules for consent when information society services are offered directly to *children*.[8] However, while it stipulates that persons have the right not to be subject to a decision based solely on automated processing, including *profiling*, which produces legal effects concerning them,[9] it does not clearly prohibit the profiling of children. Yet, in the GDPR's Preamble, it is explained that such measures should not concern children.[10]

The development of internet and social networks resulted to an unprecedented posting and publication of personal data. Regrettably, because of the structural design and operation of the internet, currently, as a rule, what is uploaded on the web stays in the web. Both the Directive and the GDPR provide for the right to *erasure*, i.e. the right to ask for and obtain the erasure of personal data, under certain justified conditions. However, the GDPR has elevated this right to the *right to be forgotten*.[11] According to this right, users, for lawful reasons defined in the GDPR, can ask and obtain from search engines the removal from the list of search results, of links to posts that infringe their right to privacy and the protection of their personal data. The establishment of the right to be forgotten became imperative after the milestone ruling of the Court of Justice of the European Union (CJEU) in the case of Google Spain of 13 May 2014,[12] though it should be noted that the relevant ruling concerned the relevant provisions of the Directive and not that of the GDPR. Paragraph 84 of the CJEU's ruling reads:

> Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.[13]

[5] GDPR Article 15(3).

[6] GDPR Article 11.

[7] GDPR Article 7.

[8] GDPR Article 8.

[9] GDPR Article 22.

[10] GDPR Preamble par. 71.

[11] GDPR Article 17.

[12] CJEU, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, Judgement of 13 May 2014.

[13] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, par. 84.

3.3 Introducing New Rights and Obligations

What happens if a person no longer wishes to be user of a social network? What if he decides to switch to another one? Can he move all the data he has posted so far to the second network? Can he also move the LIKES he had made on other users' posts? The GDPR has introduced the right to *data portability*[14] to tackle questions like these. This right obliges enterprises and organizations to transmit a person's own data from one system to another, in a machine-readable format, upon his request, if the conditions provided by the GDPR are met, that this is technically feasible and that this does not affect the rights of other persons.

The GDPR acknowledges that the development of new technologies may entail certain privacy risks. Persons downloading applications on their smart devices often have no choice but to permit access to their personal data by the applications' designers or by third parties. The GDPR obliges manufactures to embed data protection and privacy friendly safeguards into new technologies *by design and by default*.[15] For example, when registering in a social network for the first time, the default settings should be such to prevent other users from accessing the new comer's account. The new user should have the right to choose who to add on his/her list of "friends". While there are many benefits from the introduction of new technologies, such as big data operations, the Article 29 Working Party[16] acknowledges that:

> As an important part of big data operations relies on the extensive processing of the personal data of individuals in the EU, it also raises important social, legal and ethical questions, among which concerns with regard to the privacy and data protection rights of these individuals. The benefits to be derived from big data analysis can therefore be reached only under the condition that the corresponding privacy expectations of users are appropriately met and their data protection rights are respected.[17]

Directive 95/45/EC did not oblige controllers to notify their customers, for *data breaches* that may adversely affect their privacy. Such obligation is foreseen in the e-Privacy Directive,[18] as amended, but it only applies *to the provision of a publicly*

[14]GDPR Article 20.

[15]GDPR Article 25.

[16]This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[17]Article 29 Data Protection Working Party, Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, Adopted on 16 September 2016, Document ref. no. WP221, p 2.

[18]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC and by Regulation (EU) No 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC.

available electronic communication service[19] and it does not cover all data controllers. Yet, it is not uncommon for enterprises to publically inform their clients about data breaches that possibly affect their privacy. This practice however, is not based on a legal obligation, but it is rather based on each enterprise's good will or on its corporal social responsibility policy. The GDPR introduces detailed *rules*[20] for the notification of data breaches to DPAs and/or to persons affected, that cover all areas of processing, not just the communications sector.

3.4 Reducing Burdens and Red Tape

Under the Directive, enterprises operating in many MSs had to comply with non-uniform data protection rules and to deal with 28 different DPAs. DPAs did not always face cross -border cases in the same way, mainly because of the differences in their culture, administrative and judicial systems and enforcement capabilities. The GDPR introduces the concept of *one- stop- shop*[21] to tackle these problems. Put simply, the one—stop—shop will enable enterprises and citizens to bring their cases before one DPA. If a case has a cross—border nature, affecting citizens in different Member States, a single DPA shall act as lead authority and shall cooperate with other concerned and competent authorities.

The Directive provided that, under certain conditions, organizations in the private and the public sector had to notify DPAs for the processing of personal data they carried out. The GDPR abolishes the *notification* system that imposed a significant administrative cost, both to organizations and DPAs. Instead, the GDPR obliges organizations to keep *records of processing activities*[22] and to present them to DPAs, when asked to. In addition, the GDPR abolishes the Directive's prior *authorization system*, which was used, for example, for allowing transfers of personal data to third countries (countries outside the EU or the European Economic Area- EEA).

The concept of a *Data Protection Officer (DPO)* was initially introduced by the Directive as an optional tool for appointing "compliance" officers who would assist organizations in data protection issues and who would act as liaisons with DPAs and or citizens. While this concept saw its way into some national legislations, some Member States deemed it as an *unn*ecessary burden and simply ignored it. Gradually, it gained ground. EUROPOL and EUROJUST had to appoint DPOs

[19]Article 2(h) of Directive 2002/58/EC provides that "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

[20]GDPR Articles 33 and 34.

[21]GDPR Preamble par. 127 and 128.

[22]GDPR Article 30.

in line with the EU legislative Acts governing them.[23] The GDPR reintroduces the institution of DPO[24] as an obligation for all public services and, under certain conditions, for organizations in the private sector such as groups of undertakings or professional associations. It also provides detailed rules for the DPO's *position* and *tasks*.[25]

3.5 Micro, Small and Medium Size Enterprises (SMEs)

Where the legislator considers that certain aspects of the GDPR are not exhaustively regulated or may require more uniform implementation, the Commission is empowered to further regulate them with delegated or implementing acts. In the Preamble,[26] it is explained that, when exercising these *implementing powers*, the Commission should consider the specific needs of SMEs.

The needs of SMES should also be considered when drawing up *codes of contact*[27] intended to contribute to the proper application of the GDPR and when establishing *certification mechanisms or data protection seals*[28] for demonstrating compliance with the GDPR.

In addition, the GDPR exempts enterprises with fewer than 250 employees, which is the threshold for SMES, from the obligation to keep *records of processing activities*,[29] under certain conditions and it stipulates that when DPAs engage in promoting activities for raising *public awareness*,[30] specific measures should be directed to SMEs.[31]

[23]Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA,OJ L 135/53; Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, as amended by Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime.

[24]GDPR Article 37.

[25]GDPR Articles 38 and 39.

[26]GDPR Preamble par.167.

[27]GDPR Article 40.

[28]GDPR Article 42.

[29]GDPR Article 30(5).

[30]GDPR Article 57(1)(b).

[31]GDPR Preamble par. 132.

3.6 Transparency, Accountability and Self-Regulation

The Directive provided that personal data shall be processed fairly and lawfully (Principle of Lawfulness). The GDPR strengthens this principle by adding that personal data shall be processed lawfully, fairly and in a *transparent manner*[32] in relation to the data subject. Organizations are also obliged to provide transparent information in relation to the exercise of rights,[33] when the personal data are obtained from the data subject[34] and when these data are obtained from other sources.[35] Similar transparency obligations are stipulated when joint controllers inform data subjects of their respective responsibilities,[36] when associations or professional bodies prepare codes of contact,[37] when DPAs monitor approved codes of contact,[38] when certification mechanisms are established[39] and when accredited certification bodies adopt procedures for handling complaints about infringements of certifications.[40] In addition, the GDPR obliges Member States to appoint their DPAs by means of transparent procedures.[41]

When Julius Caesar was asked why he divorced his wife, he is said to have replied that not only she had to be honest but also she had to appear to be honest. The principle of *accountability* describes just that. The GDPR stipulates that controllers should comply with its provisions but also, they should be responsible (and able) to demonstrate their compliance.[42] The GDPR does not give any guidance on how the principle of accountability can be put into practice. However, *data breach notification*[43] could be seen as a tool for promoting this principle.[44] Accountability should be linked to transparency. For example, to demonstrate the validity of a person's consent, a controller should be in a position to prove that information was given to that person before he gave his/her consent. In its Opinion on the Internet of Things,[45] the Article 29 Working Party recognizes that:

> In many cases, the user may not be aware of the data processing carried out by specific objects. Such lack of information constitutes a significant barrier to demonstrating valid

[32]GDPR Article 5(1)(a).
[33]GDPR Article 12(1).
[34]GDPR Article 13(2).
[35]GDPR Article 14(2).
[36]GDPR Article 26.
[37]GDPR Article 40.
[38]GDPR Article 41(2)(c).
[39]GDPR Article 42(3).
[40]GDPR Article 43(2)(d).
[41]GDPR Article 53(1).
[42]GDPR Article 5(2).
[43]GDPR Articles 33 and 34.
[44]GDPR Preamble par. 85.
[45]Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, Adopted on 16 September 2014, Ref.14/EN, WP223, p 7.

> consent under EU law, as the data subject must be informed. In such circumstances, consent cannot be relied upon as a legal basis for the corresponding data processing under EU law.

The Directive was at times seen by the industry as hindering innovation and emerging technologies. The GDPR needed a serious "face lift" to change that perspective and the changes it introduces to that effect are not just cosmetic. It promotes the principle of *self-regulation* by encouraging the drawing up of codes of conduct,[46] certification mechanisms and data protection privacy seals and marks.[47] In addition, the abolition of the Directive's obligation to obtain an authorization prior to the transfer of personal data to third countries, in the absence of a legal basis for the transfer, should also be seen as a form of self- regulation.

3.7 Supervisory Role and Cooperation of the DPAs

One may argue that the promotion of accountability and self-regulation shifts the power of oversight from DPAs to associations and professional bodies. This is not true. The GDPR balances this shift by strengthening the *supervisory role* of DPAs. Among other things, DPAs are empowered to issue opinions, approve and review codes of contact, to accredit certification bodies and review certification mechanisms and, overall, they are armed with more investigative, corrective and authorization powers.[48] In relation to transfers of personal data to third countries, DPAs are empowered to authorize standard contractual clauses and administrative agreements and approve binding corporate rules. In the Article 29 Working Party's Action Plan[49] for the implementation of the GDPR it is recited that:

> A new governance model is on its way giving a higher role to the DPAs. It is a distributed governance model built on three pillars: national data protection authorities, enhanced cooperation between authorities and EDPB level for consistency.

The increasing number of cases of cross-border nature requires the strengthening of *cooperation* among DPAs, particularly, in the course of inspections. While the GDPR obliges Member States to provide to DPAs the resources necessary to perform their duties,[50] it remains true that, in this case, size does matter. It is reasonable to assume that the DPAs of Germany and France are bound to have more resources than the Cypriot or the Maltese DPAs. The GDPR provides that, in the course of *joint operations*, a DPA can invite and host staff from other DPAs, who

[46] GDPR Article 40(1).

[47] GDPR Article 42.

[48] GDPR Article 58.

[49] Article 29 Data Protection Working Party, Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), Adopted on 2 February 2016, Ref. 442/16/EN, WP 236, p 2.

[50] GDPR Article 52(4).

shall act under the direct guidance of the hosting DPA.[51] DPAs are obliged to offer each other relevant information and *mutual assistance*.[52] In cross-border cases that require the cooperation of several DPAs, the GDPR provides for the establishment[53] of a *Lead Authority* which shall have specific competences and tasks[54] and which shall cooperate with other concerned DPAs in an endeavor to reach consensus.[55] In addition, the Commission and the DPAs are obliged to develop *international cooperation*[56] mechanisms with the respective authorities of third countries.

Another bitter truth drawn from the implementation of the Directive is that DPAs have not always faced cross-border cases in the same manner, mainly because of differences in their culture, traditions, administrative and judicial systems and enforcement capabilities. To tackle this problem, the GDPR introduces the *consistency mechanism*,[57] which purports to ensure more uniform and homogenous enforcement approaches and results. In cases where DPAs cannot reach a consensus for the appropriate measures to be taken, the GDPR establishes a *dispute resolution*[58] mechanism, through which, binding decisions can be reached in the synergy of the *European Data Protection Board*[59] (EDPB), an independent body with legal personality, composed of the heads of each DPA and the European Data Protection Supervisor, entrusted to ensure the consistent application of the GDPR.[60]

3.8 Responsibilities, Liability and Enforcement

The Directive allowed a degree of flexibility in relation to the allocation of responsibilities to controllers, representatives and processors. In some national laws, *responsibilities* burdened mainly the controller and representatives or processors, if any, were burdened with no or few responsibilities. Furthermore, in cases of joint controllers, the Directive did not provide any clear rules about their share of responsibilities. Consequently, it was not always easy to determine who should be blamed or to what extent one should be blamed for. The GDPR introduces more legal certainty for the respective responsibilities of controllers and processors. For example, a controller must be able to *demonstrate* compliance with the GDPR,[61]

[51] GDPR Article 62(3).
[52] GDPR Article 61.
[53] GDPR Article 54.
[54] GDPR Articles 56 and 57.
[55] GDPR Article 60(1).
[56] GDPR Article 50.
[57] GDPR Article 63.
[58] GDPR Article 65.
[59] GDPR Article 68.
[60] GDPR Articles 69–76.
[61] GDPR Article 24(1).

joint controllers must determine their respective responsibilities in a *transparent manner*[62] and a processor must give to the controller all *information* necessary to be able to demonstrate his compliance.[63] In addition, the GDPR obliges controllers and processors established in a third country outside the EU to designate a representative, if they offer goods or services to data subjects in the EU, irrespective of payment,[64] or if they monitor their behavior.[65]

The GDPR provides that a person has the right to launch a *complaint*[66] with any DPA, in particular in the MS where he resides or works or in the MS where the alleged infringement has taken place. Any person has the right to an effective *judicial remedy* where his or her rights have been infringed.[67]A person, who suffered damage because of an infringement of the GDPR, has the right to receive *compensation*.[68] In cases of joint controllers or in cases where a controller and a processor are responsible for the cause of damage, each controller and processor shall be held *liable* for the entire damage.[69] Any person or organization can challenge a *DPA's* legally binding *decision* that concerns them before a national court.[70] If the DPA's decision was based on a previous opinion or decision of the EDPB in the context of the consistency mechanism, the DPA must forward the EDPB's opinion or decision to the court.[71]

Because of the defragmented transposition of the Directive and the differences among MS's cultures, administrative and judicial systems, DPAs did not share the same enforcement powers. The Danish and the Estonian DPAs for example cannot impose administrative sanctions.[72] The GDPR arms DPAs with the same *corrective powers*[73]and sets out uniform *conditions for imposing administrative fines*,[74] but it leaves it to MS to provide the rules on other *penalties* for infringements that are not subject to administrative fines.[75] Following the example of the United States Federal Trade Commission, the GDPR foresees quite dissuasive administrative fines that, in some cases, can be up to 20 million euro, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year. Ironically, during the consultation period for the preparation of the

[62]GDPR Article 26(1).
[63]GDPR Article 28(3)(h).
[64]GDPR Preamble paragraphs 23 and 80.
[65]GDPR Article 27.
[66]GDPR Article 77(1).
[67]GDPR Article 79(1).
[68]GDPR Article 82(1).
[69]GDPR Article 82(4).
[70]GDPR Article 78(1).
[71]GDPR Article 78(4).
[72]GDPR Preamble par. 151.
[73]GDPR Article 58(2) and Preamble par.151. Special rules apply to Denmark and Estonia.
[74]GDPR Article 83.
[75]GDPR Article 84.

GDPR, a number of US based enterprises were calling for the need for a level playing field on both sides of the Atlantic.

3.9 Transfers to Third Countries

In spite of criticisms associated with the Directive's model for transfers of personal data to third countries outside the EU, the GDPR maintained essentially the same model. Transfers to third countries or international organizations may still rely based on *Adequacy Decision*[76] determining that a third country or an international organization ensures a level of protection equivalent to that applied in the EU. However, the GDPR provides more detailed rules for the assessment of the level of protection offered by a third country or an international organization and obliges the Commission to monitor developments that may affect this level on an ongoing basis and to periodically review the Adequacy Decision. These improvements reflect the rational of the Court of Justice of the European Union (CJEU) in the case of Maximilian Schrems v. Data Protection Commissioner.[77] In this milestone ruling, the CJEU invalidated the Commission's "Safe Harbor" Adequacy Decision, which was used as a legal basis for transfers to the United States (US). In 2016, the Commission adopted the "Privacy Shield" Decision to regulate transfers to the US, in line with the CJEU's Schrems judgment.

Controllers and processors may also transfer personal data to third countries or international organizations on the basis of *appropriate safeguards*[78] such as legally binding instruments between public authorities, *binding corporate rules*,[79] standard data protection clauses adopted by the Commission or by a DPA and approved by the Commission, codes of contact or certifications. These safeguards do not require the DPA's authorization. Transfers may also rely on appropriate safeguards that require a DPA's authorization, in the frame of the consistency mechanism,[80] such as contractual clauses between data exporters and data importers or data protection rules inserted into administrative agreements between public authorities.

In the absence of adequacy decisions or appropriate safeguards, the transfer may take place based on *derogations for specific situations*[81] such as the data subject's consent, the performance of contracts, reasons of public security, the protection of vital interests of the data subject or others, the exercise or defense of legal claims

[76]GDPR Article 45.

[77]CJEU, *Maximillian Schrems v Data Protection Commissioner A/S,* Case C-362/14, Judgment of 6 October 2015.

[78]GDPR Article 46.

[79]GDPR Article 47.

[80]It is not clear to the authors why DPAs should apply the consistency mechanism in cases of bilateral administrative agreements, which are a purely national matter.

[81]GDPR Article 49.

and transfers from public registries. These transfers however can only take place if they are not repetitive, if they concern a limited number of persons and for compelling, overriding interests of the controller. These cases, again, do not require the authorization of a DPA, but require that the controller informs the DPA of the transfer and that the he documents his assessment for the need for the specific transfer. If a controller or a processor is ordered by a court, a tribunal or a public body of a third country to transfer or disclose personal data, the controller or processor must comply, only if there is an international agreement in force between the third country and the EU or a MS.[82]

3.10 Economic Growth and Social Integration

It is generally acknowledged that if the EU wishes to be an important player in global economy, it must invest in technology. As a rule, new technologies require a lot of background research. Therefore, researchers should be able to have access to and share information. At the same time, there is an increasing need for sharing information between the public and the private sector, in particular, for enabling the free movement, establishment and employment of persons within the internal market. For these reasons, the *subject matter* of the GDPR provides that the flow of information within the EU should be neither restricted nor prohibited under the GDPR.[83] In their Joint Statement of 26 November 2014,[84] DPAs recall that:

> Our daily life is increasingly digital. In less than a decade, professional, economic and private activities have gradually shifted towards a digital environment. This evolution has opened a world of new opportunities and has enabled the development of extraordinarily innovative goods and services, which meet individual and collective demands. Personal data is the basic building block of this digital world.

In the Preamble of the GDPR, it is explained that the fragmentation of the Directive has resulted in differences in the level of protection across MS, which may constitute an obstacle to the pursuit of economic activities and distort competition.[85] To pursue their activities, organizations in both the private and the public sector make use of personal data on an unprecedented scale. This scale is further increased by rapid technological developments and globalization.[86] Enterprises can profit from a more coherent and homogenous set of data protection rules that will enhance citizens trust, in particular, in their on line economic activities.

[82]GDPR Article 48.

[83]GDPR Article 1(3).

[84]Article 29 Data Protection Working Party, Joint Statement of the European Data Protection Authorities assembled in the Article 29 Working Party, Adopted on 26 November 2014, Ref. 14/EN, WP 227, p 2.

[85]GDPR Preamble par. 9.

[86]GDPR Preamble par. 6.

In the Preamble, it is further explained that the right to personal data protection is not an absolute right but it must be considered in relation to its function in society and be balanced against other fundamental rights.[87] The GDPR pays particular attention to the right of freedom of expression. For example, it stipulates that the right to be forgotten shall not be applied, inter alia, to the extent that processing is necessary for exercising the right of freedom of expression and information.[88] In addition, it obliges MS to reconcile by law the right to personal data protection with the right of freedom of expression and information.[89]

4 Closing Remarks

Readers, particularly newcomers in the field of data protection, may find it difficult to understand how one piece of legislation, the GDPR is supposed to protect natural persons against the processing of their personal data and, at the same time, pursue economic growth and social integration by allowing the free movement of these data. They may also reasonably argue that the flow of information may not be so free after all, owing to all obligations that the GDPR imposes on controllers and processors. An easy way to understand the dual nature of the GDPR is to imagine it as a set of traffic lights. At red lights drivers stop, at green lights they move ahead. The GDPR does not prevent the flow of data, it merely regulates it, by a system of dos and don'ts, in a similar way that traffic lights regulate the flow of cars. The obligations that the GDPR imposes to controllers and processors should not be seen as obstacles hindering the free flow of personal data but as a way of regulating this flow. After all, the essence of the GDPR is trying to strike the right balance between these dos and don'ts.

If this article was meant to be a critique of the GDPR, the authors would agree that it is certainly a very ambitious piece of legislation that sets the bar of expectations quite high. Expectations however, may often be subjective and a matter of different perspectives. Stakeholders with different interests may have different expectations. For example, it would be reasonable to assume that enterprises and the industry wish that the GDPR introduces more legal certainty and harmonized rules in the data protection regime, that DPAs expect the GDPR to strengthen their powers and that, parents would simply like to see more protection for their children. Therefore, ultimately, the question everyone raises is: "Will the GDPR deliver what is expected to deliver?" While the authors believe that the legislator, through the GDPR, has managed to accommodate the needs of different stakeholders and to balance their interests, they prefer to abstain from the temptation of assessing the GDPR by attempting to answer this question, which, as

[87]GDPR Preamble par. 4.
[88]GDPR Article 17(3)(a).
[89]GDPR Article 85(1).

explained in the introduction, deserves a more thorough legal analysis. After all, the real assessment of the GDPR will be the test of time, when it is put into practice.

Educators and psychologists would argue that that there is no right or wrong method of learning. The authors assume that the assimilation of new information may be easier when it can be associated to familiar experiences or knowledge. To that effect, the authors have adopted the following two hypotheses. First, familiarizing readers with some of the core provisions of the GDPR would enable some readers to better grasp its essence. Second, associating some of the core provisions of the GDPR to what the GDPR is expected to deliver would assist some readers to have an insight to the legislators' will, as it is reflected in the GDPR. The authors acknowledge that this article is not tailored–cut as a one–size-fit-all. Readers and in particular newcomers in the field of data protection will need to go through the GDPR, article by article to understand the detailed letter of the Law. It should also be emphasized that readers should be free to interpret the GDPR and draw their own conclusions based on their individual experiences and set of expectations form this legislation, without prejudice to the opinions of the authors, as reflected in this article. After all, ultimately it is the job of the CJEU or the national competent courts to interpret the spirit and the letter of the GDPR.

References

Article 29 Data Protection Working Party, Joint Statement of the European Data Protection Authorities assembled in the Article 29 Working Party, Adopted on 26 November 2014, Ref. 14/EN, WP 227, p 2

Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, Adopted on 16 September 2014, Ref.14/EN, WP223, p 7

Article 29 Data Protection Working Party, Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, Adopted on 16 September 2016, Ref. 14/EN, WP221, p 2

Article 29 Data Protection Working Party, Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), Adopted on 2 February 2016, Ref. 442/16/EN, WP 236, p 2

Chapter 2
The General Data Protection Regulation: A Law for the Digital Age?

Lilian Mitrou

Abstract In 2016, the General Data Protection Regulation has opened a new chapter for the protection of informational privacy in Europe. More than a simple revision of the Data Protection Directive (1995) and less than a regulatory paradigm shift, the Regulation attempts to keep path with technological and socio-economic changes while guaranteeing the persons' fundamental rights and enabling the control over their data. This contribution aims at examining whether this reform deals adequately with the challenges of the digital era.

The analysis gives an overview of the new framework, its background and goals, focusing on some issues that are Internet relevant. In this respect, we discuss the provisions regarding the extended material and territorial scope of the Regulation and the implementation issues that may arise. We also addressed the consent and the way the European legislator tries to foster it as a legal ground of data processing and core manifestation of the right to protection of personal data. Further, we examine the new rights (right to be forgotten, right to data portability) that are introduced in the data protection law to reinforce the individuals' rights as digital users. By assessing the new framework, we conclude that the changes introduced in combination with innovative regulatory elements, such as privacy by design or data protection impact assessments, constitute an important improvement in the sustaining and maturing of data protection law and may serve to respond to face technological challenges and mitigate risks.

L. Mitrou (✉)
University of the Aegean, Samos, Greece
e-mail: l.mitrou@aegean.gr

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_2

1 Introduction: New Law to Address New Challenges?

1.1 The Emergence of Internet as Challenge for Data Protection Law

The European Data Protection Directive (Directive 95/46/EC),[1] adopted in 1995, has been a milestone in the history of personal data protection with worldwide impact and influence. Directive 95/46/EC has been credited with creating one of the world's leading paradigms for privacy protection.[2] However, despite the substantially positive track record and general acceptance of the Directive, its efficiency, if not the applicability itself, has been contested. The Directive 95/46/EC was conceived (in 1990), discussed and adopted before the explosion of the Internet and its impacts on economy, society, governance, communication and life.

The convergence of the network around a single interoperable platform, the emergence of the "semantic Web" and Web 2.0, as well as the changes in identification and authentication techniques, identity management and profiling, have created a new environment. Technological and social phenomena like social networks, cloud computing, Radio Frequency Identification (RFID) and geo-location devices and applications, the new possibilities of data mining and big data analysis have profoundly changed the way, and the extent to which, data are processed and pose crucial challenges for data protection. While there were threats to privacy long before the Internet era, the Internet has increased the capabilities of businesses, governments and individuals to intrude on the privacy of others.[3]

Several inherent features of Internet (and especially Web 2.0) supported technologies and platforms (e.g. digitization, availability, recordability and persistency of information, public or semi-public nature of social media profiles, messages, etc.) encourage not only new forms of communication and interaction but also monitoring, surveillance and the so-called "omniveillance".[4] The exponential growth of smart technologies gave rise to new forms of tracking individuals' activities, behavior, habits, and personality.[5] Individuals may be targeted and

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281/31). In this text we refer to this Directive as Directive 95/46/EC to avoid the confusion with "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA" (Directive).

[2] Robinson et al. (2009), pp. 6 f., 22 f.

[3] "Never before hence the behaviour of individuals was so closely observed and recorded, the attempts to expand the use of the data collected so persistent, the proliferation of ever more detailed personal profiles so intensive". See Simitis (1999), p. 5ff.

[4] About the notion of "omniveillance" see Blackman (2009), p. 313 ff.

[5] Skouma and Léonard (2015), p. 35f.

tracked (and/or vice versa: tracked and targeted) for many reasons, varying from advertising for lucrative purposes to political motives or reasons related to public and state safety, as well as public security.

1.2 *Internet: A Field for Pervasive Surveillance and Data Collection*

Exactly the aspects of the Internet that make it such a powerful information and communication medium, transform it into a fertile ground for collecting personal data about users.[6] The technical infrastructure of the Internet combined with ever-advancing computer technology makes it easy and cheap to collect, combine and use vast amounts of personal data.[7] Web sites, on line businesses and Internet Service Providers offering goods, services and information on-line, typically collect, process and store immense amounts of information about consumers, without consumers, necessarily, either knowing their data is collected, or consenting to that collection. Online tracking applications analyze users' data using algorithms and profiles/patterns or dig into digital traces users leave on social media thus resulting into quite accurate individuals' profiles. Through data aggregation,[8] data mining[9] and profiling[10] of users, companies tailor their policies and marketing efforts specifically towards their specific interests.[11]

The conscious or unconscious exposure of personal information to an indefinite audience of social media suggests both a "traditional" and "social panopticism".[12] Web 2.0 is becoming, slightly but definitely, an ideal "topos for social surveillance"[13] and "participatory panopticism",[14] an Omniopticon, in which "the many

[6]Froomkin (2000), p. 1486.

[7]Regarding the definition and notion of personal data according to EU law see Article 29 Data Protection Working Party (hereafter Article 29 Working Party), Opinion 4/2007.

[8]Data aggregation is understood as any process in which information is gathered from various sources and expressed in a summary form.

[9]Data mining is understood as the automated processing of digital materials, which may include texts, data, sounds, images or other elements, or a combination of these, to uncover new knowledge or insights.

[10]The General Data Protection Regulation (EU) 2016/679/EU (hereafter GDPR or Regulation) includes a definition of profiling in Article 4(4) that states that profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

[11]This practice is characterized as "behavioral tracking" that leads to "behavioral/targeted advertising". See Hotaling (2008), p. 529ff; Skouma and Léonard (2015), p. 37f.

[12]See Nevrla (2010), p. 5ff.

[13]Tokunaga (2011), pp. 705–713.

[14]Whitaker (1999), p. 139ff.

watch the many".[15] Every Online Social Network (OSN) user can equally be "observer" and "observed", controller and data subject.OSN users' profiling may become an every-day routine, a "peer-to-peer monitoring", understood as the use of surveillance tools by individuals, rather than by agents of institutions public or private, to keep track of one another.[16]

Users are losing control over their data and the use thereof, as they are becoming detectable. The combination of all this information provides a powerful tool for the accurate profiling of users. Moreover, it is quite simple to identify a person, even after her key attributes (name, affiliation, and address) have been removed, based on her web history.[17] The availability of cheap interactive digital communications and the development of the mobile Internet, have enhanced the ability to monitor others as monitoring has become easier, cheaper and more efficient. Both the Web 2.0 architecture and the users' attitude create a situation that may be characterized as panoptic in design. Social connections, comments, views and preferences (expressed through "likes" or "retweets") are turning into visible, measurable, searchable and correlatable content.

Social media have widened society's opportunities for communication, while they offer ways to perform employees' screening and profiling. Employers searching for information that may provide insight on employees and extend monitoring to private spaces, activities and time also increasingly monitor online social media profiles, blogs, tweets and online fora. The nature of Internet encourages even novel surveillance tendencies via behavior and sentiments' detection and prediction. Information gathering about employees' performances, attitudes and behavior outside the—traditionally conceived—work sphere deprives them from informational privacy, i.e. the capacity to control the information concerning them, and thus the capacity for autonomous decision—and choice-making and to maintain a variety of social identities and roles.[18]

Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale to pursue their activities.[19] Despite the lack of centralized control over the Internet, its platforms and applications allow multilevel and latent surveillance, thus posing new risks for individuals by forming new power relations and asymmetries. Online media and user generated content mining provide support for decision makers to detect, track or even predict opinions and attitudes.[20] Governments' interest on information gained through data aggregation, mining of social media is growing, as law enforcement, crime prevention, and policies to face tax evasion may require "connecting the dots". Web 2.0

[15] See Kandias et al. (2013), pp. 1ff.

[16] Andrejevic (2002), p. 481 ff.

[17] Castelluccia et al. (2011), p. 17; Gritzalis et al. (2014), p. 283ff.

[18] Kandias et al. (2013), p. 229ff.

[19] As noted in Recital 7 of the GDPR.

[20] About data mining for purposes of predicting public opinion and attitudes, see Sobkowicz et al. (2012), p. 470ff.

technological features extend the possibilities of traditional surveillance: Governments may use the informational goldmine of online social media to extract implicit, previously unknown and potentially useful information and to discover or infer previously unknown facts, patterns and correlations.[21]

1.3 A New Law for Responding to Internet Challenges?

The Internet steadily creates new processing and analysis capacities and opportunities but at the same time poses intensively new challenges for regulation. Given its transnational nature and the lack of user control, the debates about privacy and data protection on the Internet relate on several questions: first, the question of informed consent, the question of transparency, the question of exercising user's rights and last, the applicability and enforceability of legal rules on the Internet. The critical question is if, how and to what extent rules and standards regarding the right to privacy and informational self-determination can regulate the online reality in an effective way?

Two decades ago, the EU legislator could neither predict the indexing, cross-referencing and profiling capabilities of Internet, nor the new communication environment, influenced by globalization, online social media and data sharing. The array of norms provided in Directive 95/46/EC, even if interpreted in an open and wide way, failed to adequately shield individuals. If the birth of data protection in Europe was linked to the impressive developments of the 70s,[22] its recent reform aimed at responding to the risk of increasing loss of relevance and effectiveness of the 3rd generation legislation[23]: a new framework had been proposed to ensure a high level of protection, in particular in view of the great challenges and big risks because of technological developments.

Is the new European framework, the General Data Protection Regulation (hereafter GDPR)[24] Internet-adequate? Does the GDPR constitute a revision of the current framework or a legislative paradigm shift in data protection thus enabling better protection of informational privacy rights of users?[25] This contribution aims to examine how the data protection reform deals with the challenges of Internet. The analysis will attempt to give an overview while focusing on some issues that are Internet relevant without any ambition of being exhaustive. Section 2 deals with

[21]Rubinstein (2012), p. 3ff.

[22]See Simitis (2014), p. 82 ff. 134 ff.

[23]See Kiss and Szoke (2014), p. 311 ff.

[24]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L.

[25]See Warso (2013), p. 496ff., who dealt with the question of whether the proposal for a GDPR meets the criteria of a new generation of regulation.

the (material and territorial) scope of the new European data protection framework. Section 3 addresses the notion of consent and the way it is regulated as a legal ground of processing in the GDPR. The fourth section concerns the new rights (right to be forgotten, right to data portability) that are introduced in the data protection law to respond to the new challenges. The last section (5) includes a first assessment of the GDPR regarding whether the new framework is able to regulate data processing in the Internet era.

2 Scope of Application: An Internet Jurisdiction?

2.1 An Internet-Conscious Definition of Personal Data

The attempt to keep pace with the technological developments is mirrored already in the way personal data and data subjects are perceived and defined in the GDPR. The data protection framework is applicable as far as data under processing can be qualified as "personal data", namely it refers to information relating to an identified or identifiable natural person ("data subject"). It is the identifiability of a person that results in the applicability of the law. Identifiability is understood as the ability to single out and/or identify an individual on the basis of particular pieces of information that we may call "identifiers", and which hold a particularly privileged and close relationship with the particular individual.[26]

The definition of personal data has been aligned with the online reality. The definition contains not only that a person may be identified "in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Directive 95/46/EC Article 2a); the "online identifier" has been added to the indicative list of features that may identify a natural person, directly or indirectly (Article 4 par 1 (a). In this sense an IP address, even if allocated to a device, falls within the category of information that can lead indirectly to the identity of an Internet user.[27] The Article 29 Working Party has considered IP addresses as data relating to an identifiable person stating that "in fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms. Therefore, the information should be considered as relating to identifiable individuals and the processing should be subject to data protection rule."[28]

The argument that offering of goods and services, as well as monitoring often addresses IPs, e.g. users, whose identity is not known, is not convincing. Tracking of internet users relates inherently with the exploitation of the information captured

[26] Article 29 Working Party, Opinion 4/2007, p. 12f.

[27] As noted by Synodinou and co-authors (2016), p. 66 ff.

[28] Working Party Opinion 4/2007, p.11. See also Article 29 Working Party, Opinion 5/2014, p. 8f.

as their personal data is extensively used as currency in exchange for services.[29] This approach has been confirmed by the new European data protection framework: Recital 30 of GDPR states that "natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".

2.2 Online Household Exception?

With regard to the material scope, a significant and controversial issue relates to the limitation of the so-called household exception. Both Directive 95/46/EC and the GDPR provide that the processing of personal data by a natural person, "in the course of a purely personal or household activity", does not fall under their provisions. The European legislator considered the impact of any processing in the context of personal and household activities as rather innocuous,[30] while another underlying justification was the difficulty to impose legal requirements to all individuals and secure compliance with the law on this level.[31] Moreover such an intrusion of the law into the "private sphere and space", in practice into the daily activities of individuals, would be perceived as unjustified and excessive, which would undermine the social acceptance of the data protection legal framework.

The household exemption, as provided in Directive 95/46/EC lacked the necessary clarity in defining personal and household activities. Recital (12) provided some guidance as to the meaning of such activities referring to "exclusively personal or domestic activities" and providing as examples "correspondence and holding of records of addresses". Although the use of words "purely" and "exclusively" indicated the need to interpret and apply the exception in a narrow way the provision of Article 3 (2) of Directive 95/46/EC remained vague.[32] Defining the scope of application of the household exception has never been an easy task and became much harder in the era of quite unlimited availability and accessibility of information and communication technologies and information. This exception can be traced back to the 1990s, when technical, social and behavioral standards put limits to personal data processing carried out by individuals.[33] The exponential increase of the use of the Internet (in combination with the ubiquity of data

[29]European Network and Information Security Agency - ENISA-(2012a), p. 1.

[30]See van Eecke and Truyens (2010), pp. 536, 540 with reference to "Rome memorandum" of the International Working Group on Data Protection in Telecommunications, 4 March 2008.

[31]Wong and Savirimuthu (2007), p. 242ff.

[32]See Xanthoulis (2013), p. 139.

[33]See Kotschy (2014), p. 277.

collection and sharing practices, advances in search methods, content creation and decreasing costs of technological products) enables perpetual storage, continuous accessibility, sharing and multiple use of information, turning the Internet into a holistic communication environment, where the boundaries between public and private sphere are continuously blurring.

In the Lindqvist case,[34] the Court of Justice of the European Union (CJEU) in a landmark judgment provided guidance as to the scope of the household exception, thus answering the question of the applicability of the law in the course of online processing activities of individuals, such as uploading on websites or activities undertaken within online social networks. The criterion invoked by the CJEU was the extent of accessibility, suggesting that the "(household) exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people" (paragraph 47 of the judgment).[35] According to the Court, that applied the public/private partition, unlimited access to an indefinite audience gives rise to the applicability of Directive 95/46/EC. This criterion has been criticized, as the CJEU specified no limit or threshold.[36]

Household Exception and Social Networks

In the context of social networking, the Article 29 Working Party suggested the use of certain factors to assess if a user is acting in a private context. In line with the argumentation of the CJEU, the Working Party considered[37] that when the information of a user profile can be accessed by all members of a social networking service or when search engines can index the data, then the user does not benefit from the household exemption. According to Article 29 Working Party, this shall be additionally the approach when the user does not select in accepting contacts and connects to people regardless of any possible link to them.[38] The extent of the exception is strictly related to the question of applicability of the Directive 95/46/EC in social networks environment. If the legislators of the regulatory framework, adopted two decades ago, had not anticipated the emergence of WEB 2.0 and the challenges it poses, the drafting of a new legal instrument was deeply influenced by the need to draw a clearer line to bound personal and domestic activities. Privacy

[34]CJEU, *Bodil Lindqvist Case* C-101/01, Judgment of 6 November 2003.

[35]Dammann and Simitis noted that an extended data processing might be an evidence to suggest that processing involves professional activities. See Dammann and Simitis (1996), p. 123f.

[36]See Xanthoulis (2013), p. 139ff who points out that the CJEU has not drawn the line between public and private purposes. See also Wong and Savirimuthu (2007), p.256.

[37]Working Party, Opinion 5/2009 on online social networking (Opinion 5/2009).

[38]See Kosta et al. (2010), p. 197.

advocates underlined that "maintaining an equally broad exception for personal or household activity in the new Regulation (would) pose an increasing danger for data protection as there will be no legal instrument to defend data protection standards versus natural persons in their online activity".[39]

The European Commission (hereafter Commission) proposed, in 2012,[40] a household exemption along the lines of the existing Directive 95/46/EC, however adding the gainful interest criterion while referring to "exclusively, (instead of "purely") personal or household activities. Moreover, Recital 15 (GDPR Proposal) clarified that such activities shall be "without any connection with a professional or commercial activity". The European Parliament advocated the deletion of the phrase "without any gainful interest", as the processing of personal data by a natural person for private and household purposes can sometimes have a gainful interest, but should still fall outside the scope of the Regulation as long as there is no connection to a professional or commercial activity. The wording of Article 2(2)(c) of the GDPR is identical to the one found in Directive 95/46/EC, confirming in this way, that the—usual—compromise[41] is to avoid running new regulatory risks. The "old" wording, namely the reference to "purely personal and household activity", has been the recourse of the European legislator. Recital 18 of the GDPR includes the lack of "connection to a professional or commercial activity" as delimitation element while "social networking and online activity" is explicitly referred as a category of personal/household activity. In parallel, it is clarified that controllers or processors which provide the means for processing personal data for such personal or household activities are subject to the provision, an addition that—strictly systematically viewed—was not necessary.

The readiness to accept the application of the law to social networks environments was restricted: if on the one side it was argued for the applicability of data protection law to data processing by individuals in their capacity as private persons, considering that nowadays home users can store terabytes of (potentially sensitive) data, which can lead to significant damage,[42] on the other side the ability of the EU legislator to provide a sufficient determination of private conduct was contested because of the vast variety of users' online activities.[43] However, a different

[39]European Digital Rights (EDRi): Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2013) p. 6.

[40]Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)—Brussels, 25.1.2012 COM (2012) 11 final.

[41]According to the so-called General Approach of the EU Member States, reached in June 2015, exempted should be personal and household activities without any reference to "exclusively" in the text of the provision. However, in Recital (15) of the General Approach it was proposed to clarify that personal and household activities include social networking and on-line activity undertaken within the context of such personal and household activities.

[42]See Van Eecke and Truyens (2010), pp. 536, 540.

[43]See Warso (2013), p. 492; See also Xanthoulis (2013), p. 138.

approach, that could impose some obligations to the privately acting individuals (such as the obligation to provide access and correction to other concerned persons), would address more adequately the challenge of strengthening individuals' rights in the Internet era without discouraging online communication and participation.

2.3 Digital Territorial Scope?

As the Directive 95/46/EC was enacted in the early phase of Internet use[44] the European legislator had as a point of reference data contained in physical documents. As the "physical element " was predominant in the Directive 95/46/EC, the distinguishing criterion for defining its scope of application referred primarily to the location of the data controller.[45] The territorial reach of Article 4 of Directive 95/46/EC induced a broad scope of application, its legal implications extending beyond the EEA territory. The ruling of the CJEU in the *Google v. Spain* case[46] clarified and confirmed the territorial scope of EU law (Directive 95/46/EC) and its application to personal data processing conducted by a foreign controller established outside the EU, which has a "relevant" establishment in the EU.[47]

The Uncertainties of "Equipment" Criterion

Alternatively, Directive 95/46/EC foresees the location of "equipment used, automated or otherwise" on the territory of EU being used when the controller is established outside the EEA to define the territorial scope of the EU legal framework. The alternative mechanism of "use of equipment" was designed to prevent the circumvention by data controllers of the protection afforded to data subjects by EU law and respectively of their legal responsibilities through relocation of their establishments outside the EU.[48] Consequently, the Article 29 Working Party drew the conclusion that the provisions of the Directive 95/46/EC can be applicable to services with an international dimension such as search engines, social networks and cloud computing.[49]

---

[44]At least before, it became frequently used and popular as a mass information and communication medium.

[45]See Baño Fos (2014), p. 19f. In its initial proposal, concerning Directive 95/46/EC the Commission identified the location of the data file as a primary determining factor but in the course of discussion within European Parliament and the Council of the EU, there was a shift, from the criterion of the location of the file, to the criterion of the establishment of the controller.

[46]CJEU, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12, Judgment of 13 May 2014.

[47]See Article 29 Working Party, Update of Opinion 8/2010 (2015).

[48]See de Terwangne and Louveaux (1997), p. 237f.

[49]Working Party, Opinion 8/2010, p. 8.

Data protection law has been the subject of an increasing number of jurisdictional disputes, many of which are related to the Internet: The scope of the EU data protection law has been contested by US government officials,[50] as well as business groups.[51] Data controllers located outside the EU have become involved in disputes with European Data Protection Authorities (DPAs) about the jurisdictional scope of the EU data protection law[52] and on the other side DPAs have complained about the extraterritorial effect of US privacy laws.[53]

International conflicts and disputes have arisen over the reach of the EU data protection framework, the most controversial basis being that of the "use of equipment". This term mirrored the roots of the Directive 95/46/EC in the pre-Internet era[54] and was generally thought to refer to information systems and/or networks that were controlled by a data controller from an establishment outside the EU and operated by him.[55] The condition of "making use" was understood as activity undertaken by the data controller with the intention to process personal data.[56] Major concerns and controversies have emerged with regard to the applicability of the Directive 95/46/EK to data processing activities of search engines especially based on the use of "cookies".[57] The Article

[50]See Ross (2001); See also Goldsmith and Wu (2008).

[51]See the comments of the US Council for International Business for the Review of the EU Data Protection Directive. It affirmed the position that the Article 29 Working Party's assertion as to the jurisdictional reach of the Directive 95/46/EC on the Internet is unwarranted and contrary to international law and jurisprudence. http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/paper/uscib_en.pdf.

[52]See the dispute between Google and the Article 29 Working Party regarding whether its data processing in Europe is subject to EU data protection law.

[53]The Article 29 Working Party, while defending the extraterritoriality of EU data protection law against accusations, pointed to the fact that also "in other countries, for example in the United States of America, courts and laws apply similar reasoning in order to subject foreign websites to local rules". See Working document (WP 56) (2002) p. 4.

[54]In addition, Kuner (2010b), p. 229, who notes that the text of the Directive 95/46/EC is of little help in determining the meaning of "equipment", and the Explanatory Memorandum gives only "'terminals, questionnaires, etc." as examples, which hardly provides much guidance.

[55]See Dammann and Simitis (1996), p. 129. Directive 95/46/EC does not attach any relevance to the ownership of any equipment. According to Article 29 Working Party, it is not necessary that the controller exercise full control over the equipment. The crucial criterion is making the relevant decisions concerning the substance of the data and the procedure of their processing. See also Article 29 Working Party document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP 56) (2002) p. 6f.

[56]Article 29 Working Party, WP 56, p. 9f.

[57]Cookies are text files installed on the hard drive of a computer, which receive, store and send back information to a server situated in another country, while a copy may be kept by the website. Cookies are small text files sent automatically by many Internet servers to users who access web pages, and are generally used to authenticate users. The European legislator attempted to regulate and restrict the use of cookies, regarded as "spyware" with the provisions of the e-Privacy Directive (2002/58/EC) and Directive 2009/136/EC that amended provisions of e-Privacy Directive.

29 Working Party affirmed that the installation of cookies enables the controller to link up all information collected from the PC of a via-cookies identified user's device during previous and subsequent sessions and create quite detailed user profiles. The Working Party took also the position that the Data Protection Directive would also apply to identified/identifiable information collected using Java Scripts[58] or spywares.[59] The Article 29 Working Party emphasized, however, that "not any interaction between an Internet user in the EU and a web site based outside the EU leads necessarily to the application of EU data protection law".[60] The approach of the Working Party has been criticized, with emphasis both on the heavy burden for service providers located outside the EU and the weak chances of enforcement.[61]

Jurisdictional controversies resulted in legal uncertainties with further implications for online transactions and the protection of users' rights in the web environment.[62] Because of the lack of legal certainty, data controllers that are conducting online tracking without being established in the EU are likely to escape strict European legislation as demonstrating the "use of means" is quite difficult and—as discussed—disputable. The European legislator had to find alternative solutions to adjust to the online reality. The determination of the applicable law on a solid basis is proved a quite difficult exercise as it implicates with inherent characteristics of the Internet, such as the disconnection from physical territory, the lack of territorial borders that help to indicate the appropriate national or supranational law.

A Functional Approach of Territorial Scope

Despite of intrinsic difficulties linked to cross–frontier situations the European legislator had to consider that the extraterritorial application of the EU data protection legislation does not pertain to an economic good and/or necessity but to an individual's right as the right to data protection, which is embedded in the Charter

[58]Java Scripts are software applications sent by a web site to the computer of a user and allow remote servers to run applications on a user PC.

[59]Defined by the Article 29 Working Party as pieces of software secretly installed on a computer, for instance at the occasion of the downloading of bigger software (e.g. a music player software) to send back personal information related to the data subject (e.g. the music titles the individual tends to listen to), Article 29 Working Party, WP 56, p. 12.

[60]Article 29 Working Party, WP56, p. 9.

[61]See Kuczerawy (2010), p. 80. See also Kuner (2010b), p. 9, who underlines that, with regard to data protection legislation, most protest does not come from states upset by other states' or the EU's extraterritorial actors, but from the data controllers themselves who are subject to extraterritorial regulation.

[62]Ryngaert (2015a), p. 221 notes that "unbounded extraterritoriality, however, has serious adverse consequences for both businesses and states as it might increase transaction costs while vigorous assertions of extraterritorial jurisdiction could cause international competency conflicts between different states".

of Fundamental Rights and Freedoms (Art. 8).[63] The positive protective duties of the EU and its Member States refer also to the need to protect the personal data of individuals falling under its jurisdiction, when such data are processed outside the EU territory. Especially in cyberspace, it is accepted that a violation is conceivable even in the absence of any detriment to the affected individual.[64] In this respect, the EU is regarded as obliged to fulfill its citizens' fundamental right to data protection beyond its territorial borders.[65] The respective provisions of the GDPR are proposed and adopted "in order to ensure that that natural persons are not deprived of the protection to which they are entitled under this Regulation" (Recital 23) merely because a controller or a processor is not established in the Union.

As the Internet trespasses upon every aspect of private and public life, thus becoming ubiquitous, defining and asserting jurisdiction over conduct occurring outside the own territory becomes common.[66] The Regulation has abandoned the "chase for the server", a task more complicated in cloud computing and "software-as-a-service" environments,[67] and focuses on the nature and the intention of data controllers and/or processors activities with regard to their interaction on the Internet.

Like the Directive 95/46/EC the provisions of the GDPR (Article 4a) apply to the processing of personal data in the context of the activities of an establishment of a controller in the Union, regardless of whether the processing itself takes place within the Union.[68] The extension of the applicability also to processors constitutes a novelty thus creating a basis for independent obligations pertaining to processors. Regardless of the location of establishment, the GDPR suggests that even non-EU based controllers and processors will be in the future subject to the provisions and requirements of EU law whether they are performing activities related to the offering of goods or services to data subjects in the Union or to the monitoring of the behavior of data subjects insofar as their behavior takes place within the Union (Recital 24).

Addressees of this provision are foreign controllers and processors that are active on the EU market through online offering of goods and services, irrespective of whether a payment of the data subject is required. Despite of the broad wording of this provision, the European legislator tried to avoid EU data protection law being applied indiscriminately to the Internet as a whole. Recital 23 states that "it should be ascertained whether it is apparent that the controller or processor

[63]Svantesson (2013a), p. 53 ff. identifies a causality between data protection's evolution from economic necessity to autonomous, fundamental right and the EU's territorial extension of its law to safeguard this right.

[64]See Milanovic (2015), p. 134, citing the Judgment of ECHR *Huvig v. France* App No. 11105/84, 24 April 1990.

[65]See Taylor (2015), p. 251 ff.

[66]See Ryngaert (2015b), p. 187. See also Svantesson (2007) p. 244f.

[67]See Hustinx (2014), p. 37, 42.

[68]As well as to the processing by a controller or a processor not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention". Criteria meant to determine whether the controller apparently envisages offering goods or services to data subjects in the Union are "the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language", these factors being indicatively and non-exhaustively mentioned in Recital 23 of the GDPR. In any case, offering of goods and services gives rise to a "(quasi)-automatic establishment of jurisdiction".[69] Based on this approach we can recognize the influence of the "effects doctrine",[70] upon which conduct on the Internet that has effects within other states may assert their jurisdiction.[71]

The criterion of territoriality ("in/within the Union") is still present in the new provisions but there is a shift to the user (data subject) as (the) main point of reference. The monitoring of the behavior of the data subjects becomes a sufficient ground for the applicability of European law.[72] However, the territoriality requirement has also to be met, as this "behavior" has to "take place within the Union" to extend the applicability of the law. In this case, territoriality corresponds to the physical location of the user, although we can assume that in this context the respective provision is referring to "online behavior". However, activities and information on the Internet are not, or at least not easily, located and IP addresses may not be geographically stable.

Furthermore, concerns can be raised with respect to the definition and perception of "monitoring of behavior" as "behavior" seems prima facie a vague and quite unsuitable notion to express the online activity of a data subject that may be tracked and monitored. On the other side, it is not surprising as reference to "behavior" mirrors the main feature of the online reality: The underlying data is typically a log of the user's web activity, and the data collection process based on a log of the user's web activity is called "behavioral tracking". It allows "behavioral profiling", which ends up to" behavioral targeting", which is the common practice of tailoring online content, especially advertisements, to visitors based on their inferred interests or "profile".[73]

As far as it concerns "monitoring", the European legislator illuminates this notion by referring to "tracking on the Internet" that includes, but, apparently, it

[69]See Svantesson (2013a), p. 58.

[70]See Svantesson (2007), p. 87 with reference to Gerber (1984), p. 190.

[71]Various authors who underline that in this case jurisdiction becomes open-ended have criticized the effects doctrine, as in principle all countries have a link to all websites by virtue of their accessibility and because in a globalized economy, everything has an effect on everything. See Kuner (2010a), p. 190 and Schultz (2008), p. 815.

[72]Skouma and Léonard (2015), p. 52; argue that the on-line tracking was one of the key factors that was considered to decide on the need of legislative reshuffling.

[73]ENISA (2012b), p. 3.

is not limited to, "potential subsequent use of personal data processing techniques which consist of profiling a natural person". By analyzing profiling in the context of monitoring, Recital 24 of the GDPR reflects the main choice of the GDPR legislators with regard to the concept of profiling: it is defined, in Article 4 (4), in a generic and technologically neutral way as "...any form of automated processing" but in combination with the purposes[74] it may serve, i.e. "particularly taking decisions concerning her or him, analysing or predicting her or his personal preferences, behaviours and attitudes".[75] In this context, the meaning of "behavior" remains unclear and in any case is not identical with the use of this term in the respective provision regarding the territorial scope. In the explanation contained in Recital 24 "behavior's" analysis and prediction is both regarded as a means and as an end of processing while "behavior" in the context of Article 4 (4) is associated with several aspects of the "online persona" of an individual. Internet tracking and monitoring of online behavior may interfere with the fundamental rights of a person and such a collection may cause a chilling effect[76]: if people know or even speculate that their activities may be tracked, they may adapt their behavior and refrain from exercising the right to information and free speech. Monitoring may have such an impact on freedom of information even if data is collected and a profile is not directly tied to an identified person.

Many have complained about the territorial scope of the GDPR—evidently also search engines, social network, cloud services providers, as well as professional or trade associations.[77] Authors have criticized the regulatory choice of the EU as "data privacy imperialism",[78] while others use the mythical monsters of Scylla and Charybdis to describe the compliance implications the wide jurisdictional scope of data protection law may bring with it.[79] On the other side authors argue for this option by underlying that "sales within such territory also include some (litigation)

[74]Without any direct reference to the process and methods. Hildebrandt (2009), p. 275, defines profiling as the process of discovering patterns in data that can be used to identify or represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify a subject as a member of a group (which can be an existing community or a discovered category).

[75]Article 4 (4) of the GDPR defines profiling as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. This definition corresponds to that of Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling of the Council of Europe that focuses on the creation or use of profiles to evaluate, analyze or predict personal aspects such as performance at work, economic situation, health, personal preferences, or interests, reliability or behavior, location or movements.

[76]See Borgesius (2016), p. 267, who suggests that people who expect being monitored might hesitate to read about diseases, politics, or other topics.

[77]See Voss (2012), p. 17.

[78]Svantesson (2013b), p. 279.

[79]Kuner (2010b), p. 236.

risks ….and providers (that) are unwilling to undertake the risk of international litigation, they may very well refuse to provide services to individuals trying to connect from third countries (through their IP addresses); after all, this is a business policy frequently implemented in order to maximize international profits or to control international".[80]

Clear criteria about the applicable law will help to ensure both legal certainties for controllers and processors, as well as a better control for individuals concerned over their data.[81] However, achieving these core goals of the data protection reform may be questioned because of the difficulties faced to enforce the law that may undermine the credibility of the law and the respect thereof. Such concerns refer mainly to data controllers that have no assets or other links with the EU and might not be inclined to take account of compliance. In this respect, the powers and implementation strategies of data protection authorities are of utmost importance but they do not suffice to ensure compliance and enforcement as DPAs may impose fines but they lack themselves the means to enforce the law against data controllers and processors located outside the EU. However, the power of DPAs as provided in the GDPR, especially in Articles 57 and 83, may allow or oblige EU states to redraw territorial boundaries on the borderless Internet by blocking access to websites controlled by data controllers that do not comply with European law.[82]

3 The Loss of Control Over Data and the Consent in GDPR

Enhancing individuals' control over their data has been one of the Commission's starting points to propose a new legislative framework. As emphasized in the Communication launched by the Commission in 2012, many Europeans (72% of internet users in Europe) "worry that they are being asked for too much personal data online. They feel they are not in control of their data. They are not properly informed of what happens to their personal information, to whom it is transmitted and for what purposes. Often, they do not know how to exercise their rights online".[83]

[80] See de Hert, et al. (2013), p. 142.

[81] Albrecht (2015), p. 119, MEP and Rapporteur of the European Parliament for General Data Protection Regulation notes that "(t)he new EU law could bestow great benefits, particularly on users of Facebook and Google or smartphone owners, because up to now, they have in practice enjoyed hardly any protection".

[82] See Ryngaert (2015b), p. 187.

[83] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World—A European Data Protection Framework for the 21st Century, [COM (2012) 9 final—25.01.2012] with reference to the findings of Special Eurobarometer 359—Attitudes on Data Protection and Electronic Identity in the European Union, June 2011, p. 23.

3.1 Consent as Tool to Exercise Informational Self-Determination

A new formulation of consent and its components has been viewed as a main point of the Commission's proposal to enable individuals to enjoy effective control over their personal information in this new digital environment. Consent or, more accurately, the normative requirements around valid consent represent a key element of data protection. Consent is considered to be a substantial, or even indispensable, instrument as it safeguards the participation of the individual regarding his/her decision of the use of his/her data.[84] Put simply, provided that the individual is informed and he/she may express his/her free will and choice, consent guarantees primarily the right to articulate choices and/or exercise the right to informational self-determination.[85] Consent has been explicitly embedded in the EU Charter of Fundamental Rights as an essential aspect of the right to data protection.[86]

While in the American approach consent alone is considered as sufficient to protect individuals' interests regarding the use of their data, in the context of the European data protection framework, consent serves as a principal legal ground enabling data processing. Reliance on consent for legitimizing data processing operations was foreseen from the very beginning of the legislative process that ended up with the adoption of Directive 95/46/EC but it was not always clear what conditions had to be fulfilled for consent to be valid.[87] Consent was used in Directive 95/46/EC both as a general ground for lawfulness of processing (Article 7), as well as a specific ground in some specific contexts such as special categories of sensitive data (art. 8 par. 2 (a)) and transborder transfer (26 par.1 (a)). Considering that through consent individuals are waiving a fundamental right, its validity must be subject to rigorous requirements.

In the European regulatory context, consent is conceived as any indication of will, by which the data subject signifies his/her agreement to personal data relating to him/her being processed. The form of indication is not defined but consent has to

[84]Also in USA, consent has been for several decades the key principle of information privacy protection. See Schwartz and Solove (2009).

[85]With regard to informational self- determination see Simitis (2014), pp. 92 f. but also the contractual-property approach of privacy relies on interactions between individuals and data controllers to determine appropriate collection and use of data thus accommodating the significance of consent as a factor to generate and maintain appropriate norms for information privacy. See Mitrou (2009), pp. 471 ff.

[86]Article 8(2) of the Charter states that personal data can be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law". Two decades before (1981), Article 5§2 of the Convention 108 of the Council of Europe, stated that data processing may be carried out only based on free, specific, informed and unambiguous consent of the data subject or some other legitimate basis the law provides.

[87]Article 29 Working Party, Opinion 15/2011, p. 3.

be freely given, specific, informed,[88] unambiguous or explicit (in the case of sensitive data). These requirements apply whenever consent is sought, independently of whether this happens off-line or on-line. The European legislator, in 1995, aimed at balancing the rights of individuals by giving flexibility and avoiding technologically specific rules and/or rigid structures.[89] However, further clarification on the meaning of unambiguous consent was regarded as necessary especially as far as it concerns the default options, used mainly in online environments, which the user-data subject is required to modify to abnegate the processing. The Article 29 Working Party required that unambiguous consent, as a legislative standard, should encompass both "explicit consent", as well as consent "resulting from unambiguous actions". Transparency and accurate information of the data subjects are also crucial conditions for rendering the consent valid and enabling the data subjects to be in control of their data. Therefore, the necessary information should address the substantive aspects of processing that the consent is intended to legitimize, namely at least the elements listed in the law as minimum information requirements.[90] Major requirements refer to the visibility, accessibility and comprehensiveness of information provided.

Thus in most cases individuals appear to agree "gladly" to the use of their personal data. As they believe or feel that they must have access to services or benefits they submit easily and not adequately aware of risks both consent and information required. Even privacy-sensitive individuals appreciate the value these services provide and not rarely concede that most of the personal data collection is a price to pay in return for convenience and benefits provided. The so-called "just click submit" phenomenon is "caused by the simple concepts of (1) must, (2) rush, (3) trust".[91] As underlined by *E. Carolan,* a "user" finding herself in a controlled online environment, being offered a restricted, mostly binary choice of options and expecting gains from a rewarding online activity is keen and encouraged to provide consent.[92] Especially in cyberspace, consent to data processing is likely to turn into an empty, ritual process, thus resulting in a "fallacy"[93] for the consenting individual. The Commission underlined, in 2010, that in the "online environment - given the opacity of privacy policies - it is often more difficult for individuals to be aware of their rights and give informed consent",[94] thus rendering the risks for individuals

[88]One issue is that the definition in Article 2 (h) of the Directive 95/46/EC did not include a reference to the requirement of unambiguity.

[89]Article 29 Working Party, Opinion 15/2011, p. 37.

[90]Article 29 Working Party, Opinion 15/2011 p. 10, notes that, beyond these elements, information to be given will also depend on when, and the circumstances in which, consent has been requested.

[91]See Ciocchetti (2008), p. 7.

[92]See Carolan (2016), p. 472.

[93]See Schwartz (2000), p. 341 f.

[94]Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final.

apparently higher as consent represents probably the most critical factor of legitimizing online tracking and profiling.[95]

3.2 Normative Requirements and the "Fallacy" of Consent

One of the main goals of the data protection reform was to improve the clarity of information with regard to data processing aiming at enhancing awareness and strengthening the position of data subjects. The requirements around informed consent have become indeed clearer and stricter. The main features of valid consent (freely-given, specific, and informed) have not changed in essence. However, the addition of "unambiguous" in the respective definition (GDPR Article 4 (11)) reinforces the notion that only consent that is based on statements or actions that signify agreement can serve as a valid legal ground.[96] The GDPR requires that consent should be expressed by a statement or a clear affirmative action (Article 4. (11)) rejecting the—unfair and quite deceptive—opt-out approach, namely that the visit of a website or the mere use of a service constitutes a valid consent.[97] The European legislator accepted explicitly that the agreement to data processing may be given by electronic means ("including ticking a box"), but they clarified that silence, pre-ticked boxes or inactivity should not therefore constitute consent (Recital 32).

As Johnson states, the use of "opt-in" rather than "opt-out" goes hand in hand with transparency.[98] For consent to be informed, the data subject should be aware, at least, of the identity of the controller and the purposes of the processing for which the personal data are intended. When the processing has multiple purposes, consent should be given for all of them.[99] In the GDPR emphasis is placed also on the way request for consent is presented requiring an intelligible and easily accessible form,

[95]Skouma and Léonard (2015), p. 52.

[96]The—principally prohibited—processing of special categories of personal data remains subject to explicit consent of the data subject (Article 9 par. 2 (a) of the GDPR). Because of the practical difficulties with regard to the definition of explicit consent and the proof of obtaining the consent, several Member States adopted, under the regime of Directive 95/46/EC, the solution of "written consent" in relation to the processing of "sensitive data". See Van Alsenoy, et al. (2014), pp. 195–196.

[97]This provision is consistent with the conditions set forth in the e-Privacy Directive (Article 5 par. 3 of Directive 2002/58/EC as amended by Directive 2009/136/EC) with regard to "cookies' installation consent" that requests an affirmative action of the on-line user (through clicking on an "I accept" or "ok" box on a website banner or by use of another technique) before installing the tracking application.

[98]See Johnson (2009), p. 105.

[99]The GDPR provides for an exception with regard to the processing for scientific research purposes as it was accepted that is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. In this case, the data subject's consenting statement may refer to areas of specific research (Recital 33).

using clear and plain language (Article 7 par. 2). In case of a request by electronic means, this has to be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided (Recital 32). Data controllers have to adapt online consent requests and privacy policies, including notices and statements, to conform to the GDPR requirements and demonstrate compliance with them.[100] Another innovative element of the GDPR regarding consent concerns the burden of proof: Where processing is based on consent, the controller has to demonstrate that the data subject has consented to processing of his/her personal data (Article. 7 par. 1).

Making information available in an appropriate and comprehensive manner in combination with the consolidation of the opt-in as a regulatory choice will arguably improve consciousness of consenting actions and awareness of potential risks of processing. However, it remains disputable if this legislative array will ensure that "users would review, rationally assess and deliberatively respond to that information when exercising their consent entitlements".[101] The European Data Protection Supervisor questions, whether it would be fair to subject individuals to terms and conditions for online services that would require, on average, 25 days a year to read them.[102] Moreover, the cost of reading notices and privacy policies is perceived as too high while the benefit thereof is regarded as too low.[103] Researchers point also out the "notice fatigue" as individuals, being repeatedly exposed to privacy notices, tend to ignore them.[104]

Even if policies and notices satisfy legal obligations, it is highly questionable, if they can educate users or elicit privacy–protective behavior. Especially as far as it concerns the online environment, research has shown that users are concerned about their privacy and the use of their data but paradoxically[105] they do not behave correspondingly online.[106] In an online environment, consenting individuals mostly do not articulate their views and preferences as fully rational actors: both the online architecture and design, as well as the "sharing culture", especially in the context of online social media encourage self-disclosure and exposure.[107] In practice, businesses apply and users react to "take it or leave it" terms under the threat of

[100] As Skouma and Leonard note (Skouma and Léonard 2015, p. 55), companies deploying on-line tools on their websites will have to promote solutions explicitly supporting an "action" and change the content and level of detail in the majority of the privacy notices and statements, instead of the very general and all-inclusive language to describe on-line tracking activities, that they mostly use.

[101] See Carolan (2016), p. 468.

[102] European Data Protection Supervisor, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of Big Data, 2016, p. 13.

[103] See McDonald and Cranor (2008). See also Beales and Muris (2008), pp. 114–115.

[104] See Van Alsenoy et al. (2014), p. 189.

[105] It is the so called "privacy paradox" firstly defined as such by Barnes (2006). See also Gross and Acquisti (2005), p. 71ff.

[106] Groom and Calo (2011), p. 16ff. See also Young and Quan-Haase (2013), pp. 487 ff.

[107] See Hollenbaugh and Ferris (2014), pp. 50 ff.; Rouvroy (2016), p. 21, Rouvroy is referring to the "choice architecture" built by players whose interests do not coincide with those of the user; Carolan (2016), p. 472.

exclusion or denial of access to digital services and information. Individuals' decisions and choices are susceptible to various psychological biases and are indicated in a context that is mostly controlled and managed by data controllers who are interested in promoting users' positive response and consent and they can subtly or surreptitiously manipulate users' choices in the desired direction.[108]

Even if the cost of protection is limited, most, online users do not engage in protecting their privacy as they lack risk awareness, tend to underestimate the privacy dangers or simply do not read privacy policies before consenting, as reading privacy policies does not usually provide users with the comfort and confidence they expect.[109] Difficulties with information and consent are related also to a lack of interest or of understanding on the part of the users. Researchers highlight the shortcomings of information policies with regard to the ability of the average user to understand the function or potential of technology and its applications, regardless of the level of information supplied.[110] Critics are referring to the shared cognitive limitations of the majority of internet users questioning whether the GDPR requirements are likely to provide protection against "technology creep".[111]

3.3 The Technological Barriers of Free and Informed Consent

Moreover, doubt is also expressed whether, because of the features of the online environment, the consent approach is adequate in addressing the challenges posed in a digital era. People are not mostly aware or informed of the technological context of data use. Usually they are not able to understand and assess the worth and uses of their data, especially in the case of secondary, tertiary or x-ry uses, which is also because the categories of uses and recipients are routinely specified in the most general terms. Individuals need also to understand the consequences of consenting and processing in the long term. However, technology and applications are changing steadily and rapidly the, often radical, technological changes having a serious impact on the foreseeability of the future uses of data based on consent submitted.[112] The substantial increase in development of processing capabilities (storage, mining, crawling, matching profiles) may entirely transform the context and the conditions under which personal data are processed thus augmenting its informative value in an unpredictable way and increasing the potential adverse effects for individuals' rights.

[108] See Carolan (2016), p. 472. See also Li et al. (2011), p. 434 f.

[109] See Groom and Calo (2011), p. 9. See also Taddicken (2014), p. 248ff.

[110] Carolan (2016), p. 469.

[111] See van Alsenoy et al. (2014), p. 189.

[112] Noain Sanchez (2016), p. 134 f.

This is especially the case with Big Data analysis that involves per se the reuse of data. Individuals are consenting to the processing of their data with regard to specified purposes after being informed about them, as well as about the possible uses. The potential of Big Data for analyzing large multi-variable data sets with the view for uncovering valuable knowledge, through their compilation and identifying correlations, is putting not only the principles of purpose limitation but also the value and functionality of consent as legal ground under threat.[113] As emphasized by *Mantelero*, "since Big Data analytics are designed to extract hidden or unpredictable inferences and correlations from datasets, the description of these purposes is becoming more and more evanescent".[114] The complexity and the transformative use of Big Data does not offer to data subjects a real chance to understand potential future uses so as to make a conscious choice.

The privacy and data protection debate is also a debate about freedom of choice and its necessary preconditions. The parameters and the conditions of choices through consent within the given online reality are of crucial importance for evaluating the legislative solutions. The challenges associated with obtaining "meaningful consent" raise the question of whether the legislators of the GDPR by insisting on consent, as a cornerstone of data protection legislation, respond adequately to the needs set by an evolving technological and socio-economic reality or whether this perception of control over personal data remains, despite the vast array of mandatory requirements, merely an illusion and seems "(in)appropriate to rely on data subject consent as a means to legitimize data processing".[115]

Principally, reliance on consent reflects both the proprietary and the autonomy/dignity approach of informational privacy that dominate the American[116] and European regulatory policy respectively. The revitalization of the discussion, both in the Anglo-Saxon and the Continental legal area, regarding the significance of consent, as the unique or primary legal ground, has been associated also with "user self-empowerment" as a supplementary mean or even a substitute of strict rules and enhanced institutional enforcement mechanisms.[117] Equating consent with a perception of privacy as "private business", alienated and/or traded at will, would result to de-construction of (informational) privacy protective institutional instruments.

A part of legal theory rejects the notice and consent model, as they believe that such a response does not face the challenges of the techno-economic environment. While pointing to the cognitive limitations of data subjects and the complexity of data processing (both in terms of actors involved and the operations they perform)

[113] International Working Group on Data Protection in Telecommunications (2014), p. 3.

[114] See Mantelero (2014), p. 652.

[115] See Van Alsenoy et al. (2014), p. 190.

[116] Freedom of alienation is the paramount characteristic of liberal property rights. The argumentation relies on the choice of individuals: "if they (the consumers) choose not to (prefer dignity), that is evidence that they do not want it in the first place". See Kang and Buchner (2004), p. 231.

[117] See Mitrou (2009), p. 477 f.

that decrease individuals informed assessment and increase rational choice fallacies, critics of notice and choice approach underline the information power asymmetries, which cannot longer be counterbalanced by the user's self-determination.[118] In this respect, they question not only the efficacy[119] of this model but, moreover, its pro-privacy function as it is more likely in fact to facilitate rather than restrict the online processing activities[120] and "opens the door for abusive data practices disguised by a cloak of legitimacy".[121]

3.4 Consent and "By Default" Data Protection

However, the consent model should not be evaluated autonomously but as a part of the whole model of the Regulation. Submitting consent does not absolve data controllers involved from their responsibilities[122] and especially from compliance with the fundamental principles of data protection with focus on purpose limitation and proportionality principle. Consent, or more generally participation of the data subject to processing decisions that principally affect him/her,[123] is a way to exercise control over data processing and as such a necessary but not sufficient condition of effective protection.[124] Adopting a holistic approach the consent model has to be assessed and reinforced in the context of the regulatory complex that relies also on accountability, transparency, privacy by default and effective enforcement mechanisms that ensure that choices are lawfully formulated and respected.

One of the key elements of the current European data protection scheme is the synergy between law and technology. This approach is mirrored not only in the enhanced role of technology in the context of security and privacy by design provisions but also in the "privacy by default" requirement. Privacy by default, a new normative requirement addressed to data controllers, is of utmost importance for the protection of individuals as it may counterbalance the shortcomings of consent in an online environment and especially in that of social networks. However, one should not leave out of consideration that the perception of privacy, the level and quality of privacy expectations of a social network user are highly formulated also by the architecture of online communication and the "code".[125]

---

[118] Mantelero (2014), p. 652.

[119] See Calo (2013), p. 1027f.

[120] See Carolan (2016), p. 473.

[121] See Van Alsenoy et al. (2014), p. 192.

[122] See Noain Sanchez (2016), p. 136.

[123] This participation may take the form of exercising the rights granted by the Charter and the GDPR to the data subject as the right to delete/erasure, the right to be forgotten or the right to object.

[124] See Cranor (2012), p. 304ff.

[125] Piskopani and Mitrou (2009).

Default settings, as well as privacy settings, may be used, to guide or manipulate users' perceptions of their control over software configuration.[126] Therefore, the Article 29 Working Party stressed the importance of privacy-friendly default settings.[127]

In strict correlation with "privacy by design", "privacy by default" is introduced as an innovative principle in the GDPR. Data controllers are required to implement appropriate technical and organizational measures for ensuring that, by default, only personal data, which are necessary for each specific purpose of the processing, are processed. Privacy by default measures may apply to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Even if not explicitly mentioned in the text of the new provision, it is clear that the European legislator focused on social networks when he clarified that in particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. That means that a social network profile shall be "by default" non-publicly visible and it will be the user-data subject who defines actively her visibility. This change would strengthen individual's control, as all the applications should provide, by design, a level of protection that conforms to the requirements of the GDPR. Embedding privacy standards by default would avoid, for instance, the automatic index of personal information without users' explicit and conscious permission.[128]

4 New Digital Rights?

In the new European data protection framework, the reinforcement of informational self-determination has been sought also by the introduction of new rights these being the right to be forgotten and the right to data portability. In combination with the requirements with regard to valid consent, the Commission has proposed these new rights to improve individuals' ability to control their data in the online environment.[129] Indeed, the right to be forgotten is inspired by what is defined as control-based theories.[130] This right was aimed at offering individuals the

[126]See Rouvroy (2016), p. 7 who refers to the inertia that occurs when erasing our "digital footprint" demands an effort whose rewards are not certain or clear".

[127]Article 29 Working Group Opinion 5/2009 p. 7ff.

[128]See Noain Sanchez (2016), p. 130.

[129]See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World -A European Data Protection Framework for the 21st Century, (25.01.2012) COM (2012), p. 6.

[130]Expressed at first by Westin (1967), who defended the right of persons "to determine for themselves when, how, and to what extent information about them is communicated to others". An approach that has been adopted also on European level with the German Federal Constitutional Court affirming in 1983 (Census case) the right to informational self-determination.

opportunity to re-assess their digital presence and re-evaluate the use of their data for ever-changing purposes in dynamic contexts thus enabling them to take or regain control over the use of their data in the web[131] and restoring forgetfulness as a choice.[132]

4.1 The Right to Be Forgotten

The technology of the Web is not oriented at forgetting: on the contrary, its architecture and features facilitate retrieval and encourage dissemination of information. Because of technology, information lasts longer than the context and consequently it is available for analysis and use in totally different interpretative contexts. Enormous storage capacities and processing capabilities enables circulation of information, which may no longer be valid or accurate. Information stored and accessed on the Internet consists of fragments of people's lives that may be out of context, random, incomplete or wrong.[133] However, even correct information may be out of relevance or harmful. Easily accessible and permanent web records can "fridge the past". Search engines can bring to the surface the slightest piece of information, gathering all the pieces and offering various recomposed or heterogeneous portraits of a person.[134] Moreover, search results are often dominated by embarrassing information about individuals despite the time that has passed, because sensational information, widely disseminated and reproduced in the past, appears among the top results of a search.[135] Even if personal identity is dynamic, individuals are often confronted with the—often irremediable—consequences of static choices in a past time. At stake is the identity of a person and his/her ability to change and re-define or re-invent himself/herself.[136]

The idea of a "right to be forgotten" has been permeated through scholars, commentators and policy makers already since 2009,[137] but it was the regulatory proposal of the Commission (Proposal), presented in early 2012, that has initiated a scientific and public discussion on the (normative) content of such a right and its legal, technical and organizational implications for users, web actors, society and the legislator. Despite strong criticism regarding its applicability and its

[131] With regard to this right see Ausloos (2012), De Terwangne (2012).

[132] Or correcting the '(un)forgetfulness' deficiency of the web 'brain'. See Markou (2015), p. 204. Markou seems to share the assessment of Ambrose and Ausloos who casts doubts on the idea of permanently available information. See Ambrose and Ausloos (2013), p. 3.

[133] See Solove (2007), p. 32, 37, 49.

[134] De Terwangne (2012), p. 112.

[135] Also, Ambrose and Ausloos (2013) p. 3 that underline that in our age "you are what Google says you are".

[136] Mitrou and Karyda (2012), p. 9.

[137] Novotny and Spiekermann (2014), p. 1.

(conflicting) relation to freedom of expression[138] the Commission had emphasized the introduction of this right as one of the main elements of the new framework to be adopted with the ambition to preserve for individuals the possibility to co-define their digital identity. The Proposal had indeed produced an extraordinary amount of legal analysis in a relatively short time, although this right was far from new and its "precedent", the "right to oblivion", is rooted in many legal provisions at national and European level. In this perspective, the "right to be forgotten" indicated much more than a new formulation of the "traditional" right to oblivion. This new "digital right" was conceptualized in relation to certain Internet characteristics: wide—and usually uncontrolled—availability, accessibility, searchability, persistence, comprehensiveness, ubiquity, de–contextualization of information.[139]

The ruling of the CJEU in the case Google v. Spain has triggered off a more intense public and legal debate on the impact of the right to be forgotten. Characterized as "one of the ground-breaking judgments of the Information Age",[140] the judgment of the CJEU reflects and confirms the attempt of empowering individuals to manage their data and their respective rights, including digital forgetting.[141] This goal was ambitious and raised great expectations. However, the right to be forgotten was viewed merely as an extension, or clarification, of the already existing right to erasure as the emphasis is on deletion of data when there is no good reason to keep them. Commenting on the initial versions of the right to be forgotten, the European Data Protection Supervisor underlined that the autonomous right, formulated as a right to request the erasure and/or abstention from further dissemination, "goes together with a duty to make reasonable efforts to contact third parties so as to undo the effects of publication of data on the Internet".[142]

The Proposal raised complex questions not only in relation to the impact on the freedom of expression but also regarding the precise obligations of the data controller and the "downstream third parties".[143] Article 17 of the GDPR has faced many amendments from the original text of Commission's Proposal back in 2012 The right to object is expanded and Article 17 of GDPR requires the controller to erase all data pertaining to the objecting data subject if one of the grounds provided in paragraph 1 apply. Regarding digital forgetfulness the most important

[138]de Hert et al. (2013), p. 135.

[139]Moreover, it relates and applies to everyone and not just to convicted criminals who may object to the publication of the facts of their conviction once they have served their sentence.

[140]Rees and Heywood (2014), p. 577.

[141]See Iglezakis (2014), p. 2.

[142]See the comments of Hustinx (2014), p. 31. The former European Data Protection Supervisor points out that the CJEU in case *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* goes in the same direction at 73–74, 88, 93–94 and 98–99. This was the approach of the European Commission as expressed in the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union" COM (2010) 609 final, p. 8.

[143]Schwartz (2013), p. 1995.

requirements are found in Article 17 (2): As clarified in Recital 66 "to strengthen the right to be forgotten in the online environment, the right to erasure (is) extended in such a way that(w)here the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, (the controller), taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data". In this way, the European legislator tried to face a prevailing phenomenon in Internet networks called "bouncing", namely where a content published on some website is replicated (normally by users) on other websites.[144] The final version is a far more moderate text than the one initially proposed by the Commission.[145]

Enforcement is essential for the viability of the right to be forgotten.[146] The enforceability of the right to be forgotten has been questioned. The obligation to inform third parties about the request to erase the data is apparently an innovative element. To assess the extent and impact of this obligation one needs to consider that the data controller has to comply with taking account of available technology and the cost of implementation. The obligation of inform third parties about the erasure of data and their respective obligation is further restricted by the introduction of the criterion of proportionality. More specifically the GDPR requires that "reasonable" steps must be taken to achieve this goal, thus giving the data controller a wide range of maneuver to justify quite easily the failure to comply with this obligation. The possibility to refrain from this obligation has to be assessed also in the light of the accountability principle (Article 5 par. 2 GDPR): The data controller is ascribed a general responsibility to take all reasonable steps to implement compliance measures, including technical measures. Apart from this, the data controller should be able to demonstrate the adequacy and effectiveness of these measures or the unreasonableness thereof.

However, the obligation to take reasonable steps to inform other controllers does not in itself guarantee that these third parties are being informed and, moreover, (that) they are going to follow the request to erase those data.[147] Information of third controllers may also serve the purpose to enable them, including the initial publishers of the information, which could also perform processing for different purposes, to assess the decision by which the request to erasure was granted and, if needed, take steps to ensure that their rights and interests are duly considered. Third parties may have different, autonomous grounds for the lawfulness of their data

[144]Bartolini and Siry (2016), p. 229.

[145]It is interesting to note that data controllers are no more required to take "all reasonable steps" but simply "reasonable steps". Another significant change is that the expiration of the retention period consented is no more included in the legal grounds that may result to data erasure on request of the data subject while the requirement to abstain from further disseminating of erased data has also been deleted.

[146]Cuijpers et al. (2014), p. 11.

[147]Ibid, p. 11.

processing and consequently the erasure request may not be effective towards them even if it is for the original controller.[148] In these situations, the data controller might not know or be able to contact all third parties.

Another concern refers to the difficulty to define who the third-party controller, responsible for the (Internet) bounce, actually is, whether it is the manager of the service or its users. As far as it concerns the enforceability and the technical measures that could support it, the technical challenge lies (a) in tracking the "copies" of an item and all copies of information derived from the data item and (b) in effecting the erasure or removal of all exact or derived copies of the item Various authors have suggested that controllers should be required to implement technical solutions to allow the tracking of bounces.[149] The European Union Agency for Network and Information Security (ENISA) reported that the enforcement by "a purely technical and comprehensive solution is generally impossible in the open Internet".[150]

4.2 The Right to Data Portability

The enhanced control of data subjects over their personal data can be seen as the basis of the Proposal regarding Data Portability.[151] This control should enable the transfer of data "*from one electronic processing system to and into another, without being prevented from doing so by the controller*"'.[152] In general, the right to data portability consists of two aspects: the right of data subjects to receive data, which they have provided to a data controller[153] and the right to transmit those data to

[148]Bartolini and Siry (2016), p. 232.

[149]Bartolini and Siry (Ibid, p. 231) point out that tracking of bounces is already a reality in several cases as major Internet services tend not to replicate shared content from an external source, but rather to create a link to it and keep track of the link (this is also more sustainable in terms of storage and performance). In the case of erasure of the original resource, all links would be invalidated, thus actually achieving the erasure. They propose a combination of the "distributed model" (keeping track of all links that reference a given content) with the "centralized model" (every dissemination of the data is simply a reference to the original data; invalidating the originally published data makes every copy inaccessible) will enable the enforcement of the respective provision.

[150]It has to be clarified that this assessment of ENISA referred to the initial GDPR Proposal where the provision regarding the right to be forgotten was more ambitious. See ENISA (2012b), p. 2.

[151]With the introduction of this new right, the European legislator aimed at strengthening, furthermore, the control (of the data subject) over his or her own data. See Recital 68 of GDPR.

[152]Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data COM (2012) 11 final, p. 9.

[153]This aspect of the right to data portability consists in allowing the data subjects to get a copy of the data for their proper use. As noted by Cuijpers et al. (2014), p. 11. whether this copy can be used on another platform is left on the provider's discretion to invoke proprietary rights.

another controller from the controller to which the personal data have been provided (Article 20 par. 1 GDPR). The right to data portability could be viewed as an extension of an individual's right to access.[154] However, the core idea was to strengthen the individuals' right to move around their personal data from controller to controller, where personal information is compiled over time and could be transferred to another provider.[155] The right to obtain and transmit the data should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in the GDPR (Article 20 par. 3).

The Commission aimed to target social networks.[156] As mentioned in the Impact Assessment Report, the personal data that might be transferred under the right to data portability may be "*photos or a list of friends*" and "*contact information, calendar history, interpersonal communications exchanges and other kinds of personally or socially relevant data*".[157] The right to data portability was conceived as an "internet specific new right" but the scope of its application is not limited to social networks. The new right will apply to all controllers that process personal data by "automated means".[158] It would therefore address also other forms of web services, cloud computing etc.[159]

Despite the aim to foster the position of individuals in the online environment by increasing their choices with regard to online services, the scope of this right is quite limited. The right to data portability applies only when processing was originally based on the user's consent or alternatively on a contract.[160] A further precondition for the exercise of the rights afforded by Article 20 is that the data subject himself/herself has provided the data to the data controller thus the control rights provided by the GDPR are being significantly weaker when the relevant data processing relies on a legal basis other than consent. Concerns about this restriction are rooted also in the reality of digital era as "data are being harvested constantly, often without the data subject knowing, not to mention, actively participating".[161]

---

[154]This was the approach of the European Parliament that amended the Commission's Proposal by merging the right to data portability with the right of access.

[155]See de Hert and Papakonstantinou (2016), p. 189f. Also, Costa and Poullet (2012), p. 527.

[156]There was an explicit reference in the (initial) recital 55 ("from one application, such as a social network, to another one"), a reference that does not appear in the final text of Recital 68.

[157]Impact Assessment Report—Commission Staff Working Paper—Impact Assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data SEC (2012) 72 final, p. 28.

[158]The applicability to cases of offline data processing has been from the beginning of drafting excluded.

[159]Graef et al. (2013), p. 4.

[160]This restriction of the right has been criticized. See Cuijpers et al. (2014), p. 12. Further, the European Data Protection Supervisor suggested that the right of the data subject to data portability should be extended to all cases of processing of personal data [Opinion on the data protection reform package (2012), para. 151].

[161]Cuijpers et al. (2014), p. 12.

To enable data portability, data controllers will need to use "structured, commonly used and machine-readable[162] data formats" and templates.[163] All these distinct formatting requirements have to be satisfied, though, as underlined by *Swire and Lagos*, a structured format is not necessarily commonly used, and many standards are not widely adopted.[164] Furthermore, it is interesting to note that the text of the respective Recital (68) of the GDPR refers also to "interoperable format", a reference that is not included in the text of Article 20. GDPR has left to the service providers themselves to define and agree upon standard, "commonly used" formats. Data controllers should be encouraged to develop interoperable formats that enable data portability (Recital 68). Although interoperability is not a mandatory requirement, in practice, without it the right to data portability would lose most of its sense, as the data would not freely circulate between different networks and IT systems.[165]

The new provision mandates the data controller not to hinder the exercise of the right to data portability, namely not to technically block the transfer. As mentioned, the inability of users to move their data between social networks has been a distortion that European regulator intended to address.[166] Yet, the final text of the GDPR refers to the right of individuals to "have the personal data transmitted directly from one controller to another, where technically feasible" (Article 20 par. 2), while the data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible (Recital 68). This possibility to escape from direct transfer may result to the obligation being only applied if the required technical measures/context already exist. In this perspective, the balance struck in Article 20 may undermine both goals of the legislative intervention, namely facilitating interoperability, and thus competition, and enhancing individuals' control over their data.[167]

---

[162]Machine-readable data is data (or metadata), which is in a format that can be understood by a computer. There are two types; human-readable data that is marked up so that it can also be read by machines (microformats, RDFa) or data file formats intended principally for processing by machines (RDF, XML, JSON).

[163]The use of these terms has been criticized and some authors expressed their concerns regarding the scope of application of this rule. See Graef et al. (2013), p. 4. See also Engels (2016), p. 150. It is the author's opinion that these terms have to be principally interpreted with respect to the—current 'state of the art".

[164]Swire and Lagos (2013), p. 346.

[165]Article 29 Working Party, Opinion 8/2014, p. 20.

[166]As noted by de Hert and Papakonstantinou (2016), p. 189 "internet social networks operate for the time-being as closed gardens for their users", while Graef et al. (2013), p. 6 underline that social network providers do not allow third-party sites to directly acquire the user's information resulting to a kind of lock-in, as in practice, users thus have to manually re-enter their profile information, photos, videos and other information in the new platform if they want to switch from one social network to another.

[167]de Hert and Papakonstantinou (2016), p. 190 note that data portability is expected to affect in many and important ways the internet social networks market.

5 Protecting Personal Data on the Internet: A Herculean or a Sisyphean Task? – A Provisional Conclusion

Because of its omnibus and comprehensive nature the GDPR is expected to "affect the way Europeans work and live together"[168] as—in combination with the Data Protection Directive(2016/680/EU[169])—it regulates any data processing in Europe. Data protection has taken a central stage in the political debate and has become relevant to all areas of life and economy.[170]

Are the new rules designed to guarantee a continued effectiveness of the—fundamental—right to the protection of personal data in an ever-advancing information society? The discussion on the new data protection framework was based on the premise that the protection level as embedded in Directive 95/46/EC and the respective jurisprudence had to be maintained. The aim of the reform was to improve the "data protection acquis" by evolving and modernizing existing rules so that individuals are put in control of their data in the context of technological developments and globalization of services and information flows.[171]

The GDPR has maintained, in principle, the regulatory scheme: Controllers-processors, data subjects and supervisory data protection authorities. The new data protection framework relies on the interplay of the rights of the data subjects and the obligations of the actors involved in data processing: the data controller and the data processor.[172] The rules are addressed to the "controller" as the main responsible and accountable figure to assess and balance the competing rights and interests and comply with—still complex—obligations while the GDPR adopts a repartition of obligations between controllers and processors also by imposing directly explicit obligations on processors.[173] We should note however that in current processing

[168]Ibid p. 180.

[169]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA".

[170]Albrecht (2015), p. 129.

[171]Koops (2014), p. 250. See also Irion and Luchetta (2013), p. 63.

[172]The distinction seems to be more pragmatic and based on a case-by-case evaluation. See Cuijpers, et al. (2014), p. 6.

[173]While under Directive 95/46/EC the processor is referred to solely in the provisions concerning definitions and data security measures, the GDPR establishes directly processor-specific obligations or "joint obligations" that refer both to controllers and processors (privacy by design, privacy impact assessment). This will enhance the position of data subjects and is positive regarding liability and accountability.

environment, gradually dominated by cloud computing[174] and big data analysis, this distinction is not easy.[175]

Data subjects may exercise their right to informational self-determination through informed consent and the rights provided in Chapter III of the GDPR, in an environment, though, of information power asymmetries. Individuals are equipped with new rights such as the right to be forgotten and the right to data portability, the situations where individuals can meaningfully use them being, yet, quite limited. As far as it concerns the third pillar of the data protection model, the data protection authorities, the GDPR (Articles 51–59) provides for strengthened safeguards for their independence and strong enforcement powers.[176] Data Protection Authorities are, indeed, endowed and, at the same time, overflowed with multiple tasks and duties, but it remains to be seen if these powers and tasks are internet adequate and future-proof.

The data protection reform has been criticized for being stuck in the 1970s roots, namely the "traditional regulatory model" that served as an inspiration for Directive 95/46/EC.[177] Indeed, with the exception of the addition of some new notions and respective legal imperatives, such as pseudonymization or privacy by design, the European legislator has extended past wordings to current and future problems. The GDPR relies in several of its articles on the "available technology", meaning probably the "state of the art", or the use of "new technologies" to define the scope of obligations imposed on data controllers.[178] Yet the European legislator has avoided specific "technical" terms. It is noteworthy that the Regulation does not contain any reference to the word "cloud", much less any cloud specific provision per se.[179]

[174]Concerns have been expressed regarding the difficulty in determining the roles of controllers and processors particularly in the context of cloud computing.

[175]What is relevant is the factual influence on data processing. Furthermore, and especially in the context of cloud computing, processors are of significant importance. See Article 29 Working Party, Opinion 1/2010 and Opinion 5/2012.

[176]The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. (Recital 117). In comparison to Directive 95/46/EC the monitoring and compliance ensuring powers are tightened while the cooperation between DPAs has also been improved.

[177]Blume (2014), p. 2, criticizes the choice to insist on imposing obligation to controllers instead of giving a leading role to data subjects while other authors indicate that the GDPR is based on false assumptions or "fallacies". See Koops (2014), p. 256.

[178]Such as the obligation provided in Article 17(2) with regard to the right to be forgotten or the obligation to carry out a data protection impact assessment (Article. 35 (1)).

[179]Criticism has also been expressed with regard to the adequacy of location focused approach of the GDPR to solve the complexities in applying the transborder flow rules in operations of Internet enabled technologies such as cloud computing and the respective cloud transactions. Nwankwo (2014), p. 36. This criticism underestimates, however, the impact of the provisions concerning the territorial scope on the cloud computing relationships and transactions.

The criticism of data protection regulation echoes also the concern that a single general framework is inadequate for addressing the challenges posed by intensive, ubiquitous and distributed information processing.[180] Refraining from technology-specific terminology and provisions seems to be a conscious choice to be attributed to the "technological neutrality approach".[181] Emphasis is put not on the technology used for data processing but on the effects to be regulated, on the risks and impacts on fundamental rights that are to be faced. Technology neutrality concept emerged as a regulatory principle, a canon, where states are proceeded to promulgate technology impartiality.[182] The technological neutrality of law requires that the latter generate the same effects irrespective of the technological environment where these norms apply,[183] a policy that presupposes, however, that the legislators have in mind and have considered both the issues posed by current technologies and the future trends.

Although the difficulties and complexities of digital environments have been considered by the designing of the data protection regulatory strategy, the regulatory choice of the GDPR consists more of what is perceived as technology—independent legislation. Technology independent rules are regarded as a means to stand firm with technological turbulences.[184] Technology, obviously, develops quicker than the law. Even within the 5-year period between the Commission's Proposal and the adoption of the GDPR, technology, or at least the spectrum and the extent of its uses, has changed substantially: mobile apps, Internet of Things or Internet of Everything, cyber-physical systems, etc.

Adopting technology-neutral provisions seems to be the path to deal with the unforeseeability of technological developments and consequently ensure that the law is sustainable to respond successfully to such—unpredictable—developments over a sufficiently long period. The GDPR has not adopted a sunset clause, which would provide by default that the law will expire after a certain period, unless it will be extended. Article 97 of GDPR provides for the competence of the Commission to submit by 25 May 2020, and every four years thereafter, a report to the European Parliament and to the Council. The Commission shall, if necessary, submit

[180] A main concern is that the framework applies linear protection concepts to a world of ubiquitous and distributed personal data processing. Irion and Luchetta (2013), p. 53.

[181] With the GDPR, the European legislator adheres explicitly to the technological neutrality approach as Recital 15 cites that the protection of natural persons should be technologically neutral and should not depend on the techniques used.

[182] As stated in a Commission's Communication, in 1999, technological neutrality means that "legislation should define the objectives to be achieved, and should neither impose, nor discriminate in favor of, the use of a particular type of technology to achieve those objectives". Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Towards a new Framework for Electronic Communications Infrastructure and Associated Services: the 1999 Communications Review COM (1999) 539 final, p. 14.

[183] Hildebrandt and Tielemans (2013), p. 510.

[184] Koops (2006), pp. 1., 21.

appropriate proposals to amend this Regulation, in particular, with consideration of new developments in information technology and in the light of the state of progress of the Information Society. Principally the rules and principles of the GDPR, such as the notion of identifiability of the data subject, are flexible enough to cover future technological changes and confer lasting protection. Moreover, one should not ignore the risk that the vagueness that characterizes some terms and notions may, over time, result in large divergences in interpretation of the law and -consequently- legal uncertainty.[185]

The EU data protection reform does not constitute a revolution[186] and was never intended to be one. The efforts to reform EU data protection framework have shown that the aim was principally to secure high standards of data protection which are more harmonized and appropriate for the internet age, while retaining the fundamentally worthwhile principles of the Data Protection Directive.[187] Despite the criticism, the Regulation is an important improvement in the sustaining and maturing of data protection law[188]: Innovative regulatory elements, such as privacy by design or data protection impact assessments requirements, may serve to respond also proactively to unforeseen technological challenges and anticipate and/or mitigate the respective risks. For the Data Protection Authorities not to remain "paper tigers" trapped, into their multiple roles and tasks,[189] they need to strike a fine balance between imposing the strict sanctions provided in the GDPR, encouraging individuals to change their perception around the fancy online tools and world and sensitizing data controllers about their accountability and the importance of implementing the law.[190] *A Herculean but - hopefully - not a Sisyphean task. . ..*

References

Albrecht J (2015) Hands off our data. The Greens-EFA, p 191
Ali R (2009) Technological neutrality. Lex Electronica 14(2)
Ambrose ML, Ausloos J (2013) The right to be forgotten across the pond. J Inform Policy 3:1–23
Andrejevic M (2002) The work of watching one another: Lateral surveillance, risk, and governance. Surveillance & Society" People Watching People"
Article 29 Data Protection Working Party (2002) Working Document on determining the international application of EU data protection law to personal data processing on the Internet by

[185] Ali (2009), p. 9, points out that technological neutrality of the law may result in regulations whose meaning is so vague that its application to the technology is often a matter of guesswork.

[186] Although, as noted by Kiss and Szoke (2014), p. 328, the unprecedented lobby activities of different organizations show that many organizations also consider the proposed changes as a revolution in data protection legislation.

[187] See the assessment of Albrecht (2015), p. 137.

[188] Blume (2014), p. 5.

[189] About the risk of the multitude of supervisory and enforcement tasks see Mitrou (1993), p. 273.

[190] Skouma and Léonard (2015), p. 56.

non-EU based web sites (WP 56). Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data. Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party (2009) Opinion 5/2009 on online social networking. Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

Article 29 Data Protection Working Party (2010a) Opinion 1/2010 on the concepts of "controller' and "processor". Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party (2010b) Opinion 8/2010 on applicable law. Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party (2011) Opinion 15/2011 on the definition of consent. Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party (2012) Opinion 5/2012 on Cloud Computing. Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party (2014a) Opinion 5/2014 on anonymization techniques. Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party (2014b) Opinion 8/2014 on the Recent Developments on the Internet of Things. Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29 Data Protection Working Party (2015) Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain. Available via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Ausloos J (2012) The right to be forgotten – Worth remembering? Computer Law & Security Review 2012. Available via SSRN: http://ssrn.com/abstract=1970392

Baño Fos JM (2014) An Individual's Quest to Always Be Remembered: A Critical Approach to the Right to Be Forgotten in the European Data Protection Directive. Available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2395296

Barnes S (2006) A privacy paradox: Social networking in the United States. First Monday, 11(9). Available via www.firstmonday.org

Bartolini C, Siry L (2016) The right to be forgotten in the light of the consent of the data subject. Comput Law Secur Rev 32(2):218–237

Beales JH, III, Muris TJ (2008) Choice or consequences: protecting privacy in commercial information. Univ Chicago Law Rev 75(1). Available via: http://chicagounbound.uchicago.edu/uclrev/vol75/iss1/6

Blackman J (2009) Omniveillance, google, privacy in public and the right to your digital identity: a tort for recording and disseminating an individual's image over the internet. Santa Clara Law Rev 49:313 ff

Blume P (2014) The myths pertaining to the proposed General Data Protection Regulation. International Data Privacy Law, ipu017

Borgesius FJZ (2016) Singling out people without knowing their names–behavioural targeting, pseudonymous data, and the new data protection regulation. Comput Law Secur Rev *32* (2):256–271

Calo R (2013) Digital Market Manipulation. 82 George Washington Law Review Research Paper No. 2013-27. pp 995–1051. Available via SSRN: https://ssrn.com/abstract=2309703 or doi:10.2139/ssrn.2309703

Carolan E (2016) The continuing problems with online consent under the EU's emerging data protection principles. Comput Law Secur Rev 32(3):462–473
Castelluccia C, Druschel P, Hübner S, Pasic A, Preneel B, Tschofenig H (2011) Privacy, accountability and Trust-Challenges and opportunities. ENISA. [Online]. Available via http://www.enisa.europa.eu
Ciocchetti C (2008) Just click submit: the collection, dissemination and tagging of personally identifying information. Vanderbilt J Entertain Technol Law 10(Spring):553–642
Costa L, Poullet Y (2012) Privacy and the regulation of 2012. Comput Law Secur Rev 28 (3):254–262
Cranor LF (2012) Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. J Telecomm High Technol Law 10:273–308
Cuijpers C, Purtova N, Kosta E (2014) Data protection reform and the internet: the draft data protection regulation. Forthcoming In: Savin A, Trzaskowski J (eds) Research handbook on EU internet law. Edward Elgar 2014 Tilburg Law School Research Paper No. 03/2014. Available at SSRN: https://ssrn.com/abstract=2373683
Dammann U, Simitis S (1996) EG-Datenschutzrichtlinie, Kommentar, Nomos Verlag, p 341
de Hert P, Papakonstantinou V, Wright D, Gutwirth S (2013) The proposed Regulation and the construction of a principles-driven system for individual data protection. Innov Eur J Soc Sci Res 26(1-2):133–144
de Hert P, Papakonstantinou V (2016) The new general data protection regulation: still a sound system for the protection of individuals? Comput Law Secur Rev (2):179–194
de Terwangne C, Louveaux S (1997) Data protection and online networks. Comput Law Secur Rev 13(4):234–246
de Terwangne C (2012) Internet privacy and the right to be forgotten/right to oblivion. In: VII international conference on internet, law & politics. Net neutrality and other challenges for the future of the internet. IDP. Revista de Internet, Derecho y Política. No.13, pp 109–121
Engels B (2016) Data Portability and Online Platforms - The Effects on Competition [Extended Abstract]. In: 29th Bled eConference- Digital Economy, Bled, Slovenia, 19–22 June, 2016
European Data Protection Supervisor (2016) Opinion 8/2016 on coherent enforcement of fundamental rights in the age of Big Data, 2016
European Network and Information Security Agency (ENISA) (2012a) Privacy considerations of online behavioral tracking. Available via http://www.enisa.europa.eu/
European Network and Information Security Agency (ENISA) (2012b) 'The right to be forgotten – between expectations and practice'. Available via http://www.enisa.europa.eu/
Froomkin MA (2000) The death of privacy? Stanford Law Rev 52:1461–1543
Gerber D (1984) Beyond balancing – international law restrains on the reach of national laws. Yale J Int Law 10:190
Goldsmith J, Wu T (2008) Who controls the internet? illusions of a borderless world. Oxford University Press, Oxford
Graef I,Verschakelen J, Valcke P (2013) Putting the right to data portability into a competition law perspective. J High Sch Econ Annual Rev pp 53–63. Available via https://ssrn.com/abstract=2416537
Gritzalis D, Kandias M, Stavrou V, Mitrou L (2014) The social media in the history of information: privacy violations and security mechanisms. In: Proceedings of the History of Information Conference, pp 283–310
Groom V, Calo R (2011) Reversing the Privacy Paradox: An Experimental Study (September 25, 2011). TPRC 2011. Available via https://ssrn.com/abstract=1993125
Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005. pp 71–80
Hildebrandt M (2009) Profiling and AmI. In: Rannenberg K, Royer D, Deuker A (eds) The Future of Identity in the Information Society. Springer, Berlin, Heidelberg, pp 273–310
Hildebrandt M, Tielemans L (2013) Data protection by design and technology neutral law. Comput Law Secur Rev 29(5):509–521

Hollenbaugh EE, Ferris AL (2014) Facebook self-disclosure: examining the role of traits, social cohesion, and motives. Comput Hum Behav 30:50–58

Hotaling A (2008) Protecting personally identifiable information on the internet: notice and consent in the age of behavioral targeting. Commlaw Conspec 16:529–565

Hustinx P EDPS (2014) EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation

Iglezakis I, Mitrou L, Jougleux P, Synodinou T (2016) The legal regulation of cyberattacks. Kluwer, Netherlands, p 229

Iglezakis I (2014) The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet? Available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323

International Working Group on Data Protection in Telecommunications (2014) Working Paper on Big Data and Privacy -Privacy principles under pressure in the age of Big Data analytics. Available via https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/

Irion K, Luchetta G (2013) Online personal data processing and EU data protection reform. In: CEPS Task Force Report of the CEPS Digital Forum. Available via https://www.ivir.nl/publicaties/download/TFR_Data_Protection.pdf

Johnson D (2009) Computer ethics. Pearson, Upper Saddle River, p 216

Kandias M, Galbogini K, Mitrou L, Gritzalis D (2013) Insiders trapped in the mirror reveal themselves in social media. In: International Conference on Network and System Security, Springer Berlin Heidelberg, pp 220–235

Kang J, Buchner B (2004) Privacy in Atlantis. Harv J Law Technol 18(1) Fall 2004. Available via https://ssrn.com/abstract=626942

Kiss A, Szoke GL (2014) Evolution or revolution? Steps forward to a new generation of data protection regulation. In: Gutwirth S, Leenes R, de Hert P (eds) Reforming European data protection law. Springer, Netherlands, pp 311–331

Koops BJ (2014) The trouble with European data protection law. Int Data Priv Law 4(4):250–261

Koops BJ (2006) Should ICT regulation be technology-neutral? In: Koops B-J, Lips M, Prins C, Schellekens M (eds) Starting points for ICT regulation. Deconstructing prevalent policy one-liners, it & law series. T.M.C. Asser Press, The Hague, pp 77–108. Available via https://ssrn.com/abstract=918746

Kosta E, Kalloniatis C, Mitrou L, Gritzalis S (2010) Data protection issuespertaining to social networking under EU law, transforming government: people. Process Policy 4(2):193–201

Kotschy W (2014) The proposal for a new general data protection regulation—problems solved? Int Data Priv Law 4(4):274–281

Kuner C (2010a) Internet jurisdiction and data protection law: an international legal analysis (Part 2). Int J Law Inform Technol 18:227. Available via SSRN: https://ssrn.com/abstract=1689495

Kuner C (2010b) Data protection law and international jurisdiction on the internet (Part 1). Int J Law Inform Technol 18:176–193

Kuczerawy A (2010) Facebook and its EU users – Applicability of the EU data protection law to US based SNS. In: Bezzi M et al (eds) Privacy and identity. IFIP AICT, Vol 320, pp 75–85

Li H, Sarathy R, Xu H (2011) The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decis Support Syst 51(3):434–445

Mantelero A (2014) The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. Comput Law Secur Rev 30 (6):643–660

Markou C (2015) The right to be forgotten: ten reasons why it should be forgotten. In: Gutwirth S et al (eds) Reforming European data protection law. Springer, Netherlands, pp 203–226

McDonald AM, Cranor LF (2008) Cost of reading privacy policies. J Law Policy Inform Soc 4:540–565

Milanovic M (2015) Human rights treaties and foreign surveillance: privacy in the digital age. Harv Int Law J 56:81–146

Mitrou L, Karyda M (2012) EU's data protection reform and the right to be forgotten: a legal response to a technological challenge?. Paper presented at the 5th International Conference of Information Law and Ethics, Corfu-Greece, 29–30 June 2012. Available via https://ssrn.com/abstract=2165245

Mitrou L (2009) The commodification of the individual in the internet era: informational self-determination or "Self-alienation"? In: Proceedings of 8th international conference of computer ethics philosophical enquiry - CEPE 2009, pp 466–484

Mitrou E (1993) Die Entwicklung der institutionellen Kontrolle des Datenschutzes: Kontrollmodelle und Kontrollinstanzen in der Bundesrepublik und in Frankreich. Nomos Verlag, p 296

Nevrla J (2010) Voluntary surveillance: privacy, identity and the rise of social panopticism in the twenty-first century. In: Commentary - The UNH Journal of Communication Special Issue, pp 5–13

Noain Sanchez A (2016) 'Privacy by default 'and active 'informed consent by layers: essential measures to protect ICT users' privacy. J Inform Commun Ethics Soc 14(2):124–138

Novotny A, Spiekermann S (2014) Oblivion on the web: an inquiry of user needs and technologies. Available via http://epub.wu.ac.at/4112/

Nwankwo IS (2014) Missing links in the proposed EU data protection regulation and cloud computing scenarios: a brief overview. J Intellect Prop Inform Technol E-Comm Law 5 (1):32–38

Piskopani AM, Mitrou L (2009) Facebook: reconstructing communication and decostructing privacy law? MCIS 2009 Proceedings. Available via http://aisel.aisnet.org/mcis2009/70

Rees C, Heywood D (2014) The "right to be forgotten" or the "principle that has been remembered". Comput Law Secur Rev 30(5):574–578

Robinson N, Graux H, Botterman M, Valeri L (2009) Review of EU data protection directive. Available via http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf

Ross P (2001) Congress fears European privacy standards. CNET News (8 March 2001). Available via http://news.cnet.com/2100-1023-253826.html

Rouvroy A (2016) Of Data and Men- Fundamental Rights and Freedoms in a World of Big Data, Report – Council of Europe - Directorate General of Human Rights and Rule of Law. Available via http://www.coe.int/en/web/data-protection/reports-studies-and-opinions

Rubinstein IS (2012) Big Data: The End of Privacy or a New Beginning? New York University Public Law and Legal Theory Working Papers. Paper 357

Ryngaert C (2015a) Symposium issue on extraterritoriality and EU data protection – Editorial. Int Data Priv Law 5(4). Available via https://academic.oup.com/idpl/article/5/4/221/2404465/Symposium-issue-on-extraterritoriality-and-EU-data

Ryngaert C (2015b) Jurisdiction in international law. Oxford University Press, Oxford, p 272

Schultz T (2008) Carving up the internet: jurisdiction, legal orders, and the private/public international law interface'. Eur J Int Law 19(4):799–839

Schwartz P, Solove D (2009) Notice and Choice: Implications for Digital Marketing to Youth prepared for the Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children (June 29–30, 2009), Available via http://digitalads.org/documents/Schwartz_Solove_Notice_Choice_NPLAN_BMSG_memo.pdf

Schwartz PM (2013) The EU-U.S. privacy collision: a turn to institutions and procedures. Harv Law Rev 126:1966; UC Berkeley Public Law Research Paper No. 2290261. Available via https://ssrn.com/abstract=2290261

Schwartz PM (2000) Privacy, participation and cyberspace – an American perspective. In: Simon D, Weiss P (Hrsg.) Zur Autonomie des Individuums – Liber Amicorum Spiros Simitis. Nomos Verlag, Baden-Baden, pp 337–352

Simitis S (1999) Die Erosion des Datenschutzes. Von der Abstumpfung deralten Regelungen und den Schwierigkeiten, neue Instrumente zu entwickeln. In: Bettina Sokol (Hrsg.): Neue Instrumente im Datenschutz. Wuppertal, pp 5–40

Simitis S (2014) Bundesdatenschutzgesetz – Kommentar. Nomos Verlag, pp 2072
Skouma G, Léonard L (2015) On-line behavioral tracking: what may change after the legal reform on personal data protection. In: Gutwirth S et al (eds) Reforming European data protection law. Springer, Netherlands, pp 35–60
Sobkowicz P, Kaschesky M, Bouchard G (2012) Opinion mining in social media: modeling, simulating, and forecasting political opinions in the web. Gov Inform Q 29(4):470–479
Solove D (2007) The future of reputation – Gossip, Rumor and privacy on the internet. Yale University Press
Svantesson DJB (2007) Private international law and the internet. Kluwer Law International, Netherlands, p 464
Svantesson DJB (2013a) The extraterritoriality of EU data privacy law - its theoretical justification and its practical effect on U.S. businesses. Stanford J Int Law 50(1):53–117
Svantesson DJB (2013b) A "layered approach" to the extraterritoriality of data privacy laws. Int Data Priv Law 3(4):278–286
Swire P, Lagos Y (2013) Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique. Maryl Law Rev 72(2):335–380
Taddicken M (2014) The "Privacy Paradox" in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. J Comput Mediat Comm 19:248–273
Taylor M (2015) The EU's human rights obligations in relation to its data protection laws with extraterritorial effect. Int Data Priv Law 5(4):246–256
Tokunaga R (2011) Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. Comput Hum Behav 27:705–713
van Alsenoy B, Kosta E, Dumortier J (2014) Privacy notices versus informational self-determination: minding the gap. Int Rev Law Comput Technol 28(2):185–203
van Eecke P, Truyens M (2010) Privacy and social networks. Comput Law Secur Rev 26:535–546
Voss WG (2012) Preparing for the proposed EU general data protection regulation: with or without amendments. Bus Law Today 1
Warso Z (2013) There's more to it than data protection fundamental rights, privacy and the personal/household exemption in the digital age. Comput Law Secur Rev (29):49, 1–500
Westin A (1967) Privacy and freedom. Athenaeum, New York, p 487
Whitaker R (1999) The end of privacy: how total surveillance in becoming a reality. New Press, p 195
Wong R, Savirimuthu J (2007) All or nothing: this is the question-the application of article 3 (2) Data Protection Directive 95/46/EC to the Internet. J Marshall J Comput Inform Law 25:241–266
Xanthoulis N (2013) Negotiating the EU data protection reform: reflections on the household exemption. In: International Conference on e-Democracy Springer International Publishing, pp 135–152
Young AL, Quan-Haase A (2013) Privacy protection strategies on facebook: the internet privacy paradox revisited. Inform Commun Soc 16(4):479–500

Chapter 3
Developing a Right to be Forgotten

Andres Guadamuz

Abstract For many years, various authors have postulated the possible existence of a right to be forgotten. The Court of Justice of the European Union in the landmark ruling in Google Spain v Costeja González (C 131/12) enacted a limited version of the right. Now the General Data Protection Rules includes a "right to erasure". This article looks at the evolution of the right, paying special attention to its future.

1 Introduction

Imagine being subjected to continuous, relentless online harassment, and not being able to do anything about it from a legal perspective. This is what has been happening for the last couple of years to American journalist Dune Lawrence, who has been subjected to a vicious series of online attacks.[1] As a journalist covering financial markets, she wrote several articles few years ago about an investment firm, and the owner initiated an online defamation campaign against her and other targets. He posted images of her to his website and called her a racist, a fraud, incompetent and dumb, among many other insults. Remarkably, these images quickly rose to the top of Google's image search results for her name, and are still there at the time of writing, making it easy for anyone to find the defamatory comments about her. In fact, these results still display highly although the creator of the site has already lost a defamation case, has been charged with fraud, and is in the process of defending yet another defamation case.

One of the great advantages—and disadvantages—of the Internet is that it lets anyone easily publish anything they want. If someone publishes defamatory comments about you, or personal information or explicit photos of you, what can you do? Suing the host of the potentially illegal content is difficult, expensive, and it

[1] Lawrence (2016).

A. Guadamuz (✉)
Freeman Centre, University of Sussex, Brighton, UK
e-mail: a.guadamuz@sussex.ac.uk

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_3

may even be impossible if they are in another country or are protected by strong free speech laws. Unfortunately for Dune Lawrence, this is precisely the case in the United States, where publishers are protected by strong laws that make them almost immune from liability when publishing potentially defamatory content.[2]

Citizens of the European Union that find themselves in a similar situation to that of Dune Lawrence now have a legal recourse in trying to fight derogatory comments online, and this is the so-called "right to be forgotten" (RTBF). This allows European citizens to request that search engines such as Google remove entries from their search results that lead to content that is irrelevant, excessive, or unnecessarily defamatory.

This chapter looks at the rise of the right to be forgotten, from the earliest proposals that gave rise to it, to the most recent iteration of the right contained in recent regulations. It also analyses the debate that has erupted by the implementation of the right, and it finishes asking whether it is a valid addition to defend information self-determination, or if it infringes on freedom of speech and the public's right to know.

2 Precursors to the Right to be Forgotten

The so called "right to be forgotten" (RTBF) relies on the idea that one has the legal right to remove information about oneself that is accessible online and that is potentially damaging to one's enjoyment of a private life, or more accurately, to have it de-listed from search engine results.[3] Before we go into the details of how the concept was enacted, it is important to review how it got started.

While there are various legal predecessors, arguably the conceptual origin of the right to be forgotten can be found in ideas of self-governance and self-determination found in Niklas Luhmann's work, where he proposes systems that should be self-organised, with legal and social regimes where humans interact is no exception.[4] These concepts eventually were implemented into law in Germany for the first time in what is known as information self-determination,[5] which is a space where the individual "is shielded from interferences in personal matters, thus creating a sphere in which he or she can feel safe from any interference."[6] It is important to note that this concept does not correspond specifically to privacy, the right to a private life being seen as protecting a related, but different type of interests.

[2] Ardia (2010).

[3] As implemented by the Google Spain decision, see infra footnote 23.

[4] Luhmann (1995), Sørensen and Triantafillou (2016).

[5] Hornung and Schnabel (2009).

[6] Ibid.

Concerning privacy, Europe has a robust system to ensure the protection of this right. Article 8 of the European Convention of Human Rights (ECHR) clearly specifies that "everyone has the right to respect for his private and family life, his home and his correspondence." This robust right has been adopted into the European legal system. However, information self-determination is not the same as privacy, although they may interact from time to time. Information self-determination is protected through the data protection regime enacted with the 1995 European Data Protection Directive (DPD).[7] The Data Protection Directive has the main objective of safeguarding the rights of an identified or identifiable natural person (known as a data subject), by setting a number principles and situations in which any information relating to the data subject (known as personal data) can be processed lawfully. Any legal entity that can determine the purpose and means of controlling a subject's personal data is known as a data controller.[8]

The existing Data Protection Directive regime received in 2016 an update in the shape of the General Data Protection Regulation (GDPR). This text updates most of the existing provisions contained in the Data Protection Directive to better accommodate data protection to the digital era. Specifically, the GDPR contains specific provisions regarding the right to be forgotten, which we will be covered in more detail in following sections.

The right to privacy and the data protection regime do not exist in a vacuum: a person's right to enjoy a private life can often clash with other rights, particularly the right to freedom of expression present in Article 10 of the European Convention on Human Rights. Over the years, this conflict between privacy and freedom of expression has been the source of countless legal battles in the courts.[9] There is a long list of cases that pit those two rights against one another, including the cases of *Douglas v Hello*[10], and *Campbell v MGN*,[11] just to name a few.[12] In these decisions, courts have tried to reach a balance between competing rights, which tends to be largely dependent on the facts of the case. As a general rule, courts have favoured an approach that places individual privacy above freedom of expression when the subjects are ordinary citizens, as in *Wainright v Home Office*[13] and *Google v Vidal-Hall*.[14] On the contrary, courts are generally more likely to side with the public

[7]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

[8]Bygrave (2002).

[9]Bignami (2008).

[10]*OBG Ltd v Allan and Douglas v Hello!* [2008] 1 AC 1.

[11]*Campbell v MGN Ltd* [2004] UKHL 22.

[12]*Murray v Express Newspapers Ltd* [2007] EWHC 1980 (Chancery Division); *Abbey v Gilligan* [2012] EWHC EWHC QB 3217; *Vidal-Hall & Others v Google Inc* [2014] EWHC QB 13.

[13]*Wainwright v Home Office* [2003] UKHL 53.

[14]*Google Inc v Vidal-Hall & Others* [2015] EWCA Civil 311.

interest to know and with freedom of expression in cases involving public figures, such as the aforementioned *Douglas* and *Campbell* decisions.

While European courts have tended to provide a careful balance of these two rights, this is not the case in the United States, where the traditionally strong protection of freedom of speech has its counterpart in a considerably weaker level of privacy safeguard.[15] Indeed, the U.S. has been following an almost opposite view of privacy to that present in Europe, specifically, what Werro calls the 'right to inform'[16], and others have gone as far as labelling the 'right to remember'.[17] This right does not exist in any legal sense, but the name neatly encapsulates the different approaches to privacy. While Europe has protected privacy to the point of creating a new right to be forgotten, the U.S. protects freedom of expression to the extent that it almost constitutes a right to remember.

Progressing from the concepts of privacy and data protection, various authors have advocated for the expansion of the right to information self-determination into something else. In particular, Viktor Mayer-Schönberger has been a vocal advocate for a right that allows Internet users to remove undesired information from the network.[18] The argument is that the Internet serves as a perfect storage place for memories of all sorts, and some of these memories serve no purpose, and may even prove to be extremely damaging. While society could simply change to give lower credit to these memories, his argument is that there should be a right to delete unwanted information from public online spaces.

Finally, there is an interesting legal precursor to the RTBF, and it is found in the English case of *AMP v Persons Unknown*.[19] In June 2008, a female university student in the UK had her mobile phone stolen from a Nottingham public transport.[20] The phone contained images "of an explicit sexual nature which were taken for the personal use of her boyfriend at the time". Shortly after the theft, the images were copied from the phone and uploaded to a picture-sharing site with her name and a link to her Facebook page attached. Someone warned her of this fact, and an email was sent to the hosting website, which promptly removed the images. However, the images were bundled into a torrent file and uploaded to The Pirate Bay under the title "Sexy Rich Chick Mobile Phone Found By IRC Nerdz". At the same time a person named Nils Henrik-Derimot contacted her on Facebook and threatened to have her exposed unless she friended him. Similarly, her parent's company was contacted with blackmail threats. The torrent file spread around the various tracker sites.

[15]Charlesworth (2000).

[16]Werro (2009).

[17]Balkam (2014).

[18]Mayer-Schönberger (2009).

[19]*AMP v Persons Unknown* [2011] EWHC QB 3454 (TCC).

[20]For obvious reasons, her identity is kept hidden in the proceedings.

The victim tried to have the files removed by various legal recourses. First, they filed a DMCA takedown notice[21] to Google to have the search engine remove links to the torrent files from searches on copyright grounds. They then filed for an injunction in the High Court of England and Wales "to prevent transmission, storage and indexing" of the pictures based on the claimant's right to privacy under Art 8 of the European Convention on Human Rights, and under Section 3 of the Protection from Harassment Act 1997. The ruling makes an interesting application of existing privacy law to protect the victim of a serious breach to her privacy. Ramsey J opines that privacy law does not affect freedom of expression in cases like this, and the possible damage done to the claimant's enjoyment of a private life outweigh other considerations, and therefore should preclude the publication of the images through any media.

However, RTBF does not use privacy, it is an application of data protection law. Next section will explain the application of this concept in the courts.

3 Google Spain

As stated above, since early 1995 European law had started covering the issue of information self-determination with the enactment and implementation of the data protection regime. By 2014, all the building blocks for what would become the right to be forgotten were already in place; as the DPD gives data subjects a variety of rights that, in combination, can eventually give rise to the so-called right to be forgotten. Article 6 of the Directive imposes an obligation for data controllers to keep personal data "accurate and, where necessary, kept up to date", and Article 12 permits data subjects to request for rectification, erasure or blocking of data that is incomplete or inaccurate, or where one of the following conditions has been met: (a) the processing is unlawful; (b) the data is no longer necessary in relation to the purpose for which it was collected; (c) the data subject withdraws consent; (d) the data subject objects to the processing.[22] All of these are important for the courts to create a right to be forgotten on the Internet.

A limited version of this right has now been enacted by the CJEU in the landmark ruling of *Google Spain v Costeja González*.[23] This is the first case that directly applies existing data protection principles to the Internet in a way that permits the erasure of search data. The case involves Mario Costeja González, a Spanish national, whose name was mentioned in a webpage from the Spanish newspaper La Vanguardia detailing a real-estate auction connected with proceedings for the recovery of social security debts. Whenever someone searched for his

[21] Cobia (2008).

[22] Szekely (2014).

[23] *Google Spain v Agencia Española de Protección de Datos and Mario Costeja González*, case C131/12, 13.05.2014. ECLI:EU:C:2014:317.

name, these pages came up near the top. Mr Costeja González filed a complaint with the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*, AEPD) using his prerogatives under the Spanish transposition of the Data Protection Directive. Based on the aforementioned Articles 6 and 12 of the Data Protection Directive, Mr Costeja González requested the removal or alteration of the pages from La Vanguardia, and he also requested *Google Spain* to remove or conceal the personal data relating to him, so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia.

The AEPD denied the request regarding the newspaper La Vanguardia, alleging that the publication of such data was legally justified, and it is a common procedure to make such information public in the national press. However, the AEPD granted the order concerning Google, and required that search engine results involving Mr Costeja González should not include a link to the offending pages. In a 2010 decision, the AEPD considered that "operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society." Unsurprisingly, Google appealed the ruling to the national high court (*Audiencia Nacional*), which referred several questions to the CJEU asking for clarification as to the application of the Data Protection Directive.

The questions involved in this case are complex, but they can be summarised as follows. Is the operation of indexing and crawling the web[24] an act of personal data processing? If the answer is yes, are search engines (and potentially web crawlers) data controllers, in the sense that they are under an obligation to protect personal data? If the answer is again yes, then can data protection authorities order a search engine to remove from their results links to websites where personal data has been published, without having to address those websites directly?

Simply, the question is whether search engines should be considered data controllers, and therefore whether they should provide users with tools to amend or remove listing to inaccurate personal data. The CJEU decided that:

1. Search engines are to be classified as processing personal data, and therefore are to be considered data controllers.
2. As such, search engines will be deemed to operate in the country by having an office, branch or subsidiary "for the purpose of promoting and selling advertising".
3. As a data controller, the search engine will have an obligation "to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person", even if the information displayed in that page is lawful.
4. When analysing a data subject's request to remove links to a search result, authorities should balance the interest of the subject in accordance to her rights under the European Convention on Human Rights, the economic interest of the

[24] A technical act performed either by a search engine as in the case of the Google Spain case, or by a web archiving crawler.

service provider, the role played by the data subject in public life, and the public's interest to have access to the information.

While the decision has been universally become known as the "right to be forgotten", it would be more accurate to describe it as the power to delist. The ruling has not created a new right as such, it has simply applied to search engines the existing rights to rectification, erasure, blocking and objection which are present in the Data Protection Directive and were already applied to personal data gathered by public authorities or processed by private entities. The Advocate General stated as much when he commented in his opinion that "the Directive does not provide for a general right to be forgotten in the sense that a data subject is entitled to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests."[25] However, the Advocate General was of the opinion that the court should not extend these rights to search engines, which the CJEU eventually did.

This case seems to pit privacy against freedom of speech. Indeed, if a result cannot be found—even if it can technically be accessed to when performing another search query, based on other words than the name of the person (e.g. the facts or the date)—the practical effect will be obscurity. While the court does mention freedom of speech, and makes a few considerations about the ongoing balancing act between both, the main thrust of the legal opinion seems directed at the privacy issue. The Court comments:

> Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page.

Put simply, there may be a privacy violation in a web page that shows up when the data subject's name is queried, but this is less important than the page actually showing up in search engine results when the name is queried. However, the court has left open the possibility of a case-by case appraisal by data protection authorities when asked to grant an order to remove search results:

> [I]nasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

[25]The Advocate General provides an opinion before the decision, the court can decide to follow it, rely on it, or ignore it (Jääskinen 2013).

Notably, there have been a few decisions that support the interpretation that the right to be forgotten will be applied on a strict case-by-case basis. The most noteworthy case happened in the Netherlands, where a court used *Google Spain* to answer a request to remove links to potentially damaging information. A court in Amsterdam denied a request by the owner of an escort agency who was convicted for attempted incitement of arranging a contract killing, a matter currently under appeal.[26] The subject wanted links to the reports of the crime removed from search results, but the Dutch court refused the request with an interesting application of the interaction between privacy and freedom of expression. The court commented:

> The [Google Spain] judgment does not intend to protect individuals against all negative communications on the Internet, but only against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions.[27]

This seems a rational interpretation of *Google Spain*, as its rationale was always to remove links that may cause an excessive invasion of privacy. The Dutch court concluded:

> The claimant now has to bear the consequences of his own actions. One of the consequences of committing a crime is that a person can be in the news in a very negative way and this will also leave its tracks on the Internet, maybe even for a very long time.[28]

This type of approach will probably be followed by national courts in future cases, and the fear expressed repeatedly by many commentators that *criminals will misuse Google Spain* and other undeserving recipients may very well be unfounded.

4 Application of the Ruling

The right to be forgotten mostly covers the type of information that is liable to affect significantly "the fundamental rights to privacy and to the protection of personal data",[29] and it specifically mentions that the court seeks to have a fair balance between those rights and the public's right to access personal information. Simply put, the decision does not give an unlimited right to remove anything that we do not like from the Web, it simply gives users the right to request the removal of links to search results which may seriously infringe a person's privacy. To do so, Google has made available a search removal request form[30] in which a subject may apply to exercise their rights within the European Union. This means that currently, it is entirely up to Google to decide whether such a request will be met or not.

[26] Spauwen and van Den Brink (2014).

[27] Ibid.

[28] Ibid.

[29] *Google Spain*, at 38.

[30] Search Removal Request Under Data Protection Law in Europe. https://support.google.com/legal/contact/lr_eudpa?product=websearch. Accessed 03 Nov 2016.

How is Google applying the RTBF? In 2015, the company released a transparency report for European privacy requests for search removals.[31] At the time of writing, Google had received 558,789 requests, and had evaluated 1,689,482 URLs for removal. Of these, 57% were not removed, a figure that has remained unchanged from the first report.[32] The requests came from all over Europe, but perhaps unsurprisingly, the company received more requests from the largest countries in the EU (France, Germany, UK and Spain), with the UK accounting for 96,229 alone at the time of writing.

As to the sites targeted by requests, this produces also some interesting statistics about the nature of the application of the right. The site hosting most links is perhaps unsurprisingly Facebook, with 14,314 URLs removed at the time of writing. The second highest site is Profile Engine, which is a website dedicated to finding people online by building profiles using publicly available data. Other top targets of RTBF requests are other social media sites such as Twitter, Badoo and Google Plus.

In the report, Google cites examples of requests received and how they were evaluated:

> A victim of rape asked us to remove a link to a newspaper article about the crime. The page has been removed from search results for the individual's name. We received multiple requests from a single individual who asked us to remove 20 links to recent articles about his arrest for financial crimes committed in a professional capacity. We did not remove the pages from search results.
>
> We received a request from a crime victim to remove 3 links that discuss the crime, which occurred decades ago. The pages have been removed from search results for her name.
>
> An individual asked us to remove links to articles on the internet that reference his dismissal for sexual crimes committed on the job. We did not remove the pages from search results.
>
> After we removed a news story about a minor crime, the newspaper published a story about the removal action. The Information Commissioner's Office ordered us to remove the second story from search results for the individual's name. We removed the page from search results for the individual's name.[33]

Assuming that this quick snapshot gives a representative picture of the requests received by Google, there seem to be two main categories of complaints. Firstly, there are people who either have been convicted or are suspected of having committed a crime, and these requests seem to be usually denied. Secondly, there are requests addressing more serious privacy threats, such as the aforementioned rape victim; those requests are usually granted, and we could argue that in this regard the right to be forgotten is working as intended. However, this is a limited take on the actual application, as we do not have access to the entire number of requests.

[31] Google (2014).

[32] When the report was first released in 2015, the figure stood at 58%.

[33] Ibid.

Having said that, a quick browse through the highlighted removal requests emphasises just how expensive this is for large intermediaries such as Google, and it explains why they object to the adoption of this right.

It is important to point out that if the above is an accurate representation of the actual RTBF application, then it would at least operate in a similar manner to limited witness and victim protection legislation in many countries. For example, in the UK, some vulnerable victims of crimes are protected by the law, a protection that can be extended to censoring the press.[34] In the past, injunctions and gag orders attempting to keep information from the public eye have easily been circumvented with Internet searches, making it impossible to enforce them online.[35]

Google has also released a list of most links removed by the website that receives the requests. Most of the application of the RTBF is cantered towards removal of social media posts, with the top recipient of removal requests being Facebook. The second top recipient of removal requests is a website called Profile Engine, which gathers information held about individuals online. However, it should be emphasised again that this analysis rests entirely on the little information available from the Google transparency report. More data is needed for a better analysis of the true impact of RTBF on freedom of expression and the public interest.

Interestingly, another source of information for analysis of removal requests is to be found when third parties, which have had links to them delisted by Google, tell the public of such removals. The best source of information outside of Google now is Wikipedia, as they have a reader-friendly transparency report that now includes RTBF request removals.[36] While these reports are an important source of information, they are limited as they only provide detail of the pages that have been delisted, without indication of who actually made the request, or for what reason. At the time of writing, there have been 282 Wikipedia articles removed from search results by Google because of an RTBF request, with the Dutch and English version of Wikipedia having received the majority of delistings. No pattern can be identified by looking at the removed pages, as these include reality TV shows,[37] a porn actress,[38] a former criminal,[39] and a trans-gender winner of a reality show.[40] In short, there may well be legitimate reasons to delist in these circumstances, but it is impossible to make a full assessment.

Commentators around the world have both hailed and criticised the RTBF decision. On the one hand, opponents worry that the decision may interfere with free access to information, and that it will herald an era of abuse of these amendment orders, even if the court has specified that authorities should consider the

[34]Temkin (2003).

[35]Matthiesson (2010).

[36]Wikimedia Foundation (2016).

[37]Wikipedia https://nl.wikipedia.org/wiki/Temptation_Island. Accessed 02 Nov 2016.

[38]Wikipedia https://nl.wikipedia.org/wiki/Helen_Duval. Accessed 02 Nov 2016.

[39]Wikipedia https://en.wikipedia.org/wiki/Gerry_Hutch. Accessed 02 Nov 2016.

[40]Wikipedia https://en.wikipedia.org/wiki/Nadia_Almada. Accessed 02 Nov 2016.

public interest aspect of the linked data.[41] Supporters point out that there are valid reasons why a person would like some personal data not to show up when her name is searched, and that there should be a legal recourse to those whose privacy is being severely affected.[42]

Overall, the coverage of the RTBF has been surprisingly negative. Particularly, commentary in the press and US academia has heavily criticised the decision. This is a topic that once more unearths the growing chasm between the US and Europe when it comes to the interaction between privacy and free speech, with many US commentators seeing the RTBF as an infringement on free speech. A common denominator in the criticisms is that the RTBF is going to be used to bury information that should be remembered. For example, commentators accused the RTBF of favouring censorship and preventing freedom of information: "one person's right to be forgotten may be another person's right to remember".[43] Because Google does not host the data, it should not be responsible for it.[44] Indeed, Internet Service Providers managed to get safe harbour legislations limiting their responsibility. Concerns for culture and memory if archiving is hampered have also been raised: "The need to remember" also happens in "online spaces of remembrance".[45]

Other authors have highlighted the vagueness of the right, stressing, for example, that "since the right to be forgotten is such an amorphous concept, when employed in the service of guarding one's reputation, it makes the task of balancing rights even more complicated".[46]

Finally, some commentators[47] have criticised the ruling as being a good example of the so-called "privatisation of censorship"[48]; this is because Google is given the power to determine which results should be removed, instead of this important function going to a court of law. However, if a user is denied the application, this could be litigated in court. While it is true that Google retains considerable control over the RTBF enforcement, users can indeed still appeal decisions to data protection authorities and/or the courts. The power of the national Data Protection authorities tends to be forgotten in the debate.

This being said, the question of Google's applications is perhaps the most important point of debate and an aspect of the ruling that has been lost in the privacy *versus* freedom of expression discourse. The current implementation of the RTBF rests considerably on a firm, who has the power to review the decision and deny the application, and who is directly responsible for existing unsuitable

[41] Zittrain (2014).
[42] Guadamuz (2014a).
[43] Solon (2014).
[44] Rosen (2012).
[45] Parmar (2014).
[46] Fazlioglu (2013).
[47] Tréguer (2014).
[48] Tambini, et al. (2008).

examples. This kind of power has led several academics to issue a request[49] to Google for more transparency about the way it applies the right. As Google has become such an important broker in this area, there is a growing need to understand the type of requests that are handled, and what parameters are being used to make decisions. This open letter says:

> We all believe that implementation of the ruling should be much more transparent for at least two reasons: (1) the public should be able to find out how digital platforms exercise their tremendous power over readily accessible information; and (2) implementation of the ruling will affect the future of the RTBF in Europe and elsewhere, and will more generally inform global efforts to accommodate privacy rights with other interests in data flows.[50]

The RTBF could work mirroring an existing mechanism that helps to remove false positives, this is the notice and take down procedures for copyright infringing materials.[51] Over the years, content has been removed in Google services such as YouTube because of mistaken or malicious removal requests, only to be restored once the affected party has complained. It would be possible to deploy a similar regime for RTBF requests, both with more transparency and with a stronger system of protection for freedom of expression.

While some of these concerns are legitimate, some critics apparently fail to understand how limited the new right is in practice. As stated before, the CJEU tried to base their decision on privacy, leaving out most of the balancing act between privacy and data protection. There is something to be said about the political power of remembrance, particularly in countries that housed secretive and repressive regimes where people were "erased" from history; but we must understand the *Google Spain* decision as a much more nuanced allowance to delist information to protect privacy.

There has been a rush to assume that the right will affect data integrity, freedom of expression, and archiving.[52] However, the ruling mostly covers the type of information that is liable to affect significantly "the fundamental rights to privacy and to the protection of personal data", and it specifically mentions that the court seeks to have a fair balance between those rights and the public's right to access information. In fact, a large part of the debate so far has been tainted by overlooking the precise wording of the ruling.

[49]Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data (2015), https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd#.mxjhd34sh. Accessed 02 Nov 2016.

[50]Ibid.

[51]Urban and Quilter (2006).

[52]Hole (2014).

5 General Data Protection Regulation

While the RTBF was originated from the interpretation given to the existing data protection law by the CJEU in 2014, a new development will move the debate forward considerably. The aforementioned General Data Protection Regulation (GDPR),[53] which came into force in 2016, repealed the Data Protection Directive and established an updated regime geared towards the digital age. One of the biggest changes present in the Regulation is that it consolidates the various rights and principles from the existing Directive that were dealing with outdated and/or erroneous data, and puts them together into a new full-fledged right, the "right to erasure."

Article 17 of the GDPR will create an obligation for Member States to provide data subjects with the right to obtain from the controller erasure of personal data where one of various requirements contained in Articles 5 and 6 have not been met. Some of these requirements are:

(a) The data is no longer necessary in relation to the purposes for which it was collected or processed.
(b) The data subject has withdrawn his consent.
(c) The data subject objects to the processing and there are no legitimate grounds to deny this request.
(d) The data has been processed unlawfully.

Simply, the right to erase can be brought by data subjects to remedy a situation in which one of their listed rights is under threat. There is a glaring omission to the above, and it is the existing requirement that data must be "must be accurate and kept up to date", which is an important part of the existing iteration of the RTBF contained in the Google Spain decision. While the proposed right to erase gives some more power to the user to object processing, the very founding principle behind *Google Spain* may no longer relevant. In some ways, this makes the right to erase very different from the existing RTBF version. While it will perhaps be easier to bring an action, it seems like the requirement of removing excessive information that makes RTBF what it is has been diluted. However, one could argue that the right to object to inaccurate and out-dated information is already contained in the prohibition against unlawful processing, as it is broad enough to accommodate such action.

Furthermore, Article 17 contains an inbuilt reference to balance with freedom of expression, and paragraph 3 has an exception to the right to erase in "exercising the right of freedom of expression and information." This should hopefully lay to rest most of the criticism mentioned above which see the RTBF as a possible threat to

[53]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.

freedom of expression. However, the in-built balance may serve to further dilute the power of the right.

Besides that, another major concern with RTBF is being addressed. It is often forgotten that the RTBF does not undermine the original content directly; it only requires that a search engine should remove the link to the content. This is why the term "right to delist" or "power to delist" may be more accurate, as the Internet does not forget easily. Indicative of this type of thinking is the use of the term "right to remember".[54] As it has been stated already, this is a concept that does not have any legal basis, and it is used mostly as a rhetorical device. Opponents usually support this argument by highlighting and publicising cases where links were removed undeservedly, and then they make an argument on behalf of the public's right to know, freedom of speech, or in this case, a non-existent right to remember.

The GDPR addresses some of these criticisms directly with other exceptions. For example, Article 17(3)(d) states that there will not be a right to erase "for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes," given that the right to erase is likely to "render impossible or seriously impair the achievement of the objectives of the archiving purposes in the public interest, or the scientific and historical research purposes or the statistical purposes." Similarly, there are now exceptions for public health information, and for legal claims. While the new exceptions are not fully ironclad, they help to address some concerns about the possible abuse of RTBF.

However, much as the RTBF is not really about forgetting, the right to erasure could also be a misnomer. While Article 17 requires the data controller and the regulatory authorities to erase offending data, what seems to be happening is again more of a delisting, with the controller having to abstain from further dissemination. The largest targets of RTBF action in the last few years have been search engines, and what takes place is not so much erasure as de-listing.

However, it is early days, as Member States will have two years to implement the GDPR, and it is likely that we will see new guidelines and practices about how to implement the new right. For the time being, the ambiguity present in the RTBF *Google Spain* ruling is about to disappear.

6 Should There be an RTBF?

In a video about surveillance and privacy, French activists La Parisienne Libérée and Jérémie Zimmermann remark that "everyone has something to hide".[55] It can be something innocuous, like a mild Farmville addiction, a guilty musical pleasure, or an embarrassing viral video. Some things can be graver, such as a sexting session that has been made public, an incriminating picture that may seriously hinder future

[54] Lee (2014).

[55] Youtube (2014) https://youtu.be/rEwf4sDgxHo. Accessed 03 Nov 2016.

employment efforts, information about one's sexual orientation while living or working in a community that has low thresholds of tolerance; affiliation to a political entity or union. What if a link to that sensible personal information was made available online for the world to see? Could you have a legal recourse to remove it? Or does the public have a right to know?

The Google Spain decision materialised the theoretical conflict between the concept of information self-determination and freedom of speech, or put simply, we have the individual's interest to privacy against the need for public knowledge. The legal obligation arising from the RTBF may conflict with the public's genuine interest to access certain information. Wikipedia, an institution that can be considered as a vault of human knowledge, has vocally opposed the ruling through the voice of several of its advocates.[56] Wikipedia founder Jimmy Wales, fears that the removal of links will create censorship, "memory holes",[57] and others believe that the decision would be "undermining the world's ability to freely access accurate and verifiable records about individuals and events".[58] Others, mostly US legal scholars with a vision of freedom of expression more extensive than the European conception mindful of privacy, also strongly opposed the ruling, fearing that the right could "destroy the Internet archive and become a way to bury evidence"[59] or permit "Orwellian airbrushing of history".[60]

Collective rights to remember and to memory, free access to information, and freedom of expression seem to clash with private individual rights to privacy. These visions seem exaggerated to say the least, as evidenced by the practical application of the right described above suggests. The nightmarish scenario of a crippled Internet filled with "memory holes" has failed to materialise, and at most, it seems like those links that are actually delisted from search results are indeed worthy of the removal.

At most, the worst argument that can be made against the RTBF is about the privatisation of justice, where a company such as Google is given a role that in other times would have gone to regulators.[61] Besides this privatisation of quasi-judicial decisions, other aspects could be criticised about RTBF, such as the lack of process transparency, and the reinforcement of a quasi-monopolistic hegemony of the search engine on freedom of information. However, the actual right as enacted by Google Spain and by the GDPR is not likely to have more nefarious effects against freedom of information and freedom of speech. Moreover, the ruling as such is not likely to prevent preservation. It must be stressed again that the RTBF does not remove content in many instances, it is mostly used to delist links from search results. Thus, the digital resource does not disappear, it remains available on the web and can be further analysed and disseminated. This means that the impact of

[56]Curtis and Philipson (2014).
[57]Ibid.
[58]Tretikov (2014).
[59]Levine (2014).
[60]Lyons (2014).
[61]Sebastion (2015).

the right is not too negative. On the contrary, the benefit for the victims of privacy abuses cannot be overstated.

Broadly speaking, the right to forget relies on broader foundations than data protection. The threat to individual's privacy created by mass-surveillance and big data gathering and processing, by both public and private players, has become one of the most important subjects of our time.[62] As a response to algorithmic governance, RTBF may be the best solution by allowing a limited right to delete. The object of such a right is not to hinder memory, it is to limit the effect of data mining and data analysis and restore balance in the power relation between surveillance and other marketing information systems and individuals.[63]

Furthermore, the question is broader than a binary choice between disclosing and deleting information, and even beyond the mere legalistic existence of a legal right. We can see the general subject of self-management of information as a potentially technical issue in the digital environment, where individuals are given the power to manage different levels of publicity through technical means. As such, we can see different circles of divulgation: family, work, medical services.[64] Similarly, the rise of tools such as Privacy Enhancing Technologies (PETs), more recently labelled Privacy-by-Design solutions, are developing "contextual approaches".[65] User-centric identity management systems propose to implement laws and preferences, and crawl the web to delete photos after a specific time.[66] Thus, the question would be not to rely on legal tools, but on the technical implementation and feasibility of an actual and real RTBF, which would remove all instances of the resource and make it impossible to access, reproduce and disseminate them.

7 Conclusion

While the right to be forgotten has been interpreted as a potential threat to freedom of expression, the intended application of the right to be forgotten has been limited in scope, at least as far as one can discern from the limited information available through Google's transparency report.

The RTBF has been maligned in some quarters, as an abuse of data protection in detriment of freedom of speech, but those who make that claim tend to ignore that we already have regimes in place that remove links to offending information online. Online intermediaries are already deleting instances on request, particularly with legal frameworks such as the copyright notice and takedown procedure.[67] However,

[62] Schneier (2015).
[63] Supra n 22.
[64] Ibid.
[65] Nissenbaum (2011).
[66] Supra n 22.
[67] Guadamuz (2014b).

the entry into force of the General Data Protection Regulation should put most of the debate to rest, the presence of exceptions to the right to erase for freedom of expression and other instances such as web archiving and the public interest serving to make potentially damaging disruption much more difficult. Future work in this area may explore wider issues.

References

Ardia DS (2010) Free speech savior or shield for scoundrels: an empirical study of intermediary immunity under section 230 of the communications decency act. Loyola Los Angeles Law Rev 43(2):373–506

Balkam S (2014) The Right to Remember, Huffington Post. http://www.huffingtonpost.com/stephen-balkam/the-right-to-remember_b_5338223.html. Accessed 3 Nov 2016

Bignami F (2008) The case for tolerant constitutional patriotism: the right to privacy before the European courts. Cornell Int Law J 41(2):211–249

Bygrave LA (2002) Data protection law: approaching its rationale, logic and limits. Kluwer Law International, London

Charlesworth A (2000) Clash of the data Titans? US and EU data privacy regulation. Eur Public Law 6(2):253–274

Cobia J (2008) Digital millennium copyright act takedown notice procedure: misuses, abuses, and shortcomings of the process. Minn J Law Sci Technol 10(1):387–411

Curtis S, Philipson A (2014) Wikipedia Founder: EU's Right to be Forgotten is 'Deeply Immoral'. The Telegraph. http://www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html. Accessed 3 Nov 2016

Fazlioglu M (2013) Forget me not: the clash of the night to be forgotten and freedom of expression on the internet. Int Data Priv Law 3(3):149–157

Google (2014) Google Transparency Report for European Privacy Requests for Search Removals. https://www.google.com/transparencyreport/removals/europeprivacy/. Accessed 3 Nov 2016

Google Spain v Agencia Española de Protección de Datos and Mario Costeja González, case C131/12, 13.05.2014. ECLI:EU:C:2014:317

Guadamuz A (2014a) Developments in intermediary liability. In: Savin A, Trzaskowski J (eds) Research handbook On EU internet law. Edward Elgar, p 132

Guadamuz A (2014b) You have the right to be forgotten. Technollama Blog. http://www.technollama.co.uk/you-have-the-right-to-be-forgotten. Accessed 2 Nov 2016

Hole J (2014) Do you have the right to be forgotten?. State of Digital. http://www.stateofdigital.com/right-to-be-forgotten/. Accessed 02 Nov 2016

Hornung G, Schnabel C (2009) Data protection in Germany I: the population census decision and the right to informational self-determination. Comput Law Secur Rev 25(1):84–88. doi:10.1016/j.clsr.2008.11.002

Jääskinen (2013) Opinion of Advocate General Jääskinen, Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González. Reference for a preliminary ruling from the Audiencia Nacional (Spain), Curia, 25.06.2013

Lawrence D (2016) The journalist and the troll: this man spent two years trying to destroy me online. Bloomberg. http://www.bloomberg.com/features/2016-benjamin-wey/. Accessed 3 Nov 2016

Lee D (2014) BBC to Publish 'Right to be Forgotten' Removals List. BBC News. http://www.bbc.co.uk/news/technology-29658085. Accessed 2 Nov 2016

Levine D (2014) The MH17 Disaster Demonstrates the Dangers of "Right to be Forgotten". Slate Future Tense. http://www.slate.com/blogs/future_tense/2014/07/22/mh17_investigation_and_the_right_to_be_forgotten.html. Accessed 3 Nov 2016

Luhmann N (1995) Social systems. Stanford University Press, Stanford
Lyons D (2014) Right to be forgotten? Forget About it. Tech Policy Daily. http://www.techpolicydaily.com/technology/right-forgotten-forget/. Accessed 3 Nov 2016
Matthiesson S (2010) Who's afraid of the limelight? The Trafigura and Terry super-injunctions, and the subsequent fallout. J Media Law 2(2):153–167
Mayer-Schönberger V (2009) Delete. The virtue of forgetting in the digital age. Princeton University Press, Princeton
Nissenbaum H (2011) A contextual approach to privacy online. Daedalus J Am Acad Arts Sci 140 (4):32–48
Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data (2015), https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd#.mxjhd34sh. Accessed 2 Nov 2016
Parmar M (2014) Memorialising 40 years since Idi Amin's Expulsion: Digital "Memory Mania" to the "Right to be Forgotten". South Asian Pop Cult 12(1):1–14
Rosen J (2012) The right to be forgotten. Stanford Law Rev 64:88–92
Schneier B (2015) Data and Goliath: the hidden battles to collect your data and control your world. W.W. Norton & Company, London
Search Removal Request Under Data Protection Law in Europe. https://support.google.com/legal/contact/lr_eudpa?product=websearch. Accessed 3 Nov 2016
Sebastion A (2015) The online right to be forgotten in the European justice evolution. Int J Manag Knowl Learn 4(1):59–68
Solon O (2014) People have the right to be forgotten, rules EU court. Wired UK. http://www.wired.co.uk/article/right-to-be-forgotten-blog. Accessed 2 Nov 2016
Sørensen E, Triantafillou P (2016) The politics of self-governance. Routledge, Abingdon
Spauwen J, van den Brink J (2014) Dutch Google Spain ruling: more freedom of speech, less right to be forgotten for criminals. Inforrm's Blog. https://inforrm.wordpress.com/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwenand-jens-van-den-brink/#more-27910
Szekely I (2014) The right to be forgotten and the new archival paradigm. In: Pereira A, Ghezzi A, Vesnić-Alujević L (eds) The ethics of memory in a digital age: interrogating the right to be forgotten. Palgrave Macmillan, pp 28–49
Tambini D, Leonardi D, Marsden CT (2008) Codifying cyberspace: communications self-regulation in the age of internet convergence. Routledge, London
Temkin J (2003) Rape and the legal process, 2nd edn. Oxford Monographs on Criminal Law and Justice, Oxford University Press. doi: 10.1046/j.1468-2230.2003.06606009_1.x
Tréguer F (2014) Right to be forgotten: with free expression under threat, Europe needs a 'Marco Civil Moment'. Global Voices. https://globalvoices.org/2014/09/11/right-to-be-forgotten-with-free-expression-under-threat-europe-needs-a-marco-civil-moment/. Accessed 2 Nov 2016
Tretikov L (2014) European court decision punches holes in free knowledge. Wikipedia Blog. http://blog.wikimedia.org/2014/08/06/european-court-decision-punches-holes-in-free-knowledge/. Accessed 3 Nov 2016
Urban J, Quilter L (2006) Efficient process or "Chilling Effects"? Takedown notices under section 512 of the digital millennium copyright act. Santa Clara Comput High Technol Law J 22 (4):621–693
Werro F (2009) The right to inform v. the right to be forgotten: a transatlantic clash. In: Ciacchi AG et al (eds) Liability in the third millennium. FRG, Baden-Baden
Wikimedia Foundation (2016) Wikipedia, Notices received from search engines, https://wikimediafoundation.org/wiki/Notices_received_from_search_engines
Youtube (2014) https://youtu.be/rEwf4sDgxHo. Accessed 3 Nov 2016
Zittrain J (2014) Don't Force Google to "Forget". The New York Times. http://nrs.harvard.edu/urn-3:HUL.InstRepos:12921731. Accessed 2 Nov 2016

Chapter 4
The Right Not to be Subject to Automated Decisions Based on Profiling

Isak Mendoza and Lee A. Bygrave

Abstract In this chapter, a critical analysis is undertaken of the provisions of Art. 22 of the European Union's General Data Protection Regulation of 2016, with lines of comparison drawn to the predecessor for these provisions—namely Art. 15 of the 1995 Data Protection Directive. Article 22 places limits on the making of fully automated decisions based on profiling when the decisions incur legal effects or similarly significant consequences for the persons subject to them. The basic argument advanced in the chapter is that Art. 22 on its face provides persons with stronger protections from such decision making than Art. 15 of the Directive does. However, doubts are raised as to whether Art. 22 will have a significant practical impact on automated profiling.

1 Introduction

One of the most enigmatic, intriguing and forward-looking rights provided by European Union (EU) law on the protection of personal data is a qualified right for a person not to be subject to automated decisions based on profiling. In general, profiling denotes the process of (1) inferring a set of characteristics about an individual person or group of persons (i.e., the process of creating a profile), and/or (2) treating that person or group (or other persons/groups) in light of these characteristics (i.e., the process of applying a profile).[1] The above-mentioned right primarily affects the latter facet of profiling. It has the potential to curtail the increasingly widespread use by businesses and government agencies of automated

Work on this chapter was carried out partly under the aegis of the research project 'Security in Internet Governance and Networks: Analysing the Law' (SIGNAL), funded by the Norwegian Research Council and Norid AS. References to legal instruments are to their amended form as of 1 May 2017. Thanks are due to Luca Tosoni for useful input, particularly regarding Italian law. Nonetheless, the usual disclaimer applies.

[1] See further, e.g., Hildebrandt (2008), p. 19.

I. Mendoza • L.A. Bygrave (✉)
Department of Private Law, University of Oslo, Karl Johansgt 47, N-0162 Oslo, Norway
e-mail: i.e.s.mendoza@jus.uio.no; lee.bygrave@jus.uio.no

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_4

methods for categorising, assessing and discriminating between persons. These methods are instituted for a variety of ends, such as enhancing the impact of advertising, screening applicants for jobs or bank loans, and creating differentiated pricing for services. Examples include online behavioural advertising,[2] e-recruiting,[3] and weblining.[4]

Over the last two decades, the right under EU law not to be subject to automated decisions based on profiling has chiefly inhered in Art. 15(1) of the 1995 Directive on data protection (Data Protection Directive or DPD).[5] As elaborated below, it is a complex right in its formulation. It is also, in some ways, a second-class data protection right: it is rarely enforced, poorly understood and easily circumvented. Its marginality is remarkable given that we live in an era when decision making is increasingly the result of computer algorithms fed by 'Big Data'-analytics.

The Data Protection Directive will soon be replaced by the General Data Protection Regulation (GDPR),[6] which shall apply from 25 May 2018. Article 22 of the GDPR (set out in Sect. 3 below) replicates the right in DPD Art. 15(1), but with some changes. These changes raise several questions. One set of questions concern the rationale and meaning of the reformulated right: does Art. 22 signal a different set of concerns or different set of semantics than those pertaining to DPD Art. 15? Another set of questions is whether the reformulated right provides a stronger protection of the principle for which DPD Art. 15(1) stands and whether it will have a greater impact on automated profiling than has DPD Art. 15. It is with each of these questions that this chapter is concerned.

2 DPD Art. 15

Article 15 of the Data Protection Directive reads as follows:

[2]This refers to the customisation of online advertisements to a person based on his or her online profile. See further Leon et al. (2012); Borgesius (2015), ch.2.

[3]E-recruiting refers to the automated ranking of job applicants, which in turn can be used to select automatically persons for job interviews or to reject automatically other applicants. See further Faliagka et al. (2012), p. 557.

[4]Weblining refers to a situation in which a person visiting a website is offered products or services at a higher price than other (assumedly more valued) consumers have to pay, or the person is denied an opportunity of purchasing products/services that are made available to others, based on the data gleaned from the person's online activities. See further Stepanek (2000), Andrews (2011).

[5]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/31. The provisions of Art. 15 are set out in the next section.

[6]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L119/1.

> 1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
>
> 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
>
> (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
>
> (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

The roots of these provisions reach back to France's 1978 Act on data processing, files and individual liberties,[7] but DPD Art. 15 is the first pan-European legislative norm aimed at regulating purely machine-based decisions in a data protection context. One may regard it as an attempt by lawmakers to anticipate technological-organisational developments that were, in the late 1980s and early 1990s, still fairly nascent. This partly explains the broad-brush formulation of its provisions.

Several characteristics of Art. 15 make it rather special compared to other data protection norms. First, Art. 15 is directed at a type of decision rather than data processing.[8] It thereby resembles traditional administrative law rules on government decision making. Yet, Art. 15 has potentially greater impact on decision-making processes of the private sector than of the public sector, at least in jurisdictions with administrative law regimes that provide broad rights of appeal against government agency decisions. Much depends, however, on the peculiarities of each member state's implementation of Art. 15.[9]

---

[7] *Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. Article 2 of the Act in its original form stipulated: 'Aucune décision de justice impliquant une appréciation sur en comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé. Aucune décision administrative ou privée impliquant une appréciation sur en comportement humain ne peut avoir seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé'. Article 3 stated: 'Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés'. In amendments to the Act in 2004, the provisions of Art. 2 were moved to Art. 10 while the provisions of Art. 3 were moved to Art. 39(1). Both sets of provisions were also reformulated to align better with the DPD.

[8] In practice, though, the distinction between decision and data processing is blurred as decisions inevitably involve the processing of data.

[9] For instance, Italy's implementation of Art. 15 has prohibited judicial or administrative decisions involving assessment of a person's conduct that are based solely on the automated processing of personal data aimed at defining the person's profile or personality, whereas similar decisions made by private sector actors have been simply subject to a qualified right to object by the data subject: see Art. 14 of the Personal Data Protection Code of 2003 (*Decreto legislativo 30 giugno 2003, n. 196: Codice in Materia di Protezione dei Dati Personali*).

Secondly, Art. 15 embodies a principle that is not obviously part of the customary 'fair information practice' principles of data protection law. This is a principle that fully automated assessments of a person's character should not form the sole basis of decisions that significantly impinge upon the person's interests.[10]

Thirdly (and most importantly for present purposes), Art. 15 is well-nigh the only set of provisions in the Data Protection Directive that *directly* tackles aspects of automated profiling. However, it is closely complemented by Art. 12(a) which provides a person with a right to 'knowledge of the logic involved in any automated processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1)'. Further, a large number of other provisions in the DPD indirectly set limits on the profile generation process inasmuch as the latter involves processing of personal data.[11]

Its special profile notwithstanding, Art. 15 has played an extremely modest, if not marginal role in the operation of European data protection law. It has not been the subject of litigation before the Court of Justice of the EU (CJEU) or, to our knowledge, any national courts, bar those of Germany.[12] Neither has it figured prominently in enforcement actions by national data protection authorities, nor in assessments of the adequacy of third countries' data protection regimes with a view to regulating the flow of personal data to these countries.[13] In the latter respect, it is noteworthy that the right provided by Art. 15(1) neither was incorporated in the former 'Safe Harbour' agreement between the USA and EU,[14] nor is it incorporated in the successor 'Privacy Shield' agreement.[15] This is not to say that the right has been simply symbolic, but the occasions in which it has been invoked appear to have been rare.[16] Moreover, while it has inspired a proposal for a similar right to be

[10]Bygrave (2002), p. 2. Further on traditional 'fair information practice' principles, see, e.g., Bygrave (2014), ch. 5 and references cited therein.

[11]For the seminal analysis of these provisions in light of Art. 15, see Bygrave (2002), pp. 334–357.

[12]In 2014, the German Federal Court of Justice (Bundesgerichtshof) handed down an appeal judgment that touches briefly on the scope of the German rules that transpose DPD Art. 15. See further n. 36 below.

[13]The view of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established pursuant to DPD Art. 29 has been that the principle established by Art. 15 does not qualify as a 'basic' principle but as an 'additional principle to be applied to specific types of processing', at least in determining adequacy assessments of third countries under DPD Art. 25: see Working Party on the Protection of Individuals with regard to the Processing of Personal Data (1998), pp.6–7. Nonetheless, Art. 15 is sometimes taken into consideration in the context of approving Binding Corporate Rules (BCRs) for cross-border data transfer: see, e.g., approval by the Spanish Data Protection Authority (Agencia Española Protección de Datos) of the BCRs for Latham & Watkins (file number TI/00030/2017).

[14]See Commission Decision 2000/520/EC of 26 July 2000 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215/7. The decision was invalidated by the CJEU in *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, Judgment of 6 October 2015.

[15]Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207/1.

[16]See generally Bosco et al. (2015), pp. 39, 42.

incorporated in a modernised version of the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[17] and also inspired various provisions of the 1997 Code of Practice on Protection of Workers' Data drafted by the International Labour Office (ILO),[18] it has not been widely replicated in the legal regimes of non-European countries.[19]

Several features of Art. 15 undermine its traction. First, its application depends on multiple conditions being satisfied: a decision must be made; the decision must have legal or otherwise significant effects on the person whom the decision targets; the decision must be based solely on automated data processing; and the data processed must be intended to evaluate certain personal aspects of the person targeted by the decision. If one of these conditions is not met, the right in Art. 15 (1) does not apply. For this reason, the right has been aptly characterised as resembling a house of cards.[20] Secondly, a considerable degree of ambiguity inheres in these conditions and this ambiguity is exacerbated by lack of authoritative guidance on how they are to be construed. Thirdly, even if all of the conditions for its exercise are met, the right is subject to fairly broad and nebulous derogations. The most practically important of these are provided in Art. 15

[17]See Draft modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS 108], drawn up by the Council of Europe's Ad hoc Committee on Data Protection (version of September 2016). According to Art. 8(1) of the draft, '[e]very individual shall have a right: (a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration; [. . .] (d) to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates compelling legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms'. See too the Council of Europe's Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in the World of Big Data (adopted 23 January 2017; T-PD(2017)01), especially principles 7.1 ('The use of Big Data should preserve the autonomy of human intervention in the decision-making process'), 7.3 ('Where decisions based on Big Data might affect individual rights significantly or produce legal effects, a human decision-maker should, upon request of the data subject, provide her or him with the reasoning underlying the processing, including the consequences for the data subject of this reasoning') and 7.4 ('On the basis of reasonable arguments, the human decision-maker should be allowed the freedom not to rely on the result of the recommendations provided using Big Data').

[18]See particularly principles 5.5 ('Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data'), 5.6 ('Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance'), 6.10 ('Polygraphs, truth-verification equipment or any other similar testing procedure should not be used') and 6.11 ('Personality tests or similar testing procedures should be consistent with the provisions of this code, provided that the worker may object to the processing').

[19]Its replication outside Europe has occurred principally in a handful of African jurisdictions: see Senegal's Data Protection Act of 2008 s. 48; Angola's Law No.22/11 on Data Protection of 2011 Art. 29; Lesotho's Data Protection Act of 2012 s. 51; and South Africa's Protection of Personal Information Act of 2013 s. 71. By contrast, the only jurisdiction in the Asia-Pacific region with an equivalent to DPD Art. 15 is the Macau Special Administrative Region: see its Act 8/2005 on Personal Data Protection Art. 13.

[20]Bygrave (2001), p. 21; Bygrave (2002), p. 364.

(2) (aspects of which are dealt with in Sect. 4 below). Although DPD Art. 9 also requires certain derogations from Art. 15(1) in the interests of freedom of expression, it seems to have had little practical relevance.[21]

3 Rationale for GDPR Art. 22

As noted in the introduction, the GDPR will replace the Data Protection Directive in May 2018. At the same time, the essence of the right provided by DPD Art. 15 will persist, albeit in a somewhat different form, in GDPR Art. 22. A similar right has also been inserted in Art. 11 of the Directive on Data Protection and Law Enforcement (Directive (EU) 2016/680).[22] Traces of the right (or, more accurately, an associated duty) are further found in Art. 6 of the Directive on Processing of Passenger Name Record Data (Directive (EU) 2016/681).[23] However, this chapter is chiefly concerned with the provisions of GDPR Art. 22. They read as follows:

[21] See also Bygrave (2001), p. 21; Bygrave (2002), p. 357.

[22] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L119/89. Article 11 stipulates: '1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller. 2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. 3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.' Article 11(1) essentially replicates Art. 7 of the predecessor to this Directive—Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60. Article 7 of the Framework Decision is expressed as a permission rather than prohibition (i.e., automated decisions 'shall be permitted only if authorised by a law which also provides measures to safeguard the data subject's legitimate interests'), but the effect is the same as for Art. 11(1). The second and third paragraphs of Art. 11 are new—i.e., there are no equivalent provisions in the Framework Decision.

[23] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L119/132. Article 6(5) provides: 'Member States shall ensure that any positive match [leading to the identification of persons who may be involved in terrorism or serious crime and who thus need to be subject to further examination by the competent authorities] resulting from the automated processing of PNR data … is individually reviewed by non-automated means to verify whether the competent authority … needs to take action under national law'.

> Article 22 Automated individual decision-making, including profiling
>
> 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
>
> 2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.
>
> 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
>
> 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

The *travaux préparatoires* to the GDPR provide little explanation of the rationale for these provisions. Nonetheless, it is safe to assume that the rationale is at least partly rooted in the concerns that gave rise to DPD Art. 15 over two decades ago. The primary catalyst for Art. 15 was the potential weakening of the ability of persons to exercise influence over decision-making processes that significantly affect them, in light of the growth of automated profiling practices. Explaining the forerunner to Art. 15(1) contained in the 1990 DPD proposal, the European Commission stated:

> This provision is designed to protect the interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'.[24]

The Commission also expressed anxieties over the quality of fully automated decision-making processes, more specifically a fear that such processes will cause humans to take for granted the validity of the decisions reached and thereby reduce their own responsibilities to investigate and determine the matters involved:

> the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a

[24] Explanatory text for Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM(90) 314 final—SYN 287, p.29. The forerunner to Art. 15(1) granted a person the right 'not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality' (Art. 14(1) of the 1990 Proposal). These provisions were then changed in the 1992 Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422 final—SYN 287) such that a person was granted a right 'not to be subjected to an administrative or private decision adversely affecting him which is based solely on automatic processing defining a personality profile' (Art. 16(1)).

> human decision-maker may attach too much weight, thus abdicating his own responsibilities.[25]

Yet, reading between the lines of these explanatory statements, we can discern not just fear about humans letting machines make mistakes but a concern to uphold human dignity by ensuring that humans (and not their 'data shadows') maintain the primary role in 'constituting' themselves.[26]

Similar concerns undoubtedly animate GDPR Art. 22.[27] However, the discussions on various proposals for its provisions prior to the final adoption of the Regulation focused more on profiling *per se* than was the case with DPD Art. 15. While the final wording of GDPR Art. 22 does not exactly mirror any one of the proposals from the Commission, Parliament or the Council, all of the proposals targeted profiling, along with automated decisions. The Parliament's Committee on Civil Liberties, Justice and Home Affairs went the furthest here in that it wanted to give individuals a right to object to all profiling and not just particular types of decisions that might arise from profiling.[28] Yet, all three institutions were of the view that some decisions based on profiling should be subject to relatively stringent regulation, namely the decisions based on sensitive data as specified in GDPR Art. 9.

The pronounced focus on profiling is reflected in the title of Art. 22 along with the use, in its provisions, of the term 'profiling' instead of the longer phrase 'automated processing of data intended to evaluate certain personal aspects relating to him', used in DPD Art. 15(1). The term 'profiling' also receives its own definition in GDPR Art. 4(4) (set out further below).

Lastly, the protection of children deserves mention. The status of children as data subjects received much more attention in the drafting of the GDPR than in the drafting of the DPD. This attention extends to the realm of profiling. Thus, Recital 38 in the preamble to the GDPR states that 'specific protection' of personal data on children 'should, in particular, apply to the use of . . . [such data] for the purposes of . . . creating personality or user profiles', while Recital 71 states that a measure

[25]COM(92) 422 final—SYN 287, p. 26.

[26]See also Bygrave (2001), p. 18; Bygrave and Berg (1995), p. 32. Cf. recital 2 in the preamble to the Directive ('Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms . . . and contribute to . . . the well-being of individuals').

[27]They are reflected in the preamble to the GDPR. In particular, Recital 71 evidences concern about the potentially poor quality of fully automated decision-making processes, with emphasis put on the need 'to ensure, in particular, that factors which might result in inaccuracies in personal data are corrected and the risk of errors is minimised'. Recital 71 also stresses the need 'to secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of' the categories set out in Art. 9(1).

[28]European Parliament (2013), p. 93 (outlining proposed Art. 20(1)). However, two other committees in the Parliament, namely the Committee on Internal Market and Consumer Protection (IMCO) and the Committee on Industry, Research and Energy (ITRE), were friendlier to profiling than the Committee on Civil Liberties, Justice and Home Affairs (which had the lead role in negotiating the GDPR). See further European Parliament (2013), p. 308, 309, 471, 472.

involving the making of an automated decision based on profiling 'should not concern a child'.[29] While these statements in the Recitals do not create on their own a legally binding prohibition on profiling measures directed at children,[30] they will likely increase the stringency with which the provisions of Art. 22 are construed and applied in respect of such measures (e.g., in the interpretation of what decisions may qualify as having a 'significant' effect (Art. 22(1)), in disfavour of controllers.

4 Mechanics and Semantics of GDPR Art. 22

Article 22 is structured similarly to DPD Art. 15, albeit with some differences. The first paragraph provides (on its face) a right; the second paragraph provides exceptions to that right, while the third paragraph qualifies two of those exceptions by adding requirements to them. The last paragraph introduces a further qualification to all of the exceptions provided in paragraph 2, this qualification taking the form of a prohibition on automated decisions based on special categories of data—a prohibition not contained in Art. 15.

4.1 GDPR Art. 22(1)

So far, GDPR Art. 22(1) has been characterised as providing a particular *right*. This characterisation is not entirely accurate, insofar as it connotes a right that shall be exercised at the discretion of the right holder. Whereas several other rights in the Regulation obviously require the data subject as right holder to exercise them—these include the right to object to the processing of personal data (Art. 21), the right to data erasure (Art. 17) and the right to data rectification (Art. 16)—Art. 22(1) is different, as the data subject here does not have the right *to* something but the right *not to* be subject to a particular type of decision. This distinction, combined with the consent derogation in Art. 22(2), suggests that Art. 22(1) is intended as a prohibition and not a right that the data subject has to exploit. Yet, Art. 22(1) invokes the

[29]Children are also singled out in respect of the right to data erasure. Recital 65 states that such a right is 'relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the Internet'.

[30]Recitals are not legally binding. Thus, they do not create rights or obligations that are contrary to, or not inherent in, the Articles: see, e.g., CJEU, *Giuseppe Manfredi v. Regione Puglia*, Case C-308/97, Judgment of 25 November 1998, paras. 29–30; CJEU, *Criminal Proceedings against Nilsson, Hagelgren & Arrborn*, Case C-162/97, Judgment of 19 November 1998, para. 54.

language of 'right'. Article 22(4), by contrast, states that automated decisions 'shall not' be based on special categories of data.[31] It could be argued that the lawmakers would have formulated Art. 22(1) more like Art. 22(4) if the right was not to be exercised by the data subject. Moreover, Art. 22 is placed in the chapter of the GDPR that is termed 'rights of the data subject', and other provisions (e.g., Art. 12 (2)) refer to 'the exercise of data subject rights under Article ... 22'. On the other hand, the title of Art. 22 is not expressed as a 'right', unlike the titles of Arts. 15–18, 20–21.

Looking back at DPD Art. 15(1), this also does not take the form of a direct prohibition on a particular type of decision making but directs each EU Member State to confer on persons a right to prevent them being subjected to such decision making. Some states, however, chose to transpose Art. 15(1) by introducing a (qualified) prohibition on the targeted decision making.[32] Other states have simply provided persons with the opportunity to exercise such a right, leaving the actual exercise of the right to the discretion of each person and thereby permitting the targeted decision making to occur in the absence of the right being exercised (provided, of course, that the data-processing operation involved in the decision making meets the other requirements of the Data Protection Directive and of national laws implementing that Directive).[33] Yet other states have adopted a hybrid approach, creating a prohibition for some types of decision and a right to object to other types.[34] While this variation was not surprising—and perhaps even intended by the Data Protection Directive's architects—it runs against the grain of the GDPR, which as a regulation is intended to achieve a much more complete degree of harmonisation than that brought about by the DPD. Thus, it is unlikely that Art. 22(1) may be treated by some states as a prohibition and by other states as a right. This is especially so given that the practical consequences of treating it as one or the other are significantly different.

Treating Art. 22(1) as a right to object renders its effect dependant on action by the data subject, at least for decisional processes that do not fall within the three categories of derogation in the second paragraph. This is clearly a weaker result from a privacy and data protection perspective than if Art. 22(1) is treated as a prohibition. In the latter case, those decisional processes not falling within the

[31]Cf. Art. 11(1) of Directive (EU) 2016/680 – supra n. 22– which operates expressly as a prohibition.

[32]The case, for instance, in Belgium: see Art. 12bis of the 1998 Belgian data protection legislation (*Wet tot omzetting van de Richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de Bescherming van Natuurlijke Personen in verband met de Verwerkung van Persoonsgegevens en betreffende de Vrij Verkeer van die Gegegevens, van 11 december 1998; Loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlament Euroéen et du Conseil relative à la Protection des Personnes Physiques à l'égard du Traitement de Données à Caractère Personnel et à la Libre circulation des ces Données, du 11 decembre 1998*).

[33]As has been done, e.g., in Norway: see s. 25 of the Personal Data Act of 2000 (*lov om behandling av personopplysninger av 14. april 2000 nr. 31*).

[34]The case with Italy: see Art. 14 of the Personal Data Protection Code of 2003.

paragraph two derogations are prohibited regardless of the action or inaction of the data subject, effectively allowing only those decisional processes specified in paragraph two (subject to the qualifications in the third and fourth paragraphs). Such a result conforms better than the former result to the overarching aim of Art. 22—and, indeed, of the Regulation more generally—to safeguard privacy and data protection as fundamental human rights in the face of technological and other developments.[35] Further, if the right in Art. 22(1) is to be exercised by the data subject, it would effectively function as a right to ensure human involvement in the decision making concerned. This would render superfluous the safeguard of 'human involvement' that is provided in Art. 22(3) as a prerequisite for applying two of the derogations to Art. 22(1). Thus, from both a logical point of view and a more teleological perspective rooted in concern for privacy and data protection as fundamental rights, it makes most sense to conclude that the apparent right provided by Art. 22(1) does not have to be exercised by the data subject. The 'right' most likely functions as a (qualified) prohibition with which the decision maker has to comply regardless of whether the 'right holder' invokes it or not.

Turning to the substantive content of the first paragraph of Art. 22, we see that the 'right' it provides consists of four conditions. Three of these conditions are similar to those in the DPD: (1) a decision is made that is (2) based solely on automated processing and (3) has either legal effects or similarly significant consequences. The fourth condition is, on its face, quite different: the basis for the decision must have been 'automated processing, including profiling', whereas the equivalent phrasing in DPD Art. 15(1) is 'automated processing of data intended to evaluate certain personal aspects' relating to the data subject.

The first three-listed conditions are dealt with relatively briefly in the following as they have already been comprehensively analysed in scholarship on DPD Art. 15. The condition that a decision is made means essentially that a particular attitude or stance is taken towards a person and this attitude/stance has some degree of binding effect in the sense that it is likely to be acted upon. It follows from the rationale for the provisions that the decisional process may consist entirely of responses on the part of computer software.

This leads to the second condition which is that the decision is based solely on automated data processing. By this is meant that a person fails to exercise any real influence on the outcome of the decision-making process. Even if a decision is formally ascribed to a person, it is to be regarded as based solely on automated processing if a person does not actively assess the result of the processing prior to its formalisation as a decision. Conversely, an automated process may fall clear of Art. 22 when it remains a decisional *support* tool for a human being, and the latter considers the merits of the results of that process prior to reaching his or her decision, rather than being blindly or automatically steered by the process.[36] At the

[35]Further on this aim, see, e.g., Recitals 1, 6, 11 and 71 in the preamble to the GDPR.

[36]See also COM(92) 422 final—SYN 287, p. 26: 'what is prohibited is the strict application by the user [data controller] of the results produced by the system. Data processing may provide an aid to decision-making, but it cannot be the end of the matter; human judgement must have its place.

same time, the fact that a large or even predominant part of the decisional process is automated will not attract the application of Art. 22.[37]

Another issue in relation to the second condition is the data basis for the processing. On its own, the term 'automated processing' suggests on its face that the decision need not be based on personal data that relates to the data subject targeted by the decision; it could accordingly encompass non-personal data or personal data relating to other persons. Ultimately, however, there must be processing of some personal data. This follows, at least partly, from the reference to 'including profiling' directly after the reference to 'automated processing': as shown further on, 'profiling' is defined as an activity involving automated processing of *personal* data (GDPR Art. 4(4), set out fully below). While the data involved in the profiling probably need not relate, at least initially, to the person targeted by the decision, Art. 22(1) presumes that the decision will ultimately involve processing of data on that person as the right/prohibition it provides is operationalised by reference to the 'data subject'.

The third condition—that the decision has legal effects or similarly significant consequences—means that the decision either alters or determines (partly or fully) a person's legal rights or duties, or it has consequences that are, at the very least, more than trivial for a person's welfare. While such consequences probably need not be entirely adverse for the person, it is clear that the more adverse they are, the greater the chance they may properly be deemed significant. Recital 71 in the preamble to the Regulation mentions the refusal of 'online credit applications' and 'e-recruiting practices' as two examples of automated decisions with significant

---

It would be contrary to this principle, for example, for an employer to reject an application from a job-seeker on the sole basis of his results in a computerized psychological evaluation, or to use such assessment software to produce lists giving marks and classing job applicants in order of preference on the sole basis of a test of personality'. See too the judgment of the German Federal Court of Justice in the so-called SCHUFA case concerning the use of automated credit-scoring systems: judgment of 28 January 2014, VI ZR 156/13. Here, the court held, on appeal, that the credit-scoring system fell outside the ambit of the German rules that transpose DPD Art. 15 (the relevant provisions are found in §6a of Germany's Federal Data Protection Act 1990 (*Bundesdatenschutzgesetz – Gesetz zum Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20 Dezember 1990*)), as amended) because the automated elements of the decisional process pertained to the preparation of evidence; the actual decision to provide credit was made by a person. In the words of the court: 'Von einer automatisierten Einzelentscheidung kann im Falle des Scorings nur dann ausgegangen werden, wenn die für die Entscheidung verantwortliche Stelle eine rechtliche Folgen für den Betroffenen nach sich ziehende oder ihn erhebliche beeinträchtigende Entscheidung ausschließlich aufgrund eines Score-Ergebnisses ohne weitere inhaltliche Prüfung trifft, nicht aber, wenn die mittels automatisierter Datenverarbeitung gewonnenen Erkenntnisse lediglich Grundlage für eine von einem Menschen noch zu treffende abschließende Entscheidung sind': para. 34.

[37]Cf. the European Parliament Committee on Civil Liberties, Justice and Home Affairs proposed provisions to capture profiling when it is based 'solely *or predominantly* on automated processing' (proposed Art. 20(5)): European Parliament (2013), p. 94. The omission of any reference to 'predominantly' in the final version of Art. 22(1) and, indeed, in Recital 71 underlines that 'solely' is the sole operative criterion.

consequences. It also suggests other measures that the decision maker should avoid to have a fair and transparent processing, such as decisions with discriminatory effects based on racial and ethnic origins, political opinions, religion and other beliefs, health status and sexual orientation. Recital 38 in the preamble intimates too that if the automated decision targets a child, it would also be considered significant.

Some decisions covered by Art. 22(1) may have both positive and negative facets, as, for example, when a person is granted a higher credit limit from a bank but not as high as she has requested. At the same time, it bears emphasis that the wording of Art. 22(1) is slightly changed from its predecessor: whereas DPD Art. 15(1) does not draw a link between significant consequences ('significantly affects') and 'legal effects', Art. 22(1) does draw this link by inserting 'similar' before 'significant consequences'. This may signal an intention that such consequences must have a non-trivial impact on the *status* of a person relative to other persons—just as legal effects typically do. In respect of DPD Art. 15(1), it has been claimed that the consequences probably need not be pecuniary.[38] It has also been claimed that a significant consequence might arguably lie 'merely in the insult to a data subject's integrity and dignity which is occasioned by the simple fact of being judged by a machine, at least in certain circumstances (e.g., when there is no reasonable justification for [such decision making])'.[39] The validity of these claims is more tenuous with respect to Art. 22(1) in light of the linkage factor pointed to above. This factor would suggest that significant consequences cannot be entirely emotional. In addition, it reinforces some scholars' doubts—expressed in relation to Art. 15—that targeted advertising will ordinarily generate significant consequences.[40] Nonetheless, it is not inconceivable that such consequences will arise because of Art. 22(1) if the advertising involves blatantly unfair discrimination in the form of web-lining and the discrimination has non-trivial economic consequences (e.g., the data subject must pay a substantially higher price for goods or services than other persons)[41]—*a fortiori* if this occurs repeatedly.

The fourth condition—that the decision must have a basis in 'automated processing, including profiling'—also presents interpretative challenges. As elaborated further below, these arise not so much with the term 'profiling' as the term 'including'. The former term is defined in Art. 4(4) as follows:

[38]Church and Millard (2010), p. 84.

[39]Bygrave (2001), p. 19; see too Bygrave (2002), p. 322.

[40]See, e.g., Damman and Simitis (1997), p. 220. The Commission seems also to have taken the view that simply sending a commercial brochure to a list of persons selected by computer does not significantly affect the persons under Art. 15(1): COM(92) 422 final—SYN 287, pp. 26–27. This view, though, related to a draft provision expressly requiring an *adverse* effect—a requirement that was omitted from the wording of the final version of Art. 15(1).

[41]See too Vermeulen (2013), p. 12. Vermeulen takes this view from the initial version of the right proposed by the Commission in 2012, but that version had the same structure and mostly the same wording as the current Art. 22(1).

> 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements [. . .]

From this definition, we see that profiling consists of two elements: (1) there must be an automated processing of personal data; and (2) the use of the personal data must be to evaluate certain personal aspects relating to a natural person. The definition also departs from DPD Art. 15(1) in several respects. One difference is that the definition has more examples of what constitutes profiling. It is not limited to performance at work, creditworthiness, reliability, and conduct, but also embraces health, personal preferences, interests, reliability, behaviour, location or movements. This expansion of examples is in line with the focus on profiling in the preparatory works.

Another difference is that the definition does not include the criterion of 'intention' (cf. 'processing of data *intended to* evaluate certain personal aspects': Art. 15 (1)). This reduces the possibility whereby profiles that arise only as an ancillary effect of automated processing fall outside the scope of the provision—a possibility that arguably has hobbled Art. 15(1).[42] However, the omission of an 'intention' criterion is partly offset by the fact that profiling must involve an *evaluation* of personal aspects of a natural person. Thus, situations in which a decision maker merely attempts to profile the data subject without arriving at the evaluation stage would seem to fall outside the scope of the definition.

As for the term 'including', this most likely refers to the condition of automated processing—thus making profiling an element of such processing. Recital 71 in the preamble also suggests that profiling is to be regarded as an element of automated processing: it states that '[s]uch processing includes "profiling"'. Yet, this line is not without problems as Art. 4(4) defines profiling as a type of automated processing. Given that definition, the reference in Art. 22(1) to 'automated processing' is superfluous. Might it not then be better to view the term 'including profiling' as intended to separate profiling from automated processing, thus making profiling an independent alternative to the need for a decision? This possibility is arguably reinforced by the use of commas to encapsulate the term in Art. 22(1) and by the title of Art. 22 as a whole ('Automated individual decisions, including profiling'). Such a possibility does not arise with DPD Art. 15 which makes clear the need for a decision and combines the condition of an automated process with that of profiling, meaning that the decision has to be based, in effect, on a profile.

However, the consequences of treating profiling as an independent criterion for applying Art. 22 jar with the rationale and background for the provisions. Adopting the approach would make Art. 22 broader in scope than DPD Art. 15. Virtually all automated decisions targeting a person would fall within its ambit (assuming that the criteria of legal effect and significant consequences are also met)—the case,

[42] Savin (2014), p. 4.

e.g., with an automated teller machine's rejection of an attempt to take out cash. As highlighted above, the preparatory works of the GDPR focus mainly on the harms of profiling, not all automated decisions targeting a human being. The background for Art. 22 accordingly does not support the use of the condition 'automated processing' without including profiling. Simply put, it makes most sense to treat automated processing as a condition that *necessarily involves* profiling. Nothing in the preamble or preparatory works runs counter to this approach. In this regard, it is worth recalling that a proposal from the European Parliament Committee on Civil Liberties, Justice and Home Affairs for regulating profiling individually without the necessity of an automated decision was expressly abandoned in favour of an approach more in line with DPD Art. 15. Further, while treating profiling as a constituent of automated processing renders the reference in Art. 22(1) to 'automated processing' superfluous, this problem is easier to tolerate than the scoping problem with the alternative approach.

4.2 Derogations to Art. 22(1)

Article 22 operates with three categories of derogation from the right/prohibition provided in its first paragraph: (1) contract (Art. 22(2)(a) and 22(3)); (2) authorisation by EU or Member State law (Art. 22(2)(b)); and (3) data subject consent (Art. 22(2)(c) and 22(3)). These derogations replicate, augment and to some extent tighten the derogations provided by DPD Art. 15(2). The European Data Protection Board that will replace the Working Party on the Protection of Individuals with regard to the Processing of Personal Data is specifically tasked with publishing 'guidelines, recommendations and best practices' on how the Art. 22(2) derogations are to be construed and exercised (Art. 70(1)(f)). At the time of writing this chapter, such guidance has not been issued.

Dealing with the contractual derogation under Art. 22 in more detail, the main difference between it and its predecessor in the DPD is that its application is subjected to the imposition of 'suitable measures' that involve, as a minimum, the right of the data subject 'to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision' (Art. 22(3)). These sorts of measures were not required as part of the contractual derogation under DPD Art. 15(2)(a). The latter permits a fully automated decision based on profiling where the decision is taken in the course of entering into or executing a contract, *and either* the data subject's request for the entering into or execution of the contract has been fulfilled, *or* provision is made for 'suitable measures' to safeguard the person's 'legitimate interests'. The derogation has been duly criticised for operating with a fallacious assumption that fulfilment of a person's request to enter into or execute a contract will never be problematic for that person.[43]

[43]Bygrave (2001), p. 21; Bygrave (2002), p. 327.

Another difference that tightens the contractual derogation is the addition of an explicit necessity criterion—i.e., the decision must be 'necessary for entering into, or performance of, a contract' (Art. 22 (2)(a)). This criterion is not elaborated in the preamble or preparatory works, but it indicates at least that the automated decision must have been *required* for entering into or fulfilling the contract with the data subject. The Data Protection Directive also envisages a connection between the decision and the contract (i.e., the decision must have been made 'in the course of' the contractual process: Art. 15 (2)(a)), but the Regulation expresses this connection more stringently. At the same time, the necessity criterion cannot be applied so stringently that it functions as one of indispensability: it is hard to think of an example where an automated decision *has* to happen without human involvement. The rationale behind the criterion is presumably to make it difficult for the data controller to escape Art. 22(1) by merely pointing to a standardised contract with the data subject.

The last significant difference is that Art. 22 removes the condition in DPD Art. 15(2)(a) that the data subject must have been the one to request the contract. This widens the scope of the derogation as it becomes applicable also to contracts that the data controller requests. Yet, the additional condition of 'suitable measures' in Art. 22(3) has been expanded, which gives the data subject a higher level of protection overall.

Elaborating on the condition of 'suitable measures', its wording builds on that of DPD Art. 15(2)(a) but is augmented by references to 'the data subject's rights and freedoms' (in addition to his/her 'legitimate interests') and by more exemplifications of what the measures entail. Whereas Art. 15(2)(a) refers only to arrangements allowing a data subject 'to put his point of view', the GDPR mentions additionally the right 'to obtain human intervention' and the right 'to contest the decision'. These are rights that the data controller has the obligation to facilitate. All up, these rights (particularly that of human involvement) mean that there will be insignificant difference in the level of protection between the right/prohibition in Art. 22(1) and the exceptions. Put simply, the contractual derogation ends up having scant benefits for data controllers in facilitating automated decisions based on profiling. The right to human involvement also undercuts the utility of the prohibition in Art. 22(4) on fully automated decisions based on special categories of data. This prohibition appears to be largely protected *de facto* through paragraph three.

The rights listed in Art. 22(3) are not an exhaustive exemplification of 'suitable measures', but a list of minimum requirements. This raises the question as to what other rights may be invoked by a data subject in this context. The only other right that might benefit a data subject here would be a right to be given an explanation for an automated decision after it is made. Express mention of this right in the Regulation occurs solely in Recital 71, which lists the right in its elaboration of 'suitable safeguards'.[44] However, a Recital does not of itself create a legally binding right;[45]

[44]The European Parliament Committee on Civil Liberties, Justice and Home Affairs also listed such a right in its proposed Art. 20(5) of the draft Regulation: European Parliament (2013), p. 94.

[45]Supra n. 30 and references cited therein.

the latter may only be created pursuant to an Article. As already noted, Art. 22 omits express reference to a right of explanation. Further, some scholars argue that the provisions concerning controllers' notification duties (Arts. 13 and 14) and data subjects' access rights (Art. 15) deal with supply of information *prior* to an automated decision being made, and that this information concerns *ex ante* explication, in fairly general terms, of system functionality (covering factors, such as the logic of the decision tree that is used and the categories of data that are considered), not *ex post* explanation of a particular decision.[46] These scholars accordingly conclude that a right of *ex post* explanation of automated decisions is not supported by the Regulation.

While this conclusion has some merit, it fails to consider several factors that undermine it. First, the wording of Art. 15 does not *necessarily* exclude the possibility that it embraces a right of *ex post* explanation of an Art. 22 type decision. The fact that one has a right to information about the 'existence' of automated decision making suggests that such decisions already take place. Further, the reference in Art. 15 to supply of information regarding the 'significance and envisaged consequences' of such decision making could point to the practical consequences of an already taken decision which are viewed by the controller as likely to follow from that decision.[47] Much depends here on what parts of a decisional process are to be regarded as giving rise to a decision under Arts. 22 and 15. For example, if a bank makes a fully automated decision as to a person's creditworthiness and the decision is in the form of a particular credit score that the bank supplies to the person, the 'envisaged consequences' that a bank would have to supply information about (pursuant to the person exercising his/her information access right) would be that the data subject will not be able to get a particular type of loan if he/she applied for it.

Moreover, we should not discount the possibility that a right of *ex post* explanation of automated decisions is implicit in the right 'to contest' a decision pursuant to Art. 22(3). The term 'contest' connotes more than 'object to' or 'oppose'; simply put, a right of contest is not simply a matter of being able to say 'stop', but is akin to a right of appeal. If such a right is to be meaningful, it must set in train certain obligations for the decision maker, including (at the very least) an obligation to hear and consider the merits of the appeal. If the appeal process is to be truly fair, it must

[46]See especially Wachter and others (2017). Articles 13(2)(f), 14(2)(g) and 15(1)(h) all concern the supply of 'meaningful information about the logic involved [in automated decision-making], as well as the significance and envisaged consequences of such processing for the data subject', albeit in different contexts.

[47]However, the provisions of Art. 13—which concern supply of information about processing when the data have been obtained from the data subject—are best understood as only concerned with supply of information prior to an automated decision being made. This follows from the fact that the supply of information shall occur 'at the time when personal data are obtained' (Art. 13 (2)). Article 14—which concerns supply of information where personal data have been obtained from other sources than the data subject—does not operate with the latter delimitation. Nor does Art. 15.

additionally carry a qualified obligation to provide the appellant with reasons for the decision.[48] The need to give reasons is buttressed by the general principle of 'lawfulness, fairness and transparency' in Art. 5(1)(a) which animates most of the basic norms of the Regulation, including the provisions of Art. 22. This is not to say that the giving of reasons is an absolute requirement. Similar to, say, the right of data subject access, an obligation to give reasons may be trumped by other legitimate rights and interests (see generally Art. 23). Concomitantly, the stringency of the obligation will depend on the weighing up of various factors, such as the seriousness of the effects of the decision on the data subject, the degree to which the decision or the system giving rise to it has Kafkaesque qualities, and the extent to which the giving of reasons would unduly prejudice the legitimate interests and rights of the decision maker (for example, with respect to protection of intellectual property rights).

Turning to the derogation for consent in Art. 22(2)(c), this is new: under DPD Art. 15, consent from the data subject does not qualify as an exception.[49] The consent derogation must be construed in light of the definition of consent provided in Art. 4(11):

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Under Art. 22, the data subject must have been informed about the automated decision making and profiling,[50] in addition to giving a specific and unambiguous consent to this. At the same time, the criterion 'freely given' is elaborated on by Art. 7(4):

> When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

The problem of conditional offers (which create 'take-it-or-leave-it' situations) must figure in the assessment of whether the consent is freely given under Art. 22. As part of this assessment, Art. 7(4) states that one should examine whether the data

[48]The notion of 'fair' here builds primarily on the dual principles identified by Galligan (1996), p. 419: 'one is that people ought to know how they will be treated by those holding power over them; the other is that people ought to be treated equally in the sense that the criteria are applied generally and consistently.' The giving of reasons rests on both these principles. It is, at the same time, rooted in several interlinked interests, including a relatively technocratic concern about the quality of decision making (e.g., ensuring the reduction of decisional error and unwarranted bias: see further Galligan (1996), pp. 431–433) and a more dignitarian concern related to treating persons with respect. In terms of the latter, '[g]iving reasons expresses respect just as a refusal or failure to do so—where the failure evinces disregard for a person's opinion of the justice of his treatment—expresses contempt': Allan (1998), p. 500; see too Galligan (1996), p. 433.

[49]Ireland, however, has operated with such an exception (see s. 6B(2)(b) of Ireland's Data Protection (Amendment) Act 2003), but it has been the only country in Europe to do so.

[50]This follows also from Arts. 13(2)(f), 14(2)(g) and 15(1)(h).

processing is actually 'necessary' for the realisation of the contract or service provided. Applying this to Art. 22(2)(c), one should ask whether a conditional automated decision is actually necessary for the offered services. This assessment is similar to the above-noted assessment of 'necessity' under Art. 22(2)(a).

It is difficult to draw the line for when automated decisions are necessary, and it will ultimately be left to courts to clarify. However, the interest the data subject has in the automated decision is likely to be a factor in the assessment. It is easier to argue that consent is freely given if the automated decision is in the interest of the data subject, such as in the situation of loan applications and insurance underwriting. It is harder to imagine that consent is given freely for price differentiation.

Article 22(2)(c) does not mention whether the consent can be withdrawn for future automated decision making. Article 7(3), however, stipulates that consent may be withdrawn at any time, and Art. 22(2)(c) should consequently be interpreted in the same manner.

To sum up the effect of Art. 22(3)(c), the derogation in itself widens the possibility of profiling and automated individual decisions, relative to the DPD. However, the derogation does not apply in isolation, as the data controller still needs to put in place suitable measures to safeguard the data subject, including the right of human involvement under Article 22(3).

As for the derogation in Art. 22(2)(b)—allowing for automated decisions pursuant to member state law—this essentially replicates DPD Art. 15(2)(b). We are not aware of any national laws that specifically take advantage of this derogation. Nonetheless, Art. 22(2)(b) opens up for a great deal of nationally authorised automated decisional processes with potentially differing standards being applied from country to country, thereby undermining the harmonisation aims of the Regulation. Moreover, although the national legislation concerned must provide 'suitable safeguards' for the data subjects, these do not—at least as a point of departure—have to include the safeguards specified in Art. 22(3). However, there are likely to be multiple contexts in which at least some of the Art. 22(3) safeguards qualify as 'suitable safeguards' under Art. 22(2)(b).

4.3 Prohibition on Decisions Based on Sensitive Data

The fourth and final paragraph of Art. 22 provides a qualified prohibition on decisions 'referred to in paragraph 2' when they are based on special categories of data as regulated by Art. 9(1). Paragraph 2 refers to the automated decisions in the first paragraph. The reason the prohibition refers to paragraph 2 and not paragraph 1 is presumably to stress that the prohibition takes precedence over the exceptions.

Article 9(1) gives a list of personal data categories considered to be special: racial and ethnic data, political opinions, religious and philosophical beliefs, trade union membership, health, sex life, sexual orientation, and genetic and biometric data in uniquely identifying a natural person. The list replicates and supplements the list contained in DPD Art. 8.

The new prohibition does not come without possibilities for derogation. There are two possible exceptions to the ban, namely explicit consent from the data subject for one or more specific purposes under Art. 9(2)(a), or when such automated decisions are necessary for reasons of substantial public interest and have a basis in EU or Member State law under Art. 9(2)(g). Regarding the latter exception, relevant laws are not yet in place (to our knowledge), yet the exception augments the potential – already inherent in Art. 22(2)(b)) – for differing national regimes for automated decision making. As for the former exception, explicit consent in Art. 9 (2)(a) must be interpreted in the same manner as in Art. 7, as accounted for in the previous subsection. The application of 'suitable measures' to safeguard data subject rights, freedoms and interests is also obligatory for derogations under Art. 22(4), similar to the exceptions in the second paragraph. While Art. 22(4) does not spell out what these measures involve, they are presumably to be interpreted in the same manner as discussed in the previous subsection and will thus include human intervention in the decision making. If such intervention is 'at least' required of the data controller with respect to decisions based on ordinary personal data, it should also be a safeguard when decisions are based on sensitive data.

5 Conclusion

Article 22 bears a great deal of similarity with its predecessor in DPD Art. 15, particularly in respect of the right/prohibition it provides. Application of the right/prohibition still involves meeting multiple criteria, so it still resembles a house of cards. Yet, to a greater degree than Art. 15(1), Art. 22(1) is afflicted by clumsy syntax that not only muddies its interpretation but threatens to unravel the connection between decision making and profiling inherent in Art. 15(1).

The biggest difference between DPD Art. 15 and GDPR Art. 22 lies not in the scope of the right/prohibition that each posits but in the possibilities of derogations from the right. First, the new exception of explicit consent encompasses the automated decisions that have not already been derogated through a contract. Automated decisions with the possibility of discriminatory effects, such as weblining, which are potentially hit by DPD Art. 15, might qualify for inclusion under the exception for consent. The prohibition provided by Art. 22(4) also can be derogated from by obtaining explicit consent. It is standard practice, at least in the internet context, for companies to prompt data subjects to consent to various data-processing operations.[51] The new exception for consent is likely to lower the *de facto* level of protection for individuals, particularly in light of the relative strength of most individuals *vis-à-vis* banks, insurance companies, online service providers and many other businesses. However, the GDPR tightens the assessment of what is a freely given consent and what automated decisions are necessary for entering into

[51]See, e.g., Bygrave (2015), pp. 31–32.

or performance of a contract. The traction of this tightening will rest on how strictly the necessity criterion is interpreted.

The level of protection under Art. 22 will also depend on what safeguards the data controller is obliged to put in place under Art. 22(3). Here, Art. 22 offers a higher level of protection than the DPD, as the data subject will *always* have the right to demand manual re-examination of the decision. This might take away the incentive for companies to acquire either a contract or consent from the data subject, as neither move will necessarily work as an exception to the right/prohibition in Art. 22(1). On the other hand, if persons only rarely make use of their rights under Art. 22(3), the overall effect of Art. 22 on the automation of business might well end up being negligible—just as it has been with DPD Art. 15.

Finally, the traction of Art. 22 will likely be weakened by practical difficulties in implementing its requirements, particularly when applied to decisional systems that are extremely complex and opaque, also for the controller(s). As a recent editorial asks:

> in practice, how can informed consent be obtained in relation to a process that may be inherently non-transparent (a "black box")? Even if an algorithmic process can in theory be explained, what if it is impossible to do that in a way that is intelligible to a data subject?.[52]

These sorts of challenges afflict not just Art. 22 but many of the other provisions in the GDPR as well, particularly those aimed at ensuring or enhancing transparency of data processing. Yet, such difficulties are most damaging for the aspirations behind Art. 22 as it is specifically algorithm-driven 'black-box' decision making that Art. 22 is aimed at controlling.

References

Allan TRS (1998) Procedural fairness and the duty of respect. Oxf J Leg Stud 18:497–515

Andrews L (2011) I know who you are and I saw what you did. Social networks and the death of privacy. Free Press, New York

Borgesius FJZ (2015) Improving privacy protection in the area of behavioural targeting. Kluwer Law International, Alphen aan den Rijn

Bosco F, D'Angelo E, Vermeersch E (2015) National data protection authorities' views on profiling. In: Creemers N, Guagnin D, Koops BJ (eds) Profiling technologies in practice. Wolf Legal Publishers, Oisterwijk, pp 21–46

Bygrave LA (2001) Minding the machine: Article 15 of the EC data protection directive and automated profiling. Comput Law Secur Rev 17:17–24

Bygrave LA (2002) Data protection law: approaching its rationale, logic and limits. Kluwer Law International, Alphen aan den Rijn

Bygrave LA (2014) Data privacy law: an international perspective. Oxford University Press, Oxford

Bygrave LA (2015) Internet governance by contract. Oxford University Press, Oxford

Bygrave LA, Berg JP (1995) Reflections on the rationale for data protection laws. In: Bing J, Torvund O (eds) 25 years anniversary anthology in computers and law. Tano, Oslo, pp 3–39

[52]Kuner and others (2017), p. 1.

Church P, Millard C (2010) Comments on the data protection directive. In: Büllesbach A, Gijrath S, Poullet Y, Prins C (eds) Concise European IT law, 2nd edn. Kluwer Law International, Alphen aan den Rijn, pp 83–85

Damman U, Simitis S (1997) EG-Datenschutzrichtlinie: Kommentar. Nomos, Baden-Baden

European Parliament (2013) Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))(A7-0402/2013; PE501.927v05-00)

Faliagka E, Tsakalidis A, Tzimas G (2012) An integrated e-recruitment system for automated personality mining and applicant ranking. Internet Res 22:551–568

Galligan DJ (1996) Due process and fair procedures. A study of administrative procedures. Clarendon Press, Oxford

Hildebrandt M (2008) Defining profiling: a new type of knowledge? In: Hildebrandt M, Gutwirth S (eds) Profiling the European citizen. Springer, Dordrecht, pp 17–47

Kuner C, Svantesson DJB, Cate FH, Lynskey O, Millard C (2017) Machine learning with personal data: is data protection law smart enough to meet the challenge? Int Data Priv Law 7: 1–2

Leon PG, Cranshaw J, Cranor LF, Graves J (2012) What do online behavioral advertising privacy disclosures communicate to users? In: Proceedings of the 2012 ACM workshop on privacy in the electronic society. Association for Computing Machinery (ACM), New York, pp 19–30

Savin A (2014) Profiling and automated decision making in the present and new EU data protection frameworks. Copenhagen business school open archive. http://openarchive.cbs.dk/handle/10398/8914. Accessed 1 May 2017

Stepanek M (2000) Weblining. Business Week 3 April: pp EB26–EB34

Vermeulen M (2013) Regulating profiling in the general data protection regulation: an interim insight into the drafting of Article 20. 1 September 2013, EMSOC project (User empowerment in a social media culture), Brussels, http://emsoc.be/wp-content/uploads/2013/11/D3.2.2-Vermeulen-Emsoc-deliverable-profiling-Formatted1.pdf. Accessed 1 May 2017

Wachter S, Mittelstad B, Floridi L (2017) Why a right to explanation of automated decision-making does not exist in the general data protection regulation. Int Data Priv Law 7:76–99

Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (1998) Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. Working Document adopted 24 July, 1998, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf. Accessed 1 May 2017

Part II
Effective Consumer Protection in the Digital Age

Chapter 5
Regulating Contracts for the Supply of Digital Content: The EU and UK Response

Paula Giliker

Abstract This chapter examines the 2015 proposal of the European Commission for a directive on contracts for the supply of digital content and compare the proposed measure with that already enacted in the United Kingdom in Part 1 of its Consumer Rights Act 2015. In drafting the directive, the Commission was conscious of the fact that some European Member States, such as the United Kingdom, had already started enacting their own legislation relating to contracts in this field. Nevertheless, the proposal is for maximum harmonisation. This chapter engages in a detailed examination of the directive and contrasts it with the UK Consumer Rights Act 2015. It also examines the implications of the UK's decision to leave the European Union and whether the Directive (if implemented) is likely nevertheless to have some influence on UK law (and vice versa).

1 Introduction

On 9 December 2015, the European Commission (Commission) published two proposals for directives regulating European consumer law. The first, and the topic of this chapter, concerned business to consumer (B2C) contracts for the supply of digital content (the proposed Supply of Digital Content Directive).[1] The second proposal dealt with consumer contracts concerning the online and other distance sale of goods (the proposed Online Sale of Goods Directive).[2]

[1]Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM (2015) 634 final. This chapter will utilise the original wording of the Directive. This has, however, been subject to suggested amendments at both the European Parliament and Council stages of the legislative process.

[2]Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and distance sales of goods COM (2015) 635 final.

P. Giliker (✉)
School of Law, University of Bristol, Wills Memorial Building, Queens Road, Bristol BS8 IRJ, UK
e-mail: paula.giliker@bristol.ac.uk

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_5

Both would be maximum harmonisation measures, that is, they would preclude Member States from providing any greater or lesser protection than that stated in the directive. To date, it is the proposed Online Sale of Goods Directive (OSG) which has proved to be more controversial, notably because of its decision to draw a line between distance and face-to-face contracts, which is likely to be unpopular with businesses and confusing to consumers. At present, therefore, in view of the obvious disadvantages of a regime confined to online and distance contracts, it is the first proposal which has received the warmest welcome in that it is likely to bring certainty and clarity to an area of contracting to which many modern systems of contract law have been slow to respond, if at all.[3] The Commission has rightly contrasted the importance of digital contracts in our lives with the inability of European contract law regimes to provide specific rules which address the key issues arising in these areas of law which range from when (and how) a contract is made to the need for remedies moulded to meet the requirements of the digital age. This has economic implications. The Commission found that the value of retail e-commerce in the European Union (EU) grew by 13.4% in 2014 reaching a total of €370 billion, but that there was considerable untapped potential, estimating that if barriers related to contract law were lifted, cross-border EU trade could increase by around €1 billion.[4] It also found that 317 million Europeans used the internet in 2014, and, in the age group 15–24, 87% accessed music online and 58% downloaded or played games online.[5] As such, the proposed Supply of Digital Content Directive (DCD or Directive) is a proposal both to be taken seriously and which is capable of providing consumers with a favourable regime of rights together with remedies targeted at the real problems experienced by frustrated consumers.[6]

This chapter will evaluate the proposed Directive. It will consider to what extent it provides a beneficial framework for Member States and the challenges of introducing a maximum harmonisation directive. It will further consider the Directive from the perspective of a regime that has recently introduced its own reforms to contracts for the supply of digital content, namely Part I of the UK Consumer Rights Act 2015 (CRA or Act). The CRA consolidates in one place key consumer

[3]There is a clear divergence across Europe where some States e.g. the UK have legislated in this field, other States e.g. Germany have extended the scope of existing contract rules to include sale of digital content, while other States e.g. France and Poland have at present no explicit rules relating to the supply of digital content.

[4]Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Digital Contracts For Europe—Unleashing the potential of e-commerce, COM (2015) 633 final.

[5]Ibid.

[6]The European Commission reported in 2015 that at least 70 million consumers had experienced one or more problems with just four popular types of digital content (music, anti-virus, games and cloud storage) over the previous 12 months and yet only 10% of consumer received a remedy. Because of these unresolved problems, it estimated that EU consumers had suffered financial and non-financial detriment at around €9-11 billion: European Commission, Digital Contracts for Europe: What is the untapped potential? (December 2015) at http://ec.europa.eu/justice/contract/files/digital_contracts/digital_contracts_factsheet_en.pdf Accessed 19 Mar 2017.

rights covering contracts for goods, services, and digital content, establishing, for the first time, a special regime to deal with the supply of digital content.[7] The Act came into force on 1 October 2015, some two months before the proposed directives (OSD and DCD) were published. The Commission was well aware of the introduction of measures in the UK and of a proposed bill in Ireland dealing specifically with digital content,[8] but this did not distract it from its proposal for a maximum harmonisation directive. Indeed, it found this to be a powerful reason to act swiftly to prevent further fragmentation across the laws of the EU. Nevertheless, for Member States with their own national statutory provisions on contracts for the supply of digital content, the proposed Directive creates a potential conflict between national legislation and the inconsistent provisions of a maximum harmonisation directive. In the light of the decision in the June 2016 referendum that the UK should leave the EU, it might be thought that such a conflict is now of limited interest. Yet, EU law will apply in the UK until it officially leaves and, in view of the importance of contracts for the supply of digital contracts, it remains an open question whether it would be in the UK's interests to persist with provisions that conflict with maximum harmonisation provisions, which may be adopted by the rest of the European Union. As this chapter will indicate, the future of the DCD remains of interest to both EU and UK lawyers whatever future Brexit may bring. It is further submitted that lessons may also be learnt by the Commission regarding the UK's experience in drafting the CRA.

2 Proposed EU Directive on Contracts for the Supply of Digital Content (DCD)

2.1 Background to the Directive

To understand the DCD, it is necessary first to address its background and context. In examining European contract law, we can identify two trends. The first, and least controversial, is the creation of legislation, usually minimum harmonisation directives, which operate in relation to specific areas of the law of contract. Here, the EU has been active, particularly in the consumer contract context, with directives ranging from the 1985 Doorstep Selling Directive to the 2011 Consumer Rights Directive.[9] Such piecemeal legal development may be contrasted with the second

[7] See, generally, Giliker (2017).

[8] See COM (2015) 633 final, p. 3.

[9] See: Council Directive 85/577/EC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises, OJ L 372/31 now replaced by Directive 2011/83/EU of the European Parliament and Council of 25 October 2011 on consumer rights, OJ L 304/64 (Consumer Rights Directive or CRD); Council Directive 90/314/EC of 13 June 1990 on package travel, package holidays and package tours, OJ L 158/59 now replaced by the European

trend that favoured harmonisation of EU contract law because it would benefit cross-border trade if the costs of applying the different contract laws of EU Member States were extinguished. This, it is argued, would provide greater legal certainty and give consumers greater choice arising from the increased willingness of businesses to engage in cross-border transactions together with a clearer set of rights. While the DCD is a targeted directive, its content has been influenced by the fact that it derives not only from trend one but trend two, that is, from proposals for wider harmonisation of European contract law. The idea of a harmonised European law of contract can be traced back to the 1980s and the work of the Lando Commission[10] and its still influential *Principles of European Contract Law* (PECL).[11] The European Parliament has adopted a number of resolutions on the possible harmonisation of substantive private law, and, in 1989 and 1994, called for work to be started on the possibility of drawing up a common European Code of Private law.[12] Following the European Council meeting in Tampere in 1999,[13] the Commission produced three communications that examined the case for EU action in the area of contract law.[14] This led to the decision to fund an academic research

Parliament and Council Directive 2015/2302/EU of 25 November 2015 on package travel and linked travel arrangements, OJ L 326/1, Council Directive 93/13/EC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95/29;, Directive 2008/122/EC of the of the European Parliament and of the Council of 14 January 2009 on the protection of consumers in respect of certain aspects of timeshare, long-term holiday product, resale and exchange contracts, OJ L 33/10, (or Directive 94/47/EC of the European Parliament and the Council of 26 October 1994 on the protection of purchasers in respect of certain aspects of contracts relating to the purchase of the right to use immovable properties on a timeshare basis, OJ L 280/83 depending on the state of transposition), Directive 97/7/EC of the European Parliament and Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144/19 now replaced by the Consumer Rights Directive, Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers, OJ L 80/27, Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests, OJ L 166/51, Directive 1999/44/EC of the European Parliament and Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees OJ L 171/12 (CSD), and Consumer Rights Directive (CRD).

[10]See Lando (1983), Beale (2006).

[11]The work of the Lando Commission was published as Lando and Beale (1999) and Lando et al. (2003). From 1998, its work has been continued by the Study Group on a European Civil Code (SGECC) under the chairmanship of Professor Christian von Bar.

[12]OJ C 158, 26.6.1989, p. 400 (Resolution A2-157/89); OJ C 205, 25.7.1994, p. 518 (Resolution A3-0329/94).

[13]See, in particular, Presidency Conclusions, Tampere European Council 15–16 October 1999, SI (1999) 800, para 39. Note also the resolution of the European Parliament of 16 March 2000 which stated "that greater harmonisation of civil law has become essential in the internal market" and called on the Commission to draw up a study in this area: OJ C 377, 29.12.2000, p. 323 (Resolution B5-0228, 0229 – 0230/2000, p. 326 at point 28).

[14]'Communication from the Commission to the Council and the European Parliament on European Contract Law', COM (2001) 398 final, Communication from the Commission to the European Parliament and the Council 'A more coherent European contract law: An action plan', COM(2003)

project to find a "Common Frame of Reference" which would provide clear definitions of legal terms, fundamental principles and coherent model rules of contract law, drawing on the EU *acquis communautaire* and on best solutions found in Member States' legal orders, finally published as the Draft Common Frame of Reference in 2009.[15] Following public consultation in 2010,[16] in 2011 the Commission published a proposal for a regulation on a Common European Sales Law (CESL).[17] This would not cover the whole of contract law, but would be an optional instrument governing cross-border contracts for the sale of goods and digital content. It sought to provide consumers and small businesses[18] with the opportunity to opt into a self-standing set of contract law rules. The aim was to provide a second contract law regime within the national law of each Member State, which would govern cross-border contracts for the sale of goods, supply of digital content and provision of related services.[19] It received, however, a very mixed reception. Commentators raised criticisms ranging from the scope of the Regulation,[20] its constitutionality[21] and how it would operate in private international law, bearing in mind the existing provisions of the Rome I regulation on applicable law for contracts.[22] After considerable negotiation, this proposal did not receive the approval of the Council of Ministers.

The decision by the Commission in December 2014 in its 2015 Work Programme to withdraw the CESL indicated its acceptance of criticism of an optional regime with a comprehensive set of rules and that a proposal based on more targeted and focused rules would be more likely to gain acceptance.[23] The amendment of CESL by the European Parliament to restrict its scope to online and other distance sales of goods had also provided a strong indication that this should

68 final and Communication from the Commission to the European Parliament and the Council 'European Contract Law and the revision of the *acquis*: The way forward' COM(2004) 651 final.

[15]von Bar and Clive (2009 and 2010)Vols I–VI. The DCFR covered the whole of private law (including moveable property) and was criticised by many as a draft European Civil Code: see, for example, Jansen and Zimmermann (2010).

[16]Green paper from the Commission on policy options for progress towards a European Contract Law for consumers and businesses COM(2010) 348 final.

[17]Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law, COM (2011) 635 final.

[18]The draft Regulation was confined to contracts where the seller of goods or supplier of digital content is a trader and the other party is a consumer or where at least one of the parties is a small or medium-sized enterprise ("SME"). Art. 7 (draft Regulation) defined a SME as a trader which (a) employs fewer than 250 persons; and (b) has an annual turnover not exceeding €50 million or an annual balance sheet total not exceeding €43 million.

[19]COM (2011) 635 final, Explanatory Memorandum, p. 4.

[20]Kornet (2012), Mickitz and Reich (2012), pp. 11–16.

[21]The Commission sought to rely on Article 114 TFEU, but it was questioned because the proposal did not seek to harmonise national law: see Riesenhuber (2012), pp. 5–10. See also Kuipers (2011), Gutman (2014) at 6.4.4.

[22]See Whittaker (2012), Hesselink (2012).

[23]See Commission Work Programme 2015: A New Start Strasbourg, COM(2014) 910 final.

be the targeted area of law.[24] Annex 2 to the Work Programme states that CESL would therefore be replaced by a modified proposal to fully unleash the potential of e-commerce in the Digital Single Market.[25] The Commission indicated that its proposed directives would draw, however, on the experience acquired during the negotiations for CESL and the substance of the CESL itself.[26]

2.2 Why Digital Content?

On 6 May 2015, the Commission set out its strategy to complete the Digital Single Market (Digital Single Market Strategy).[27] It argued that a fully functional Digital Single Market would bring many benefits to European businesses and consumers, promoting innovation, contributing €415 billion to the EU economy each year and creating hundreds of thousands of new jobs.[28] This would entail coordinated EU action, providing a holistic approach to tackling the major obstacles to the development of cross-border e-commerce which would extend from initiatives related to the cross-border portability of content, the role of platforms, the Free Flow of Data, European Cloud, VAT related burdens and parcel delivery. Importantly, the strategy extends to enforcement and redress; a major concern for consumers.[29] The publication of two new directives in December 2015 (OSD and DCD) was a core part of this strategy, which explicitly includes a contract law dimension.[30] These would harmonise key aspects of contract law relating to online and distance sale of goods contracts and contracts for the supply of digital content with the aim of ensuring that traders in the Internal Market are not deterred from cross-border trading by differences in mandatory national consumer contract laws, while providing consumers with a higher level of protection.

The introduction of the DCD is therefore an important part of the Commission's Digital Single Market Strategy and responds to real difficulties experienced at Member State level in determining how to deal with disputes related to defective

[24]See European Parliament Legislative Resolution of 26 February 2014, P7_TA (2014)0159.

[25]See COM(2014) 910 final, Annex 2, p. 12 no 60.

[26]DCD, Explanatory Memorandum, p. 2.

[27]COM (2015) 192 final.

[28]European Commission, Digital Single Market for business and consumers https://ec.europa.eu/growth/single-market/digital_en Accessed 19 Mar 2017.

[29]Namely the entry into operation of the Online Dispute Resolution platform (see Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes, OJ L 165/1, p. 3 and https://webgate.ec.europa.eu/odr/main/index.cfm?event=main.home.show&lng=EN Accessed 19 Mar 2017) and the review of the regulation on consumer protection co-operation (Regulation (EC) No 2006/2004 of the European Parliament and of the Council 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws , OJ L 364, p. 1.

[30]http://ec.europa.eu/priorities/digital-single-market_en Accessed 19 Mar 2017.

digital content.[31] The term "digital content" covers a wide range of items that include the download of music, films, apps, and games, but also matters such as cloud storage and social media services. Applying the ordinary rules of contract law has not always proven straightforward. It is not always clear whether such contracts fall within existing forms of statutory protection. For example in the UK, it was not obvious whether digital products fell within the consumer protection measures of the Sale of Goods Act 1979 or the Consumer Protection Act 1987.[32] Further, a number of legal systems have struggled whether to classify such contracts as sales, services or rental contracts. Consider, for example, cloud computing that permits the consumer to access the supplier's server via the internet; an arrangement that resembles not a sales contract but rather that of a service or even one of rental of premises. Further, remedies appropriate to the sale of physical (tangible) items do not necessarily translate well into the digital marketplace. This causes uncertainty for the business community, but also consumers who have embraced the digital market with enthusiasm. Today, the presence of personal computers, MP3 players, and other digital equipment are a natural part of our homes while the whole family, from grandparent to grandchild, download music, software and books and stream video content for their own amusement. Few can deny the ever increasing significance and economic importance of "digital products" in our lives. Reform of the legal framework is thus a logical next step.

2.3 An Evaluation

The DCD seeks to provide fully harmonised[33] contract law rules, which will make it easier for businesses to offer digital content cross-border, while consumers will benefit and gain confidence from a set of clear rights that address the problems they face with digital content. This is a directive, not a regulation, and would not be an opt-in measure. SMEs, which would have received specific protection under CESL, are no longer to be given special status. The general objective of the Directive is to contribute to faster growth of the Digital Single Market, eliminate key contract law-related barriers to cross-border trade, increase consumer trust, reduce business cost and provide greater certainty for both consumers and businesses to the benefit of both.[34]

The Directive is confined to B2C contracts where the supplier supplies digital content to the consumer[35] and "in exchange, a price is to be paid or the consumer

[31]Of the particular problems raised by digital content contracts, see Helberger et al. (2013), Loos et al. (2011).

[32]Bradgate (2010), p. 10.

[33]DCD, Art. 4.

[34]DCD Explanatory Memorandum, p. 2.

[35]"Consumer" is defined at Art. 2(4) as any natural person who in contracts covered by this Directive is acting for purposes which are outside that person's trade, business, craft, or profession.

actively provides counter-performance other than money in the form of personal data or any other data".[36] The Directive, therefore, does not apply to digital content provided free of charge.[37] Article 5 provides that the supplier shall supply the digital content to the consumer immediately after the conclusion of the contract, unless the parties have agreed otherwise.[38] Three main areas of contract law are covered by the Directive:

(a) rules on conformity of digital content with the contract,
(b) remedies available for lack of conformity and the modalities for the exercise of those remedies, and
(c) the right to modify and to terminate long term contracts.

The DCD is not, therefore, engaging in full harmonisation. Recital 4 of the Directive indicates that the Commission believes that consumers are particularly concerned with problems relating to the quality of, and access to, digital content. The Directive leaves to national law issues such as the formation and validity of contracts and the legality of the content[39] and related issues such as the obligations of the consumer towards the supplier of digital content. It also does not determine whether the contract will be considered as a sales, services, rental or sui generis contract and leaves this to Member States (despite recognising this as a specific problem creating uncertainty in its Explanatory Memorandum).[40] Article 3 further excludes a number of contracts from its scope including healthcare, gambling and financial services and "services performed with a predominant element of human intervention by the supplier where the digital format is used mainly as a carrier". Its aim, also, is to be "future proof". Article 2.1 defines "digital content" broadly to signify:

(a) data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software,
(b) a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer, and
(c) a service allowing sharing of and any other interaction with data in digital form provided by other users of the service.

A supplier is defined at Art. 2(3) as "any natural or legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to that person's trade, business, craft, or profession."

[36]DCD, Art. 3.1. This is subject to Art. 3.4 (limits on counter-performance other than money).

[37]See DCD, Recital 14.

[38]Or to a third party which operates a physical or virtual facility making the digital content available to the consumer or allowing the consumer to access it and which has been chosen by the consumer for receiving the digital content: Art. 5.1(b).

[39]DCD, Art. 3.9. It does define a contract, however, at Art. 2.7.

[40]Mak argues that this is likely to lead to fragmentation and confusion, especially for consumers and SMEs. She recommends that the rules should be transposed into national laws as a separate set of rules for digital content contracts, similar to the approach taken in the UK Consumer Rights Act 2015: Mak (2016), pp. 12–13.

This definition is deliberately wider than that found in the Consumer Rights Directive 2011/83/EU (CRD) Art. 2(11)[41] and is specifically extended to cover the creation, processing and storage of data and developments such as cloud computing and social media, but it remains to be seen whether a "future-proof" definition is realistically possible in this technologically advanced area of law.[42] The Directive does extend, also, to goods such as DVDs and CDs that incorporate digital content in such a way that the goods function only as a carrier of the digital content.[43] This means, certainly, in contrast to the OSG, that contracts for the sale of such goods will be regulated by the DCD whether they are face-to-face or online.

Rules on Conformity of Digital Content with the Contract: Articles 6–10

Article 6 provides rules on conformity with the contract which, unlike Art. 2 of the Consumer Sales Directive 1999/44/EC (CSD), are specifically directed at digital content. Nevertheless, to those familiar with the CSD, the style is similar. Article 6.1 provides that, to conform to the contract, the digital contract shall, where relevant:

(a) be of the quantity, quality, duration and version and shall possess functionality, interoperability and other performance features such as accessibility, continuity and security, as required by the contract including in any pre-contractual information which forms integral part of the contract[44];
(b) be fit for any particular purpose for which the consumer requires it and which the consumer made known to the supplier at the time of the conclusion of the contract and which the supplier accepted;
(c) be supplied along with any instructions and customer assistance as stipulated by the contract; and
(d) be updated as stipulated by the contract.

[41]"Digital content" means data which are produced and supplied in digital form. See also CESL Art. 2(j).

[42]The UK experienced similar problems trying to make provision for internet defamation in its Defamation Act 2013, s.5.

[43]DCD, Recital 12. This leads to a complicated distinction in Recital 11 which states that the Directive does not apply to digital content which is embedded in goods in such a way that it operates as an integral part of the goods and its functions are subordinate to the main functionalities of the goods to which the proposed OSG Directive would apply. It is submitted that consumers may struggle with this rather technical distinction. In June 2017, the European Council suggested that digital content forming part of a good in a way that such good would be inoperable or would be prevented from performing its main functions in the absence of such digital content should be subject to the OSG only: see Press Release 8 June 2017, 'New rules for contracts for the supply of digital content – Council adopts its position'.

[44]A cross-reference here to the Consumer Rights Directive.

Article 6.2 provides objective conformity criteria *to the extent that the contract does not stipulate, where relevant, in a clear and comprehensive manner, the requirements for the digital content under paragraph 1*. It states that:

> . . . digital content shall be fit for the purposes for which digital content of the same description would normally be used including its functionality, interoperability and other performance features such as accessibility, continuity and security, taking into account:
>
> (a) whether the digital content is supplied in exchange for a price or other counter-performance than money;
>
> (b) where relevant, any existing international technical standards or, in the absence of such technical standards, applicable industry codes of conduct and good practices; and
>
> (c) any public statement made by or on behalf of the supplier or other persons in earlier links of the chain of transactions unless the supplier shows that
>
> (i) he was not, and could not reasonably have been, aware of the statement in question;
>
> (ii) by the time of conclusion of the contract the statement had been corrected;
>
> (iii) the decision to acquire the digital content could not have been influenced by the statement.

The italicised wording is perhaps surprising, giving as it does primary importance to the express contractual terms. It might be questioned why the Commission has chosen to limit consumer protection in this way and it seems to place considerable faith in the pre-contractual information requirements mentioned at Art. 6.1 (a). Spindler has argued that what is missing from this objective list is a benchmark for reasonable consumer expectations. He concludes that, in its current form, it is unlikely that Art. 6 DCD will actually improve the level of consumer protection for digital content in that it leaves the contract's content almost entirely to the parties' individual stipulations that, in practice, will be determined by the supplier's pre-designed terms and conditions.[45] One positive development, however, is the provision that unless otherwise agreed, digital content should be supplied in conformity with the most recent version of the digital content that was available at the time of the conclusion of the contract.[46] Article 9 places the burden of proof for conformity with the contract on the supplier, unless the supplier can show that the digital environment[47] of the consumer is not compatible with interoperability and other technical requirements of the digital content and where the supplier informed the consumer of such requirements before the conclusion of the contract. This reflects the supplier's deemed superior knowledge in matters of a technical nature. However, Art. 9.3 provides that the consumer must cooperate with the supplier to the extent possible and necessary to determine the consumer's digital environment.[48] Where the consumer fails to cooperate, the burden of proof with respect to the non-conformity with the contract shall be on the consumer. It remains

[45] Spindler (2016), p. 199.

[46] Art. 6.4. To conform with the contract the digital content must also meet the requirements of Art. 7 (integration of digital content) and Art. 8 (third party rights).

[47] "Digital environment" is defined at Art. 2.8.

[48] The obligation to cooperate is limited to the technically available means which are the least intrusive for the consumer.

to be seen just how "co-operative" consumers will be expected to be and to what extent suppliers will require the supply of information by consumers prior to purchase.[49]

The supplier will be held liable for any lack of conformity that exists at the time the digital content is supplied or, where the digital content is supplied over a period of time, during this period.[50] It should be noted, however, that while Art. 5.1, CSD provides that "the seller shall be held liable under Article 3 where the lack of conformity becomes apparent within two years as from delivery of the goods", no such limit exist under the DCD.[51] Recital 43 explains that this is because by its nature digital content is not subject to wear and tear while being used and is often supplied over a period of time rather than as a one-off supply. On this basis, national prescription rules will apply. As these are not subject to harmonisation, there will, therefore, be variation in the period of applicability of the conformity requirement that is far from ideal in a maximum harmonisation directive.

We see here a new regime modelled on the CSD, but with a genuine attempt to focus on this specific context.

Remedies: Articles 11–14

Article 11 gives an immediate right to terminate where the supplier has failed to supply the digital content in accordance with Art. 5. This is straight-forward, reflecting a serious breach of contract. Interruptions of supply once commenced will be dealt with under Art. 12.

Article 12 provides the main remedies for non-conformity and reflects the policy decision underlying the CSD that priority should be given to rectifying the defective product. As a first step, the consumer will be entitled to have the digital content brought into conformity with the contract free of charge and within a reasonable time, unless this is impossible, disproportionate or unlawful: Art. 12.1. Only under the circumstances outlined in Art. 12.3, as a second step, may the consumer demand either a proportionate reduction of the price or to terminate the contract under Art. 13. The CSD similarly provides for a hierarchical order of remedies: defective goods will be repaired or replaced or, where this is not appropriate, consumers may obtain a suitable reduction of the price or have the contract rescinded.[52] As Miller has noted,[53] such an approach reflects a civilian, rather than common law approach to remedies, and contrasts with the common law general preference for the right to

[49]Recital 33 suggests that this may be done by providing the supplier with automatically generated incident reports or details of the consumer's internet connection.

[50]Art. 10.

[51]Contrast the pOSG, Art. 8.3 where the period is set at two years from the relevant moment for establishing conformity.

[52]CSD, Art. 3.

[53]Miller (2007), pp. 92–94.

reject defective products rather than continue to pursue an ongoing relationship with a producer who is no longer trusted.[54] The right to terminate is further confined to circumstances where "the lack of conformity with the contract impairs functionality, interoperability and other *main performance* features of the digital content such as its accessibility, continuity and security", thereby excluding termination for minor defects: Art. 12.5.[55] Notice must be given. The supplier will be obliged to reimburse the price paid no later than 14 days from receipt of notice.[56] Provision is also made for the return of digital content by both consumer and supplier; measures which have received widespread criticism of being unworkable and economically unnecessary.[57] No charge may be made for use of the digital content in the period prior to termination of the contract, as this would deprive the consumer of effective protection.[58] Damages are also available under Art. 14 for financial losses to the digital environment of the consumer, that is hardware, digital content and network connections under the control of the user, caused by a lack of conformity with the contract or a failure to supply the digital content (but not, it would seem, other consequential losses).This is presented by the Commission as a complementary remedy to those for non-conforming digital content stated above.[59] Clive has remarked, however, that the very limited nature of this right merely points up the absence of any more general right to damages.[60] It is for Member States to provide the detailed rules for the exercise of this right.[61]

Again, we see provisions modelled on those of the CSD. Article 20 makes express provision to amend Art. 1.2 of the CSD to exclude from the definition of consumer goods a durable medium incorporating digital content, now covered by the DCD.

[54]"The buyer's first and primary remedy for a breach of contract by the seller is to reject the goods, and, if appropriate, to repudiate the contract": Twigg-Flesner et al. (2016), p. 435. However, the Consumer Rights Act 2015, Part 1, Ch 3 departs from this position, as will be shown below.

[55]Emphasis added. The burden of proof will be on the supplier: Art. 12.5.

[56]Where money is not paid, the supplier shall take all measures which could be expected to refrain from use of the counter-performance which the consumer has provided: Art. 13.2(b).

[57]Fauvarque-Cosson (2016), pp. 14–16; BIS (2016), p. 8.

[58]Art. 13.4. and recital 41. This is consistent with Court of Justice of the European Union (CJEU) *Quelle AG v Bundesverband der Verbraucherzentralen und Verbraücherverbände* Case C-404/06, 17 April 2008.

[59]European Commission Impact Assessment on proposals for directives of the European Parliament and of the Council (1) on certain aspects concerning contracts for the supply of digital content and (2) on certain aspects concerning contracts for the online and other distance sales of goods, Brussels, SWD (2015) 274 final/2, p. 128.

[60]Clive (2016). See also Beale (2016), pp. 23–24.

[61]Art. 14.2. The European Council in June 2017 recommended that Art. 14 should be deleted and replaced with an explicit reference to national law with regard to this issue.

Modification of Digital Content and Termination of Long Term Contracts: Articles 15–16

These provisions can be dealt with briefly. Article 15 provides that where the contract permits modifications to a long-term contract which adversely affect the way the consumer benefits from the main performance features of the digital content, the consumer is given added protection e.g. he or she must be notified reasonably in advance of the modification by an explicit notice on a durable medium and may terminate the contract free of charge within no less than 30 days from receipt of that notice. Article 16 deals with the termination of long term contracts i.e. which are indeterminate or exceed 12 months.[62] To permit competition in the digital single market, consumers are to be given the right to terminate such contracts under certain balanced conditions. These provisions highlight the Commission's awareness of the distinctive nature of digital contracts and, in particular, the specific issues related by long-term contracts.[63]

2.4 Is the DCD Likely to be Successful?

As indicated above, the Commission has, with more than a little help from commentators, recognised that this is an area of law where there is limited national guidance and therefore a directive providing a ready-made regulatory framework is more likely to be welcomed by Member States rather than a broad proposal to replace established national contract law rules with those proposed by the Commission. The choice of a directive, rather than a regulation, is likely to prove more popular in that it gives Member States greater freedom in transposing the legislation into national law.[64] Maximum harmonisation, however, is a more controversial choice, although consistent with recent Commission practice, for example in the CRD. Minimum harmonisation is generally more popular with Member States in that it allows more space for diversity and local autonomy.[65] In contrast, maximum harmonisation provides uniformity at the expense of these values with the possible risk of a diminution of existing consumer protection if it is higher than that found in the Directive. In its Reasoned Opinion of March 2016,[66] the French Senate criticised the choice of maximum harmonisation in that it would prevent Member States from implementing higher standards of consumer protection.[67] Beale and Mak have also expressed concern that full harmonisation will result in some

[62]Art. 13 will also apply to long term contracts in cases of non-conformity.

[63]See the classic article of Macneil (1978), Campbell et al. (2013).

[64]Art. 288(3) TFEU.

[65]See Weatherill (2012).

[66]Résolution 7 March 2016: see http://www.senat.fr/leg/tas15-103.pdf Accessed 19 Mar 2017.

[67]Other national Parliaments did not issue reasoned opinions but did express some disquiet as to the content of the directive: see Mańko (2016a), p. 11.

significant reductions in consumer protection for both domestic and cross-border contracts notably if a narrow reading is taken of the Art. 14 right to damages.[68] An additional fear is that maximum harmonisation will run the risk that national legislatures will be unable to respond quickly and adequately to new practices detrimental to consumers in a rapidly developing market.[69]

Concern has also been expressed at the decision to divide the sale of tangible goods and supply of digital content between two distinct directives[70] and whether the provisions concerning the right to termination are sufficiently clear.[71] Beale has also argued that the DCD does not tackle important questions such as whether consumers have the right to make second copies, to transfer digital content or to receive essential upgrades for free,[72] highlighting the real problems of "future proofing" a directive in a technologically advanced area of law. One final concern is that the provisions for digital contracts are spread across several directives—the E-Commerce Directive,[73] the CRD, the Unfair Contract Terms Directive and now the DCD. Mańko has also highlighted potential difficulties of overlap with the General Data Protection Regulation (GDPR), which will become directly applicable in Member States from May 2018.[74] One might consider whether this is desirable in terms of certainty and clarity of rights for either consumers or suppliers. It is unclear also to what extent the fate of the DCD is tied to that of the proposed OSG Directive, which, as stated above, has received a more critical reception. Nevertheless, assuming such obstacles and opposition can be overcome, one final dilemma remains: where does the DCD leave Member States who have already implemented their own legislation in the field of contracts for the supply of digital content?

[68]Beale (2016), pp. 22–24; Mak (2016), pp. 26–27.

[69]Mańko (2016b) at 2.2.

[70]Wendehorst (2016), arguing that goods in the digital age are often hybrid products consisting of the tangible substance, of digital content that is stored on the device, and of digital content that is provided online within long-term framework relationships. See also Smits (2016), p. 324.

[71]Fauvarque-Cosson (2016), p. 5.

[72]Beale (2016), p. 27. See also Spindler (2016), p. 202 who raises the question of patches to fix defects which will usually be provided neither in exchange for money nor supplied in exchange for personal data.

[73]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJL178/1. The Directive establishes harmonised rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers.

[74]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), OJ L 119/1. See Mańko (2016b) who notes at 2.1.5 that, in line with Art. 3(8) DCD, the GDPR regime is to be considered parallel with the DCD regime.

3 The UK Consumer Rights Act 2015

The process leading to the CRA can be traced back to 2004 when the UK government first considered modernising consumer law, producing, in 2009, a White Paper proposing plans for a Consumer Rights Bill.[75] Other influences were the introduction of the CRD which makes specific provision for digital contracts[76] and, in particular, the 2010 Bradgate report to the then Department for Business Innovation and Skills (BIS)[77] which identified uncertainty relating to consumer rights to quality for digital content products.[78] The UK government sought in the Act to provide greater legal uncertainty for consumers and businesses "in a market that is both of a substantial size—around £200 billion—and still developing."[79] Part 1 of the CRA thus applies where there is an agreement between a trader[80] and a consumer[81] for the trader to supply goods, digital content or services.

3.1 An Evaluation

As indicated above, the Act treats digital content as sui generis, not to be confused with goods and services. Part 1, Ch 3 of the CRA is devoted specifically to digital content. The UK legislator does, therefore, engage in classification for the sake of clarity in contrast to the Commission. Specific provision is made for mixed contracts in s. 16.[82] "Digital content" is defined in s.2(9) as "data which are produced and supplied in digital form". This reproduces the definition found in the CRD (and

[75]See Twigg-Flesner et al. (2016), pp. 497–499.

[76]Notably imposing information requirements and withdrawal rights: see, for example, Arts. 2 (10) and (11), Arts. 5.1(g) and (h), Arts. 6(1)(r) and (s), Art. 9(2)(c), Art. 14(4)(b), Art. 27 and Art. 30.

[77]Department for Business, Innovation & Skills was replaced by Department for Business, Energy & Industrial Strategy (BEIS) in July 2016.

[78]Bradgate (2010), pp. 2–6. See also BIS (2012).

[79]Lord Younger of Leckie, Hansard HL 1 July 2014 col. 1646.

[80]"Trader" means a person acting for purposes relating to that person's trade, business, craft or profession, whether acting personally or through another person acting in the trader's name or on the trader's behalf: s.2(2).

[81]"Consumer" means an individual acting for purposes that are wholly or mainly outside that individual's trade, business, craft or profession: s.2(3).

[82]s.16(1): Goods (whether or not they conform otherwise to a contract to supply goods) do not conform to it if—(a)the goods are an item that includes digital content, and(b)the digital content does not conform to the contract to supply that content (for which see section 42(1)). The remedies applicable to goods will apply here.

indeed mirrors that of Art. 2.1(a) DCD), but does not extend to cloud computer and social media services.[83] Supply of a service merely to enable consumers to access digital content, such as Internet or mobile service provision, are not covered.[84] Bearing in mind the importance of cloud computing and social media services to consumers, the limited ambition of the Act is disappointing in terms of consumer protection.

The digital content must also be supplied to the consumer for a price, even if that price was paid for other goods, services and digital content: ss.33(1),(2).[85] It does not extend to counter-performance other than money, in contrast to Art. 3 DCD. The Act does, however, at s.33(5) make provision for the Secretary of State to extend the digital content provisions to other digital contracts if "satisfied that it is appropriate to do so because of significant detriment caused to consumers under contracts of the kind to which the order relates."Commentators have noted that, in practice, contracts in which a consumer "pays" for a product or service by providing personal or other data have become an increasingly important mode of contracting.[86] The UK government has indicated, however, its concerns that an extension to such services might mean that the obligations and remedies proposed in the event of failure to comply with the contract are not proportionate in the circumstances and that they might unduly inhibit this often low margin but very innovative business model.[87] *Atiyah and Adams' Sale of Goods* argues that, in any event, the Act should apply where the consumer downloads a free app, but then purchases additional features.[88]

Rules on Conformity of Digital Content with Contract: Sections 34–41

Sections 34–41 deal with rules on conformity of digital content with the contract. These mirror the provisions concerning goods found in Chapter 1 of the Act following the approach advocated in the Bradgate report.[89] The intention, therefore,

[83]It would, however, apply to cloud computing to the extent that digital content is supplied to the consumer (e.g. accessing software), but not when a consumer simply buys access to remote storage (this would be a simple service contract): Bray and Kerry (2015), p. 272.

[84]Service contracts are covered by Part 1 Ch 4 of the CRA. S.49(1) simply requires that every contract to supply a service is to be treated as including a term that the trader must perform the service with reasonable care and skill.

[85]See also s.33(3): The references in subsections (1) and (2) to the consumer paying a price include references to the consumer using, by way of payment, any facility for which money has been paid e.g. token or virtual currency.

[86]See, for example, Mak (2016), p. 10.

[87]BIS (2016), pp. 5–6. Note also opposition from trade bodies such as UK Interactive Entertainment (Ukie) (2016), although the consumer group *Which?* had lobbied strongly for a broader definition.

[88]Twigg-Flesner et al. (2016), pp. 514–515. See also Bray and Kerry (2015), p. 271.

[89]See ss9–18 CRA.

is to provide parallel provisions to maintain coherence, although commentators have questioned whether this is entirely successful given that, in contrast to sale of goods contracts, the consumer generally only purchases a licence to use the digital content and is likely to have a limited ability to communicate with a (usually) online retailer.[90] The digital content must be of satisfactory quality (s.34), fit for a particular purpose (s.35), and as described (s.36), reflecting the influence of both the Sale of Goods Act 1979 and the CSD. These sections may be contrasted with the more concise provision in the Directive (Art. 6) discussed above. Despite the differences, the UK government is of the view that, in practice, the approach under the Directive will have the same effect as the approach in the UK.[91] In terms of the Art. 9 reversal of burden of proof, s.42(9) provides that "digital content which does not conform to the contract at any time within the period of *six months* beginning with the day on which it was supplied must be taken not to have conformed to the contract when it was supplied."[92] In other words, there is a (rebuttable) presumption of non-conformity, but only for a six-month period. It will also be lost if it is established that the digital content did conform to the contract when it was supplied, or its application is incompatible with the nature of the digital content or with how it fails to conform to the contract.[93] This replicates the provisions relating to goods at ss.19(14) and (15).No attempt is made, as in the DCD, to distinguish the particular needs of non-technologically minded consumers or the fact that six months is of limited significance in long term contracts. Special provision is made for the pre-contract information required by the CRD in ss. 36 (3) and 37.[94]

There are some provisions, however, designed especially for digital contracts. Section 40 (Quality, fitness and description of content supplied subject to modifications) is directed to ensuring that where the trader reserves a right to modify the digital content in the contract, modifications must also comply with the requirements of quality, fitness for a particular purpose and description.[95] This applies to both positive and negative modifications. Section 39 (supply by transmission and

[90]Barry et al. (2016) at 4.24.

[91]BIS (2016), p. 7.

[92]Emphasis added.

[93]s.42(10).

[94]In terms of remedies, note s.42(4): If the trader is in breach of a term that section 37 requires to be treated as included in the contract, the consumer has the right to recover from the trader the amount of any costs incurred by the consumer because of the breach, up to the amount of the price paid for the digital content or for any facility within section 33(3) used by the consumer. The pre-contractual information requirements were transposed into UK law under the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (SI 2013/3134), not, it should be noted, by the Consumer Rights Act 2015.

[95]A contract term allowing the trader to provide updates may also be assessable for fairness under Part 2 of the Act (Unfair Terms). The time limit for a consumer to make a claim relating to an update is within 6 years of when the digital content was first supplied (in Scotland this period is 5 years), unless the update is provided under a separate contract that falls within the scope of the quality rights provided in the Act.

facilities for continued transmission) deals with contracts to supply digital content where the consumer's access to the content on a device such as a smartphone requires its transmission to the device under arrangements initiated by the trader. Any such processing facility must be available to the consumer for a reasonable time, unless otherwise agreed, and must comply with the requirements of quality, fitness for purpose and description. Such specific provisions are, however, limited in comparison to the more specific focus on the needs of the digital consumer found in the DCD.

Remedies: Sections 42–46

The remedies provisions do resemble those of the DCD in that they reflect the influence of the CSD, but differences exist. Section 42(2) provides that if the digital content does not conform to the contract, the consumer's rights (and the provisions about them and when they are available) are:

(a) the right to repair or replacement (see section 43);
(b) the right to a price reduction (see section 44).

The right to a price reduction is, however, secondary to the right to repair or replace, as seen in the CSD and Art. 12, DCD.[96] If the trader is in breach of s.41 (1) (right to supply the content), the consumer does, however, the right to a refund.[97] Otherwise, it is not open to the consumer to treat the contract as at an end for breach of the terms implied in ss.34–37 and 41.[98] This means that s.42 does not include a 'right to reject', in contrast to the remedies for goods under s.19. The reason for this is that intangible digital content cannot be returned in any meaningful sense.[99] Subject to this provision, ss.42(6) and (7) do not prevent claimants seeking instead ordinary common law remedies such as damages or specific performance. What we see if an amalgam of the remedies provisions of the CSD and the common law. The quality rights and corresponding remedies cannot be excluded: s.47.[100]

Section 46 provides a specific remedial provision for damage to the device or to other digital content, regardless whether the digital content supplied under contract

[96] s.44(3).

[97] See s.45.

[98] s.42(8).

[99] Explanatory notes to Act, para 205. This does seem to be somewhat of a generalisation but it should be noted that where digital content sold on a tangible medium (e.g. on a disk or as part of a digital camera), s.16 provides that, where the digital content is substandard (as judged against the digital content quality rights), the remedies for goods will apply i.e. a right to reject will arise. See also Samuels (2016).

[100] In contrast, s.46 (below) is subject to the fairness test, stated in Part 2 of the Consumer Rights Act 2015: see section 62 (requirement for contract terms and notices to be fair).

was free or paid for.[101] The damages must, however, be of a kind that would not have occurred if the trader had exercised reasonable care and skill.[102] The intention behind this section is to engage the principles behind a negligence claim, but limit the type of loss that can be claimed.[103] The trader must either repair the damage[104] or compensate the victim accordingly. A compensation payment under this section must be made without undue delay, and in any event, within 14 days beginning with the day on which the trader agrees that the consumer is entitled to the payment.[105] This does not preclude an action to pursue damages for consequential loss under the general law of contract or tort. Willett argues that because of the difficulties of proving whether the trader has exercised reasonable care and skill, consumers may prefer to bring a simple claim for breach of satisfactory quality under s.42 or claim for damages at common law for breach of the s.34 implied term.[106]

The intention of the Act is to ensure that UK law is compliant with the CSD and the CRD. This raises a related difficulty in terms of the Commission's current Regulatory Fitness and Performance Programme (REFIT).[107] A recent Fitness Check evaluated whether the CSD was fit for purpose based on the criteria of effectiveness, efficiency, coherence, relevance and EU added value (this is due to be published in 2017).[108] The CRD was not reviewed in the fitness check, but was subject to a separate report by the Commission which reported in 2017. The reports found room for improvement and that follow-up actions should be undertaken. This does indicate the Act may soon find itself out of sync with a reformed CSD and CRD.

3.2 The Consumer Rights Act 2015 Post-Brexit

As shown above, the CRA represents an ambitious attempt by the UK to consolidate its consumer law, undertaking at the same time the integration of a number of EU consumer directives into its law. We can identify the influence of the CSD and CRD albeit within an approach which is very much influenced by the pre-existing statutory and common law sale of goods framework. In Part 1, Ch 3 of the Act, the UK legislator sought to recognise the distinctive needs of consumers making

[101] See s.33(8). A trader does not, however, supply digital content to a consumer merely because the trader supplies a service by which digital content reaches the consumer.

[102] Contrast Art. 14 DCD which assumes strict liability.

[103] Explanatory Notes to Act, para. 219.

[104] As set out in ss.46(3) and (4).

[105] s.46(5).

[106] Willett (2016), p. 34.

[107] See http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm Accessed 19 Mar 2017.

[108] See European Commission, Fitness Check of Consumer and Marketing Law, SWD (2017) 209 final. It also reviewed Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) and Directive 93/13/EEC on unfair terms in consumer contracts (Unfair Contract Terms Directive).

contracts for the supply of digital content even if, in contrast to the Directive, less effort was made to "future proof" the Act to reflect developments in digital content services. In particular, this chapter has highlighted the confinement of contracts to those where a "price" is paid and questioned whether the UK legislator should continue to ignore the growth of the market for digital contracts and whether a six-month presumption of conformity is sufficient. The Directive should also make UK lawyers consider whether they also need to pay more attention to the long-term nature of these contracts and the often real disparity between the knowledge of the consumer and the supplier in question.

It may, however, be argued that this debate is irrelevant following the result of the June 2016 referendum that the UK should leave the EU. While EU law remains for the moment binding, the future is uncertain. In March 2017, the UK Parliament passed the European Union (Notification of Withdrawal) Act 2017 permitting the Prime Minister to notify, under Article 50(2) of the Treaty on European Union, the United Kingdom's intention to withdraw from the EU. This occurred on March 29 2017. Depending on the outcome of negotiations between the UK and the EU, there is a distinct possibility that new EU directives and modifications of existing directives will not be binding in UK law. This gives rise to the interesting question how the CRA—a statute which expressly seeks to include EU directives within its remit—will be interpreted post-Brexit. It is most unlikely given the time and effort involved in drafting the CRA and the stated importance of consumer rights that the UK Parliament will seek to re-open its provisions and excise its EU content. Existing provisions will thus remain. It might also be argued that decisions of the Court of Justice of the European Union will become persuasive authority for EU sourced sections, although no longer binding, once the UK has left the EU. Given the importance of contracts for the supply of digital content in terms of the UK economy, it does remain a real possibility that the DCD, if successful, will lead UK legislators to rethink whether the CRA is in need of reform. Two major reforms can be identified immediately: extension of Chapter 3 to digital services and the inclusion of contracts where consideration is provided by counter-performance other than money in the form of personal data or any other data. It remains an interesting question to what extent the new proposed directive will lead to changes to UK law *despite* Brexit. It is one UK consumer lawyers will be monitoring with great interest.

4 Conclusions: Lessons to be Learnt from the UK Consumer Rights Act?

The DCD marks a positive step forward in terms of improving consumer rights in the vibrant digital market. By filling a gap in the majority of European contract law systems, the proposed Directive seeks to provide greater certainty for both consumers and businesses, but also offers a valuable opportunity to mould key contract

law provisions on quality and remedies to the particular context of digital content. This is an important market and encouraging cross-border trade by harmonising the key elements of a contract, which interest consumers—How do I prove non-conformity? What can I do about it?—supported by measures which enhance enforcement and render it easier to obtain compensation through, for example, online dispute resolution, is likely to be beneficial to EU Member States. It is important, however, to get it right. Here, the experience of the CRA may be of assistance.

I do not have space here to engage in a detailed breakdown of differences between the two pieces of legislation. It is important, however, to identify headline differences—those that signify different policy choices where the DCD is likely to face opposition from, in particular, representatives of the business community. Earlier, I criticised the CRA for defining "price" in s.33 too narrowly, but it is worthwhile considering why this decision was made. The UK government resisted attempts by consumer groups for a wider definition in the face of lobbying by businesses and continues to argue that inclusion might inhibit business development. The extension to counter-performance other than money is therefore likely to prove unpopular with the business community.

A further source of contention highlighted by the CRA is the dividing line between sale of goods and sale of digital content. This is of vital importance in that the Commission has produced two draft directives with different provisions. The CRA also divides itself into distinct categories—goods, services and digital content—but these are found within the same legislative instrument and some cross-reference is made. In particular, s.16 addresses "mixed contracts", that is, tangible goods that include digital content, to which the provisions related to goods will apply. This means, in particular, different remedies, such as the right to reject within 30 days, will apply to CDs. This is distinguished from digital content supplied in tangible form e.g. on a disk or pre-loaded onto a device such as a phone or tablet, which falls within the digital content provisions. In contrast, the 2015 DCD treats DVDs and CDs as within the DCD, not the OSG. One might question whether this is the obvious choice, at least to consumers. With a separate directive dealing with online sale of goods—as distinct from the supply of digital content which is not confined to the online context—then the CRA highlights that this distinction needs to be cleaner and comply with consumer expectations.

The presumption of non-conformity in the CRA of 6 months has also been criticised as too short in the digital content context, but it highlights the controversial nature of the Art. 9 reversed burden of proof. This has no time limit save that imposed by the prescription rules of each Member State (which are not harmonised). Again this is likely to split consumer and business groups and it will be interesting to see if the Commission will stick to this innovative piece of consumer protection. The General Approach adopted by Council on 8 June 2017 proposed a period of 1 year, albeit with a number of States openly dissenting from this view. The restrictions on the right to reject under the CRA do, however, highlight the complexity of the termination rules of Art. 13. Attempting termination with some degree of restitution does seem problematic in this area of law and this

chapter has noted immediate criticism of Art. 13 by commentators. Finally, UK commentators have noted the retention of ordinary contract law remedies in the Act, notably that of damages. Willett has speculated that s.46 may be rarely used, as consumers prefer the non-conformity remedies or common law damages. It is not clear where the Art. 14 right to damages (if it survives) fits within the general right to damages. Does Art. 14 act as a limit or an additional remedy for consumers? This needs to be clarified before the directive has been transposed into Member State law.

An EPRS briefing in March 2017 has indicated that Committees of the European Parliament have indeed raised some of these concerns. Recommendations include expanding the directive's scope to include digital content supplied against data that consumers provide *passively*, and strengthening the position of consumers by making objective criteria the default rule for matters of conformity.[109] On this basis, the objective criteria could only be departed from if the consumer's attention was explicitly drawn to the shortcomings of the digital content. Such measures, if adopted, would significantly improve the position of consumers, but, as the UK response has highlighted, are likely to raise further tensions with the business community. In June 2017, the General Approach adopted by Council also recommended a number of important revisions, concerning the scope of the DCD, its remedies, the test for non-conformity and supplier liability, and suggested the need for a 'compromise text'. It is likely therefore that some revisions will be made before the DCD becomes law.

Atiyah and Adams' Sale of Goods argued, somewhat optimistically, that as one of the first dedicated measures in the EU to deal specifically with regulation of digital content, the CRA might establish a template for future regulation at an EU level.[110] This has not occurred. Nevertheless, as the Commission moves forward with its two proposed directives, derived from the failed CESL project but consistent with its Digital Single Market strategy, it is submitted that even post-Brexit, the experience of the CRA may offer assistance in framing a proposal that is likely to be workable and obtain final approval from the Council of Ministers. It is clear that this is an area of law where both consumer and businesses would benefit from regulatory support. It is vital, however, that lessons are learnt and that any directive regulating contracts for the supply of digital content provides the best possible framework for contracting in Europe.

[109]Mańko (2017), pp. 8–11. See also the Opinion of the Committee on Civil Liberties, Justice and Home Affairs 21 Nov 2016 PE 582.370. This is also support for such amendments in Council: Mańko (2017), p. 11.

[110]Twigg-Flesner et al. (2016), p. 514.

References

Barry D et al (2016) Blackstone's guide to the Consumer Rights Act 2015. OUP, Oxford
Beale H (2006) The European Civil Code movement and the European Union's common frame of reference. Leg Inform Manage 6:4–11
Beale H (2016) Scope of application and general approach of the new rules for contracts in the digital environment: In: Depth Analysis. European Parliament - Policy Department for Citizen's Rights and Constitutional Affairs, PE 536.493
BIS (2012) Enhancing consumer confidence by clarifying consumer law: consultation on the supply of goods, services and digital content. Crown Copyright, London
BIS (2016) Draft directives on the online sale of digital content and tangible goods: UK government call for views. Crown Copyright, London
Bradgate R (2010) Consumer rights in digital products: a research report prepared for the UK department for business, innovation and skills.Institute for Commercial Law Studies, Sheffield and BIS, London. Available at http://www.bis.gov.uk/assets/biscore/consumer-issues/docs/c/10-1125-consumer-rights-in-digital-products. Accessed 19 Mar 2017
Bray O, Kerry B (2015) Digital content under the Consumer Rights Act 2015. Entertain Law Rev 26:271–273
Campbell D, Mulcahy L, Wheeler S (eds) (2013) Changing concepts of contract. Palgrave Macmillan Socio-Legal Studies, Basingstoke
Clive E (2016) The proposed new digital single market contract law Directives. European Private Law News, 19 January 2016. Available at http://www.epln.law.ed.ac.uk/2016/01/19/the-proposed-new-digital-single-market-contract-law-directives/. Accessed 19 Mar 2017
Fauvarque-Cosson B (2016) The new proposal for harmonised rules for certain aspects concerning contracts for the supply of digital content (termination, modification of the digital content and right to terminate long term contracts: In: Depth Analysis. European Parliament - Policy Department for Citizen's Rights and Constitutional Affairs, PE 536.495
Giliker P (2017) The Consumer Rights Act 2015 – A bastion of European consumer rights? LS 37:78–102
Gutman K (2014) The constitutional foundations of European contract law. OUP, Oxford
Helberger N et al (2013) Digital content contracts for consumers. J Consum Policy 36:37–57
Hesselink MW (2012) How to opt into the common European sales law? Brief comments on the commission's proposal for a regulation. Eur Rev Priv Law 20:195–211
Jansen N, Zimmermann R (2010) A European civil code in all but name. Cambridge Law J 69 (1):98–112
Kornet N (2012) The Common European Sales Law and the CISG - Complicating or Simplifying the Legal Environment? Maastricht European Private Law Institute Working Paper 2012/4. Available at http://ssrn.com/abstract=2012310. Accessed 19 Mar 2017
Kuipers J-J (2011) The legal basis for a European optional instrument. Eur Rev Priv Law 19:545–564
Lando O (1983) European contract law. Am J Comp Law 31:653–659
Lando O, Beale HG (eds) (1999) Principles of European contract law parts 1 and 2. Kluwer Law International, The Hague
Lando O, Clive E, Prum A, Zimmermann R (eds) (2003) Principles of European contract law: part 3. Kluwer Law International, The Hague
Loos M et al (2011) The regulation of digital content contracts in the optional instrument of contract law. Eur Rev Priv Law 19:729–758
Macneil IR (1978) Contracts, adjustments of long term economic relations under classical, neo classical and relational contract law. Northwest Univ Law Rev 72:854–905

Mańko R (2016a) Contracts for Supply of Digital Content to Consumers. Briefing: EU Legislation in Progress, European Parliamentary Research Service, PE 581.980
Mańko R (2016b) Contracts for Supply of Digital Content: A legal analysis of the Commission's proposal for a new directive: In: Depth Analysis, European Parliamentary Research Service, PE 582.048
Mańko R (2017) Contracts for Supply of Digital Content. Briefing: EU Legislation in Progress, European Parliamentary Research Service, PE 599.310
Mak V (2016) The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content: In: Depth Analysis, European Parliamentary Research Service, PE 536.494
Micklitz H-W, Reich N (2012) The Commission proposal for a 'regulation on a Common European Sales Law (CESL)' – Too broad or not broad enough? EUI Working Papers 2012/04. Available at http://cadmus.eui.eu/bitstream/handle/1814/20485/LAW_2012_04_ERPL_03.pdf. Accessed 19 Mar 2017
Miller L (2007) After the unfair contract terms directive: recent European directives and English law. Eur Rev Cont Law 1:88–110
Riesenhuber K (2012) The Proposal for a Regulation on a Common European Sales Law – Competence, Subsidiarity, Proportionality – a Report to the Committee on Legal Affairs of the German Bundestag' (in German). Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1998134. Accessed 19 Mar 2017
Samuels A (2016) The Consumer Rights Act 2015. J Bus Law (3):159–185
Smits JM (2016) New European Union proposals for distance sales and digital contents contracts: Fit for purpose? Zeitschrift für Europäisches Privatrech 319–324
Spindler G (2016) Contracts for the supply of digital content – scope of application and basic approach – proposal of the commission for a directive on contracts for the supply of digital content. Eur Rev Cont Law 12:183–217
Twigg-Flesner C, Canavan R, Macqueen H (2016) Atiyah and Adams'sale of goods, 13th edn. Pearson, Harlow
UK Interactive Entertainment (Ukie) (2016) Ukie response to BIS call for evidence on Draft Directive on the Online Sale of DigitalContent. Available at http://ukie.org.uk/sites/default/files/cms/docs/Ukie%20response%20to%20BIS%20call%20for%20views%20on%20draft%20EU%20directive%20on%20the%20online%20sale%20of%20digital%20content.pdf. Accessed 19 Mar 2017
von Bar C and Clive E (eds) (2009 and 2010) Principles, definitions and model rules of European private law: draft common frame of reference, Vols I–VI. Sellier, Munich and OUP, Oxford
Weatherill S (2012) Maximum versus minimum harmonisation: choosing between unity and diversity in the search for the soul of the internal market. In: Nic Shuibhne N, Gormley LW (eds) From single market to Economic Union. OUP, Oxford, pp 175–199
Wendehorst C (2016) Sale of goods and supply of digital content – two worlds apart? In Depth Analysis. European Parliament - Policy Department for Citizen's Rights and Constitutional Affairs, PE 556.928
Whittaker S (2012) The proposed 'Common European Sales Law': legal framework and the agreement of the parties. Mod Law Rev 75:578–605
Willett C (2016) Remedies in the Consumer Rights Act 2015. Solicitors J 160(18):33–34

Chapter 6
The Proposed New Digital Single Market Contact Law Directives: A New Start for Digital European Contract Law?

Thalia Prastitou Merdi

Abstract The proposal for a directive on certain aspects of contracts for the supply of digital content and the proposal for a directive on certain aspects of contracts for the online and other distance sale of goods were presented by the European Commission, in December 2015, as a "modified proposal" for the Regulation on a Common European Sales Law (pCESL) aiming to fully harmonise in a targeted way the key mandatory rights and obligations of the parties to a contract for the supply of digital content and the online sales of goods. This chapter examines, using a three-perspective comparative analysis, to which extent the European Commission by bringing forward these proposals has actually moved away from the pCESL project and started again and, if it has done so, whether these proposals as they currently stand form an adequate replacement for the rebirth of a truly digital European Contract Law.

1 Introduction: New Yet Familiar EU Legislative Proposals

Delivering for the first time on its Digital Single Market Strategy the European Commission presented, on 9 December 2015, two legislative proposals for simple and effective cross-border contract rules for consumers and businesses.[1] More specifically, the first legislative proposal concerned a directive on certain aspects

[1]Apart from these two legislative proposals, the European Commission brought forward, on the same day, a proposal for a regulation on the cross-border portability of online content services in the internal market (COM (2015) 627 final). This proposal is primarily important in the area of copyright law and therefore falls outside the ambit of this chapter.

T.P. Merdi (✉)
European University Cyprus, Nicosia, Cyprus
e-mail: T.Prastitou@euc.ac.cy

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_6

of contracts for the supply of digital content (pDCD)[2] while the second one concerned a directive on certain aspects of contracts for the online and other distance sale of goods (pOSD and together Proposals).[3] According to the European Commission "concretely, the two Directives will fully harmonise in a targeted way the key mandatory rights and obligations of the parties to a contract for the supply of digital content and the online sales of goods. They will contribute to faster growth of the Digital Single Market by reducing costs resulting from differences in contract law. . .creating legal certainty for businesses. . .helping consumers to gain from online cross-border shopping in the EU. . .reducing the detriment suffered by consumers with respect to defective digital content. . .[and] overall, balancing the interests between consumers and businesses".[4]

What is really interesting to note is that although, from a legal perspective, the Proposals are brand new, from a political perspective, they appear to form together, according to the European Commission, a "modified proposal" for the Regulation on a Common European Sales Law (pCESL).[5]

The European Commission unveiled the pCESL, on 11 October 2011.[6] This legislative proposal could be fairly characterised as the "first concrete step"[7] towards the creation of a European Contract Law. More specifically, it provided for a single uniform set of fully harmonised contract law rules, in a compact set of 186 provisions, which was to be considered as a second contract law regime within the national law of each Member State available in cross-border transactions[8] upon a valid agreement by the parties. In practice, the pCESL would have constituted an optional instrument, available for contracts between a business and a consumer or between businesses if one of the two businesses qualifies as a small or medium sized enterprise (SME).[9] It could be used solely for sale contracts, contracts for the supply of digital content and related service contracts. Expressly excluding from its

[2]Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM (2015) 634 final.

[3]Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM (2015) 635 final.

[4]Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Digital Contracts For Europe—Unleashing the potential of e-commerce, COM (2015) 633 final.

[5]Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law, COM (2011) 635 final.

[6]The pCESL consisted of three main parts, these being firstly the Regulation, setting out the objective, subject matter and scope of the pCESL, as well as a list of definitions of core notions used in the pCESL, secondly Annex I to the Regulation containing the Common European Sales Law and finally Annex II to the Regulation encompassing a Standard Information Notice.

[7]James (2011), p. 1.

[8]Yet, Member States had the option to extend it to domestic contracts according to Article 13 of the Regulation of the pCESL.

[9]According to Article 7 of the Regulation of the pCESL.

scope of application mixed purpose contracts and contracts linked to consumer credit.[10]

Shortly after its publication, various commentaries started appearing questioning the content[11] of this legislative proposal, as well as the competence[12] of the European Union to enact legislation of this kind based on Article 114 of the Treaty of Functioning of the European Union (TFEU). More importantly, despite the positive feedback it received by the European Parliament that adopted it enthusiastically in February 2014,[13] subject to a number of amendments, the pCESL did not find sufficient support in the Council of the European Union[14] and was finally withdrawn[15] by the, then newly appointed, Juncker Commission in December 2014 to bring forward "a modified proposal that will fully unleash the potential of e-commerce in the Digital Single Market". Few months later in its Communication for a Digital Single Market Strategy (Digital Single Market Strategy), presented in May 2015,[16] the European Commission promised to make an "amended legislative proposal before the end of 2015 (i) covering harmonised EU rules for online purchases of digital content, and (ii) allowing traders to rely on their national laws based on a focused set of key mandatory EU contractual rights for domestic and cross-border online sales of tangible goods". The European Commission kept its promise by bringing forward these Proposals in December 2015.

Looking at these Proposals one may wonder whether, *inter alia*, the European Commission has actually produced a modified proposal. Put simply, to which extent has it moved away from the pCESL project and started again? In addition, if it has done so do these Proposals as they currently stand form an adequate replacement for the rebirth of a truly digital European Contract Law?[17] By bringing forward a

[10]According to Article 6 of the Regulation of the pCESL.

[11]Eidenmueller and others (2012), pp. 356–357; Micklitz and Reich (2012).

[12]Low (2012), pp. 135–136.

[13]European Parliament Legislative Resolution of 26 February 2014 on the Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law, COM (2011)0635 – C7-0329/2011 – 2011/0284(COD), (Legislative Resolution of 26 February 2014).

[14]As well as from six Member States (these being France, Germany, United Kingdom, Austria, Netherlands and Finland) which submitted to the Commission a joint letter on 28 November 2014 highlighting disagreements between national governments in the European Union over the pCESL.

[15]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2015—A new start, COM (2014) 910 final, Annex II, no 60.

[16]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy For Europe, COM (2015) 192 final.

[17]What shall be noted is that these two legislative Proposals are currently being discussed, according to the ordinary legislative procedure, in both the Council of the European Union and the European Parliament. More specifically, it appears that although the former prefers a "fast-track" approach for the pDCD, while pursuing to reflect for longer on the pOSD, the latter is examining the two legislative Proposals in parallel.

comparative analysis of the most important aspects of the pDCD and pOSD *vis à vis* the pCESL this chapter attempts to answer these questions. This will be completed in a three-perspective comparative analysis. More specifically, this chapter assesses the extent to which these Proposals draw, firstly, on the form, secondly, on the scope and, thirdly, on the substance of the withdrawn pCESL.[18]

2 Legal Form: Shifting from Unification to Total Harmonisation

Following the harmonisation approach,[19] announced in its Communication for a Digital Single Market Strategy, the European Commission introduced the pDCD[20] and pOSD[21] as two separate full harmonisation directives based on Article 114 of the TFEU abandoning in this way the idea of a regulation for an opt in instrument which was the "essence"[22] of the pCESL. This conversion shall not come as a surprise[23] for two main reasons, which are now to be explained.

2.1 An Awaited Shift

Firstly, one may fairly argue that "harmonisation of [consumer] contract law by way of directives on the basis of Article 114 TFEU is [much] less controversial than resorting to this legal basis for an optional instrument".[24] More specifically, one shall not forget the extended criticism the European Commission received, both before and after the release of the pCESL, regarding the use of Article 114 TFEU as the legal basis for an optional instrument.[25] Interestingly the use of this Article went

[18]What must be clarified at this point is that the aim of this three-perspective analysis is not to provide an exhaustive comparison of all provisions of the Proposals vis-à-vis the pCESL but to give an overall picture as to whether these Proposals actually form a modified pCESL.

[19]Although as Manko (2015), p. 18, interestingly points out the Commission in its Inception Impact Assessment (http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_just_008_contract_rules_for_digital_purchases_en.pdf) left open for consideration both options of a regulation and a directive as although it stated that the proposed EU Online Sales Act "will create uniform rules for digital content products avoiding legal fragmentation" it simultaneously claimed that "it will bring forward a fully harmonised targeted set of key mandatory rules".

[20]Article 4 of the pDCD.

[21]Article 3 of the pOSD.

[22]Manko (2015), p. 18.

[23]Although the Parliament in its Legislative Resolution of 26 February 2014 opted to keep the proposal in the form of a regulation.

[24]Manko (2015), p. 18.

[25]Kuipers (2011).

"against the grain of received wisdom".[26] In fact before the publication of the pCESL some legal scholars,[27] using the *European Cooperative Society* case,[28] ruled out the use of Article 114 TFEU and instead supported the use of Article 352 TFEU as the appropriate legal basis for the pCESL. This view was largely based on the optional nature of the pCESL as an additional set of rules operating alongside national contract legislation. This view remained intact, even after the publication of the pCESL in October 2011, with the vast majority of legal scholars and practitioners questioning again whether there was a clear basis for the pCESL being an optional instrument.[29]

Secondly, moving towards harmonisation of consumer contract law by way of directives is not something new for the European Commission. It is in practice an already established 30-year old tradition in the EU. More specifically, after the establishment of the Single Market Program in 1985, the EU started having an indirect impact on national contract laws by developing a harmonised contract law strategy through the enactment of various minimum,[30] and later on, certain maximum harmonisation[31] directives.

2.2 A Positive Shift?

Because of this long established tradition, the European Commission appears to be much more confident and secure with this shift. This is visible twice within the Explanatory Memorandum of both Proposals.

[26]Low (2012), p. 132.

[27]Hesselink and others (2007), pp. 49–50; Kuipers (2011), pp. 559–560.

[28]CJEU, *European Parliament v Council,* Case C – 436/03 [2006], Judgment of 2 May 2006.

[29]Van der Weide and De Tavernier (2012).

[30]Council Directive 85/577/EC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises, OJ L 372/31 now replaced by Directive 2011/83/EU of the European Parliament and Council of 25 October 2011 on consumer rights, OJ L 304/64 (Consumer Rights Directive or CRD); Council Directive 90/314/EC of 13 June 1990 on package travel, package holidays and package tours, OJ L 158/59 (Package Travel Directive) now replaced by the European Parliament and Council Directive 2015/2302/EU of 25 November 2015 on package travel and linked travel arrangements, OJ L 326/1 (New Package Travel Directive); Council Directive 93/13/EC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95/29; Directive 97/7/EC of the European Parliament and Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144/19 now replaced by the CRD; Directive 1999/44/EC of the European Parliament and Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees OJ L 171/12 (Consumer Sales Directive or CSD).

[31]Directive 2005/29/EC of the European Parliament and Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ L 149/22, Consumer Rights Directive, New Package Travel Directive.

Firstly, the Explanatory Memorandum of the pOSD reads, *inter alia,* that "the choice of a Directive leaves Member States freedom to adapt the implementation to their national law".[32] Furthermore, according to the Explanatory Memorandum of the pDCD "the proposal does not determine whether the contract for the supply of digital content is to be considered as a sales, services, rental or a *sui generis* contract; it would leave this decision to Member States. A Regulation would require a much more detailed and comprehensive regime than a Directive in order to allow its effects to be directly applicable. As a consequence, this would have considerably more interference into national laws".[33]

However, this positive picture presented by the European Commission needs to be nuanced in some way. Interestingly this statement appears to be valid when comparing a minimum harmonisation directive with a regulation. This is because of the fact that minimum harmonisation directives contain semi-mandatory rules directed to the Member States. As Kurcz (2001) interestingly points out although "the applicable Community legislation sets a floor, the Treaty itself sets a ceiling and the Member States are free to pursue a discretion between these two parameters".[34] Yet, this does not seem to be the case when comparing a full harmonisation directive, like the pDCD or the pOSD, with an opt in instrument, as it was the case for the, now withdrawn, pCESL as, in contrast to the above scenario, total harmonisation directives, "conflate the floor and ceiling leaving the Member States with no room for manoeuvre. They must implement the standard provided for by the directive, without departing from it; neither in favour of consumers, nor in favour of businesses".[35] Consequently, as Beale (2016) rightly notes "in many respects [the Proposals] are much more intrusive upon the laws of the Member States than the [p]CESL would have been, in the sense that they will result in a larger change in the Member State's existing consumer protection".[36] Furthermore, leaving various matters open to be determined at national level within two full harmonisation directives is not as unproblematic as it sounds, as it opens up the possibility of fragmentation of EU law at national level. What is more interesting is that within the 2001 Communication on European Contract Law ('2001 Communication'),[37] which was the first document opening up the discussion for creating a truly European Contract Law, these potential divergences, which are presented within the Proposals as a positive step, were seen by the European Commission as one of the major problems for the uniform application of EU law. More specifically, within the 2001 Communication it was stated that "the absence of a uniform understanding in EC [now EU] law of general terms and concepts at least in specific

[32]pOSD, p. 8; The same statement is made in the pDCD, p. 6.

[33]pDCD, p. 6.

[34]Kurcz (2001), p. 296.

[35]Manko (2015), p. 20.

[36]Beale (2016), p. 6.

[37]Communication from the Commission to the Council and the European Parliament on European Contract Law, COM (2001) 398 final.

or linked areas may lead to different results in commercial and legal practice in different Member States".[38] It is therefore questionable and interesting how a situation, characterised by the European Commission itself, as completely problematic is now regarded as the way forward.

Secondly, in both Proposals, the European Commission states that "the choice of full harmonisation will lead to simple and modern rules that remove contract law barriers and create a favourable legal framework for businesses while at the same time ensuring that consumers benefit from the same high level of consumer protection throughout the EU".[39]

Again, although as will be shown in this chapter this statement appears to be true regarding specific issues regulated by the Proposals, this can be argued to be solely the one side of the story. More specifically, as both Proposals are full harmonisation measures, if approved as currently standing, they will result, as will be exemplified later on, in significant reductions in consumer protection in various Member States, removing at certain instances several rights and remedies that consumers currently enjoy.

2.3 Comments

Based on the above analysis it becomes clear that the European Commission has actually moved away from the failed pCESL, in legal form, introducing the Proposals as full harmonisation directives. All in all this "moving away" from unification to total harmonisation, can be seen as one of the awaited changes for the modified pCESL. However, although in theory, this swift cannot be argued to be wrong considering the Proposals limited substantive content, in practice the idea of introducing two full harmonisation directives is not as unproblematic as it sounds, as it opens up the possibility of fragmentation of EU law, as well as of the reduction of consumer protection at national level.

[38] Ibid, p. 11.

[39] pOSD, p. 8; pDCD, p. 6.

3 Scope of Application: Both Widened and Narrowed, Yet in Places Unclear

3.1 Territorial Scope of Application: Adding Domestic Contracts to the Picture

Article 4(1) of the withdrawn Regulation of the pCESL read that the Common European Sales Law may be used for cross-border contracts.[40] In contrast to this exclusive cross-border character of the pCESL, that was kept intact by the European Parliament, the European Commission introduced both Proposals as applying to both cross-border and domestic transactions extending therefore the territorial scope of application of the pCESL. According to the Explanatory Memorandum of both Proposals, a targeted set of fully harmonised rules for digital content and for the online sales of goods, both domestically and cross-border, will ensure a fully harmonised high level of consumer protection throughout the EU and will facilitate businesses to sell goods in the EU, in conformity with Articles 38 and 16 of the Charter of Fundamental Rights. Despite this general observation made by the European Commission no clear explanation is given within the Proposals regarding this extension.

Can this be regarded as a positive or as a negative alteration? The question of whether the European contract law legislative proposal shall cover both cross-border and domestic transactions has long been on the table.

Various legal scholars have argued that the pCESL should cover solely cross-border contracts. This view was based on three main arguments. Firstly, from a constitutional perspective, limiting the application of the optional instrument to cross-border transactions solely was seen by certain EU private law experts as required by the principles of subsidiarity and proportionality found in Article 5 (3) and (4) of the Treaty of the European Union (TEU). More specifically, according to Twigg Flesner, "EU legislation dealing only with cross-border transactions would be in accordance with subsidiarity, because individual Member States cannot create a legal framework to regulate cross-border transactions that would be applicable in all the other Member States".[41] Furthermore, from a political perspective, bringing forward an exclusive cross—border instrument could be regarded as the safest option available to gain the required political support of the Member States.[42] Lastly, from a socio-economic perspective, limiting this optional instrument to cross border transactions would "leave some room to individual Member States to respond to particular local challenges for consumer protection,

[40]Yet, according to Article 13 of the Regulation of the pCESL, Member States had the option to extend it to purely internal contracts.

[41]Twigg Flesner (2011), p. 251.

[42]Basedow and others (2011), p. 421.

at least to the extent that this is compatible with existing harmonising directives and the EU treaties".[43]

Yet, this approach can be argued to be quite restrictive and three main arguments will be put in place why this extension to domestic contracts appears overall to be a positive amendment.

Firstly, from a commercial perspective, a limitation to cross-border contracts would have led consumers and traders to be subject to two different contract law regimes, one for purely domestic and one for cross-border contracts. "This would clearly weaken the instrument's attractiveness".[44] In fact, considering that most businesses who sell cross-border proceed additionally to domestic transactions, a single operating system is much more appealing and useful "in order to achieve the desired rationalizing effect and avoid the complexities of working with parallel contractual regimes".[45] Furthermore, it has been argued, in the discussions that preceded the introduction of the pCESL, that the "a consumer who is looking on the Internet for a good deal should be in the position to press the "blue button"[46] irrespective of whether the seller has its seat in the same or in another Member State. Only then will the parties be convinced that the optional instrument is not another foreign law, but part of their own legal system".[47]

Secondly, from a national law perspective, having in mind that the European Commission has now moved from a complete set of contract law to specific contract law rules, one could fairly argue that limiting the scope of these specific provisions solely to cross-border contracts would have created extended legislative incoherence and fragmentation at national level. More specifically, national legislators would have been forced to modify specific contract law rules, regarding for example conformity with the contract and available remedies, solely for cross—border contracts, subjecting in this way consumers and professionals to different legislative provisions for these specific issues while the rest of the contract law provisions would have been the same irrespective of whether the consumer and the supplier had their habitual residence and seat, accordingly, in the same Member State.

Lastly and most importantly, from an EU law perspective it can be initially claimed, in response to the principle of subsidiarity argument brought forward by various EU private law experts, that in a commercial market that disregards internal frontiers[48] "subjecting internal and cross-border contracts to different legal regimes

[43]Twigg Flesner (2015), p. 245.

[44]Basedow and others (2011), p. 421.

[45]Ibid, p. 421.

[46]Meaning a button showing the European flag (12 golden stars) the electronic pressing of which, by the consumer, would trigger the application of the optional instrument (pCESL); See Schulte-Nölke (2007), pp. 348–349.

[47]Fuchs (2011), p. 5.

[48]Considering that according to Article 26(2) of the TFEU "the internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties".

is in fundamental opposition to the spirit of the internal market".[49] In practice, as it has been fairly argued, "the general goal of attaining a functional internal market cannot be attained regardless of divergences among the legal systems of the different Member States. Otherwise there is a risk of market fragmentation".[50] Furthermore, "it would [have] be[en practically] difficult to establish clear-cut criteria for distinguishing between domestic and cross-border contracts"[51] especially for transactions completed online. This is the reason why the majority of consumer contract law directives so far have not in fact drawn this distinction. Considering that the European Commission has now shifted from unification to harmonisation, practically having just two cross-border solely directives applying in parallel and together with multiple both cross-border and domestic directives would have additionally led to horizontal fragmentation at EU law level.

3.2 Exclusive Distance Sale of Goods vis à vis on Premises and Distance Sale of Digital Content

As originally proposed the pCESL, would have applied to distance, off premises and on premises contracts[52] for both the sale of goods and the supply of digital content. Interestingly although this appears to be, according to its Article 3, the scope of the pDCD, this does not appear to be the case for the pOSD. More specifically, according to Article 1(1) of the pOSD, the latter applies solely to online and other distance sales of goods.[53] In relation to face-to-face contracts for the sale of goods, according to Article 19 of the pOSD these will continue to be regulated by the Consumer Sales Directive (CSD).[54] Looking at this confusing picture one may initially ask why there should be such a limitation for the pOSD?

It appears that the main reason behind this limitation lies in the fact that, although the European Commission could demonstrate a need for harmonisation of online and other distance contracts, it could not additionally demonstrate such need for on and off premises contracts.[55] Yet, according to the Explanatory

[49]Lando (2011), p. 213.

[50]Arroyo Amayuelas (2016), pp. 478–479.

[51]Basedow and others (2011), p. 421.

[52]Although the European Parliament in its Legislative Resolution of 26 February 2014 suggested for the pCESL to be limited solely to distance contracts.

[53]Although it must be noted that the term "online" does not appear to bear any real significance. In practice, within the Explanatory Memorandum of the pOSD it is stated within a footnote that "for the purpose of this Explanatory memorandum, any reference to "online sales" shall be understood as "online and other distance sales" where within the Directive itself it is not defined within Article 2 but it is used various times within its Preamble and within Article 19 regarding the amendments to other Directives. Therefore, one could fairly argue that it could be totally erased.

[54]Supra n30.

[55]Loos (2016), p. 4.

Memorandum of the pOSD provided that "the Commission has, in the context of its Regulatory Fitness and Performance Programme, launched an in-depth analysis of the existing EU consumer legislation...its possible conclusions if pointing to the need for a Commission initiative on the face-to-face sales of goods, could feed into the progress made by the co-legislators on the proposal for online and other distance sales of goods".[56] However, one could fairly ask why has the Commission followed this "sectorial approach",[57] currently excluding face to face contracts, notwithstanding this in depth analysis *was*[58] being in progress? According to Dalli (2016) the European Commission "struggles to explain convincingly...how this...submission will lead to any real benefits since (i) it is doubtful whether it will actually result in early adoption because the results of the Fitness Check on consumer rules (still to be completed) will have to feed into the debate about the proposals, and (ii) if the proposals are indeed adopted without taking into account the results of the Fitness Check there is the risk of non-corresponding rules for online and offline goods".[59] More specifically, this sectorial approach can be argued to be problematic in two different perspectives.

Firstly, from a EU law perspective, although based on the definition given in Article 1(1) of the pOSD, it is clear that the Proposal is aimed at cross border and domestic consumer sales contracts concluded at a distance only, this limitation might in practice increase the risk of borderline disputes over whether the rules of the pOSD are applicable in specific cases which include both distance and face to face elements regarding the conclusion of the contract. More specifically, in a case

[56]pOSD, Explanatory Memorandum p. 3.

[57]Smits (2016), p. 8.

[58]It should be noted that, in June 2017, the European Commission completed its Fitness Check of consumer and marketing law and its evaluation of the CRD. Unsurprisingly the results show that "national ministries, business and consumer organisations alike strongly support having a single set of rules on offline and online consumer sales. They believe that bringing the...[CRD's] rules into line with those of the...[pOSD] would improve transparency, reduce complexity and make the system easier to understand for both consumers and traders. This would make it easier to buy and sell across borders, boost competition and cut traders' compliance costs and prices", see Commission Staff Working Document, Report of the Fitness Check on Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'); Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts; Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers; Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees; Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests; Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising, SWD (2017) 209 final, p. 63.

[59]Dalli (2016), p. 8.

where a consumer negotiates and completes a transaction for the purchase of a laptop over the phone, through the call centre of a local supplier, yet three days before proceeds to a double visit to the local store of the supplier, to find out about the specifications of the laptop, as well as to negotiate about the terms and conditions of the sale, would that be clearly regarded as a distance sale contract and therefore the pOSD provisions should apply? Or could one argue that this type of transaction should be regarded, instead, as a face to face contract, and the CSD's provisions would instead be applied, considering that what is vital for characterising a specific contract as a distance sale contract is, according to Article 2(e) of the pOSD, "the *exclusive use*[60] of one or more means of distance communication, including via internet, *up to and including*[61] the time at which the contract is concluded"?

Moreover, the distinction between distance and face-to-face sale of goods contracts might lead to great complication at national law level. As Manko (2016) comments "for face-to-face transactions. . .Member States will be allowed to preserve their more consumer-friendly rules, whilst for online transactions they will have to stick precisely to the level provided for in the proposed directive".[62] This can be argued to be true for the United Kingdom, Portugal, Lithuania and Greece[63] that allow consumers to reject defective goods and demand a refund, without waiting for the businesses to attempt a repair or replacement. "In consequence, those Member States which wish to keep a higher level of protection for offline sales, will have to introduce a dual regime of consumer sale of goods rules – an online regime. . .and an offline regime".[64] Such a scenario will inevitably lead to national fragmentation of law. More importantly, in practice "given the increasing importance of the omni-channel distribution model (i.e. selling at the same time via multiple channels such as directly in a shop, online or otherwise at a distance)"[65] establishing different rules for distance and face to face sale of goods contracts will force traders to run in parallel two separate systems for identical sale of goods transactions. Such a scenario can be argued to be confusing and uninviting for traders, as well as consumers that will enjoy different rights, in case of non-conformity, depending on whether they will buy the good at distance or face-to-face.

[60]Emphasis added.

[61]Emphasis added.

[62]Manko (2016), p. 4.

[63]Schulte-Nölke and others (2008), p. 675.

[64]Manko (2016), p. 4.

[65]pOSD, Explanatory Memorandum p. 3.

3.3 Shrinking the Personal Scope of Application of the pOSD and of the pDCD: Excluding B2B

In contrast to the pCESL, which covered business to consumer contracts (B2C) contracts, as well as business-to-business contracts (B2B),[66] when one of the two businesses qualified as a small to medium sized enterprise (SME),[67] the personal scope of both the pDCD and the pOSD is expressly limited[68] solely to B2C contracts. This limitation comes as no surprise for two main reasons.

Firstly, one shall not forget the great opposition and criticism received by the pCESL regarding this matter. Unsurprisingly the selective B2B approach followed by the pCESL was regarded by various academics as full of uncertainties and problems. More specifically, although one could admit that very detailed criteria were available as to when a business could qualify as an SME,[69] these were quite complex[70] and even if one could, in theory, find his way out, in practice it was difficult to investigate whether a potential customer was actually one before the conclusion of the contract.[71] In practice, how possible is it for an enterprise to find out whether the other party has an annual turnover not exceeding EUR 50 million or an annual balance sheet total not exceeding EUR 43 million? Secondly, according to the Explanatory Memorandum of the pOSD,[72] the B2C only option was the one favoured by the majority of Member States and businesses in the consultations carried out before the publication of the Proposals.

One could interestingly ask can this amendment be regarded as a positive or as a negative one? In practice, it can be fairly argued that the shrinking of this extended, yet the European Commission can see selective, personal scope of application of the pCESL as both a positive and negative amendment.

More specifically, by limiting the scope of both Proposals to cover solely B2C contracts, rather than additionally B2B contracts, when one of the two businesses qualifies as an SME can be argued to be a positive amendment as it erases the practical problem, faced by the pCESL, of investigating whether a specific business can be regarded as an SME. Furthermore, from a consumer perspective, considering that the Proposals are introduced as a supplement to the existing EU consumer

[66] According to Article 7 of the Regulation of the pCESL.

[67] However, according to Article 13(b) of the Regulation of the pCESL Member States had the option to make the Common European Sales Law available for contracts where all the parties were traders but none of them was an SME.

[68] According to Article 1 of the pDCD and Article 1(1) of the pOSD.

[69] According to Article 7(2) of the Regulation of the pCESL "an SME is a trader which (a) employs fewer than 250 persons; and (b) has an annual turnover not exceeding EUR 50 million or an annual balance sheet total not exceeding EUR 43 million, or, for an SME which has its habitual residence in a Member State whose currency is not the euro or in a third country, the equivalent amounts in the currency of that Member State or third country".

[70] Law Commission and the Scottish Law Commission (2011), p. 89.

[71] Dannemann (2013), p. 40.

[72] pOSD, Explanatory Memorandum, p. 9.

legislation,[73] granting additional rights and protection solely to the consumer party boosts, firstly, the latter's confidence and assists him to enter into a digital contract much more easily, feeling more secure and protected and, secondly, the consistency of the consumer *acquis* as a whole.[74]

On the other hand, it has been fairly argued that from a business perspective "to leave B2B contracts entirely to one side would be to miss a real opportunity to provide a simple system by which traders may make simple online purchases without having to worry about withdrawal rights, inadequate information or unfair terms. This would make it significantly easier for traders, particularly SMEs, to do business with each other across borders, and thus would contribute to the development of the Internal Market".[75] Furthermore, although limiting the scope of both Proposals erases the problem of identifying whether a business operates as an SME in practice another similar problem might be created. More specifically, in practice it might be difficult to know, especially for online sales of goods and the online supply of digital content whether the prospective customer is a consumer or a business. As Beale (2016) comments "many businesses are run from home rather than from an obviously business address, and there is no guarantee that the means of payment (such as a debit or credit card) will enable the trader to detect that the customer is a business".[76]

3.4 Type of Contracts Covered: Online Contracts for the Sale of Goods and Contracts for the Supply of Digital Content: As Clear as That?

The withdrawn pCESL could be used according to Article 1 of the Regulation of the pCESL, for contracts for the sale of goods, for contracts for the supply of digital content, as well as for contracts for related services.[77] As it has become clear, the two main types of contracts covered by the pCESL are divided accordingly within the two Proposals.

[73] Supra n30 and n31.

[74] Within the consumer *acquis* protection is granted, in all related directives, solely, to national persons acting outside their trade or profession (with the exception of the New Package Travel Directive (supra n30) that uses the notion of traveler, rather than consumer, thus covering additionally business travelers).

[75] Beale (2016), p. 28.

[76] Ibid, p.28.

[77] Meaning for repair and maintenance contracts regarding goods sold.

Regarding contracts for the sale of goods,[78] according to the title of the pOSD, the Proposal covers certain aspects concerning contracts for the online[79] and other distance *sales of goods*.[80] Yet, reading Article 1(1) of the Proposal one notes that the phrase "sale of goods" is missing from its content. It only becomes apparent in Article 1(2) that the European legislator is primarily concerned with the sale of goods where it is stated that "this Directive shall not apply to distance contracts for the provision of services. However, in case of sales contracts providing both for the sale of goods and the provision of services, this Directive shall apply to the part relating to the sale of goods". Two comments must be put forward at this point.

Firstly, one could claim that the phrase "sale of goods" should have been inserted for purposes of clarity additionally in Article 1(1). Secondly, regarding mixed contracts according to Recital 12 of the Preamble "where a contract includes elements of both sales of goods and provision of services, the Directive should apply only to the part relating to the sale of goods in line with the approach taken by Directive 2011/83/EU". Yet, the picture within the Consumer Rights Directive (CRD)[81] is not so crystal clear. More specifically, although Recital 50 of the preamble to that directive, regarding the right of withdrawal, states that "for contracts having as their object both goods and services, the rules provided for in this Directive on the return of goods should apply to the goods aspects and the compensation regime for services should apply to the services aspects", Article 2 (5) of that directive defines contracts having as their object both goods and services as sales contracts. As Loos (2016) fairly argues "it is therefore uncertain whether the Court of Justice will follow the European Commission's interpretation of the Consumer Rights Directive on this point"[82] and it could therefore be suggested that the European legislator should attempt to clarify it further.

Regarding contracts for the supply of digital content, the notion of digital content appeared for the first time in EU legislation in 2011. More specifically, both the CRD,[83] as well as the pCESL,[84] defined this notion in their content.

---

[78]The definition of a "sales contract", provided in Article 2(a) of the pOSD appears to be in line with the meaning ascribed to this notion by the pCESL (Article 2(k) of the Regulation), as well as by the CSD (Article 1(4)).

[79]Supra n53.

[80]Emphasis added.

[81]Supra n30.

[82]Loos (2016), p. 5.

[83]According to Article 2(11) of the CRD "'digital content' means data which are produced and supplied in digital form". One must note that Recital 19 of the Preamble goes further to explain that "Digital content means data which are produced and supplied in digital form, such as computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means".

[84]According to Article 2 (j) of the Regulation of the pCESL 'digital content' means data which are produced and supplied in digital form, whether or not according to the buyer's specifications, including video, audio, picture or written digital content, digital games, software and digital content which makes it possible to personalise existing hardware or software; it excludes: (1) financial services, including online banking services; (2) legal or financial advice provided

The notion of digital content is given in Article 2(1) of the pDCD. More specifically, according to this definition "'digital content' means (a) data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software, (b) a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer, and (c) a service allowing sharing of and any other interaction with data in digital form provided by other users of the service". Looking at this definition one realises that the European legislator has gone beyond the former definitions as it brings forward a broad concept that encompasses, apart from data produced and supplied in digital form, "digital services"[85] "thereby covering such diverse services as Cloud Computing, social networks and media such as Facebook or Twitter, e-commerce and trading platforms such as Amazon or eBay, search engines such as Google, blog portals, data storage systems, web-streaming, or visual modelling files for 3D printers.".[86] Interestingly, "the creation of new digital content and the amendment of existing digital content by consumers or any other interaction with the creations of other users" was explicitly excluded from the scope of the pCESL according to Article 2(j)(vi) of the pCESL.

Furthermore, one must comment that the pDCD, and the pOSD, diverge from the CRD regarding the inclusion of supply of digital content via a tangible medium. In practice, although the pDCD applies to goods, such as DVDs and CDs, incorporating digital content in such a way that the goods function only as a carrier of the digital content,[87] thus treating such supply as one of digital content, within the CRD such supply is understood differently. More specifically, according to the latter "digital content means data which are produced and supplied in digital form, such as computer programs, applications, games, music, videos or texts" clarifying, furthermore, that "if digital content is supplied on a tangible medium, such as a CD or a DVD, it should be considered as goods"[88] Therefore, based on the wording of the latter directive, these CDs or DVDs would be considered, instead, as sale of goods and will, if needed, be examined under the provisions of the pOSD, and not those of the pDCD, for their possible non-conformity. This theoretical asymmetry between the two legislative tests is problematic and must be solved by the European legislator before the Proposals becomes directives. One must not forget that inconsistent approaches between consumer law directives was one of the main identified problems in the area of EU consumer contract law that led the Commission started

in electronic form; (3) electronic healthcare services; (4) electronic communications services and networks, and associated facilities and services; (5) gambling; (6) the creation of new digital content and the amendment of existing digital content by consumers or any other interaction with the creations of other users.

[85]Beale (2016), p. 11.

[86]Spindler (2016), p. 5.

[87]Recital 12 of the pDCD; Additionally according to Article 1(3) of the pOSD "this Directive shall not apply to any durable medium incorporating digital content where the durable medium has been used exclusively as a carrier for the supply of the digital content to the consumer".

[88]Recital 19 of the Consumer Rights Directive.

thinking about the need for more far reaching action at EU level in this area of law back in 2001.[89] Therefore, such an asymmetry shall not arise again, 15 years after it was firstly identified.

Yet, the most problematic and controversial feature of the notion of digital content can be found in Recital 11 of the pDCD regarding embedded digital content. More specifically, according to this Recital the Proposal "should not apply to digital content which is embedded in goods in such a way that it operates as an integral part of the goods and its functions are subordinate to the main functionalities of the goods". Two points must be made regarding this feature.

Firstly, it has already been clarified by the Court of Justice of the European Union (CJEU), on numerous occasions,[90] that "the preamble to a Community act has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording". Therefore, "[w]hilst a recital in the preamble to a regulation may cast light on the interpretation to be given to a legal rule, it cannot in itself constitute such a rule".[91]

Furthermore, this definition is quite vague and complex. More specifically, the notions of being an "integral part" and of "subordination" of digital content to the "main functionalities" of the goods, are not defined in any way in the Proposal. Therefore, how do you draw the line between a single contract for the sale of goods with embedded digital content and a "mixed"[92] contract for the sale of goods and the supply of digital content? Although the answer might be easy for a toy that is advertised as a moving and talking toy therefore the digital content can be easily be regarded as an integral part of the toy, this does not appear to be the case for a laptop sold with Microsoft Office or Windows preinstalled on it. Again, these questions need to be answered.[93]

[89]COM (2001) 398 final.

[90]CJEU, *Hauptzollamt Bremen v J. E. Tyson Parketthandel GmbH hanse j*, Case C – 134/08, Judgment of 2 April 2009, par.16; CJEU, *Deutsches Milch-Kontor GmbH v Hauptzollamt Hamburg-Jonas*, Case C-136/04, Judgment of 24 November 2005, par. 32; CJEU, *Criminal proceedings against Gunnar Nilsson and others,* Case C-162/97, Judgment of 19 November 1998, par.54; CJEU, *Giuseppe Manfredi v Regione Puglia,* Case C-308/97, Judgment of 25 November 1998, par.30.

[91]CJEU, *Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung,* Case C - 215/88, Judgment of 13 July 1989, par 31.

[92]According to Article 3(6) of the pDCD "where a contract includes elements in addition to the supply of digital content, this Directive shall only apply to the obligations and remedies of the parties as supplier and consumer of the digital content". See Manko (2016), p. 12; Wendehorst (2016), pp. 7–8.

[93]It must be noted that Article 9 of Annex I of the pCESL dealt with mixed purpose contracts.

3.5 Comments

Looking at the above analysis one may conclude that again the European legislator has brought forward a modified pCESL in term of its scope of application both widened and narrowed. More specifically, both Proposals are wider, in that they apply additionally to domestic contracts and digital services contracts, nevertheless are narrower in that they can be employed solely for B2C transactions. Furthermore, one of the most interesting modifications noted is that the pOSD may be used solely for distance B2C transactions. Looking at this sectorial approach followed by the pOSD *vis à vis* the comprehensive approach ascribed to the pDCD, applying additionally to on and off premises transactions, as well as to the cross—border and domestic contracts approach followed by both the pOSD and the pDCD, one may fairly argue that the European Commission's overall approach regarding the scope of the Proposals is asymmetrical and consequently controversial. Although on the one hand, it follows a holistic approach eliminating in this way the possibility of various problems arising, such as that of a dual regime and of legislative incoherence, regarding cross border and domestic contracts, at both EU and national level, on the other hand, it limits the pOSD's scope, to cover solely distance contracts, opening up the possibility for facing quite similar problems. Lastly, the above analysis has shown that the scope of the pOSD and pDCD is at certain points unclear as to the types of contacts covered by each Proposal. More specifically, it is difficult at certain instances to ascertain where to draw a line between digital content contracts and sale of goods contracts, a problem inexistent or inconsequential in the pCESL, considering the asymmetries and vagueness in language especially regarding the meaning of "supply of digital content via a tangible medium", as well as the complex notion of "embedded digital content".

4 Content: Back to Piecemeal EU Consumer Contract Legislation?

Apart from examining the form and scope of the Proposals, it is vital to investigate the extent to which, if at all, these legislative initiatives depart from the content of the pCESL regarding their content. Interestingly reading through the provisions of the Proposals one realises that the provisions of the Proposals appear both limited and different *vis à vis* those of the pCESL.

4.1 Limited Content: A Missed Opportunity

According to Recital 6 of the Regulation for a pCESL "Differences in national contract laws. . .constitute barriers which prevent consumers and traders from

reaping the benefits of the internal market. Those contract-law-related barriers would be significantly reduced if contracts could be based on a single uniform set of contract law rules irrespective of where parties are established. Such a uniform set of contract law rules should cover the full life cycle of a contract and thus comprise the areas which are the most important when concluding contracts". Based on this argument the pCESL included rules on a wide variety of topics including, *inter alia*, formation of contract, interpretation of contract, content and effects of contract, unfair contract terms, obligations and remedies of the parties, damages, restitution and prescription, thus bringing forward "an almost complete law of contract".[94]

In contrast, the Proposals are extremely limited in scope. According to Recital 11 of the pOSD the Proposal includes "rules on conformity requirements, remedies available to consumers for lack of conformity of the goods with the contract and modalities for their exercise". Similarly, according to Recital 8 of the pDSD the Proposal includes "rules on conformity of the digital content, remedies available to consumers in cases of lack of conformity of digital content with the contract and certain modalities for the exercise of those remedies...also...certain aspects concerning the right to terminate a long term contract, as well as certain aspects concerning the modification of the digital content". Reading these provisions one realises that the Proposals are in practice, essentially, resembling the content of the CSD, rather than that of the pCESL, regulating yet the online sale of goods and the supply of digital content accordingly.

In practice, although one of the main reasons the pCESL was withdrawn was that its scope was regarded as too broad by many Member States[95] and therefore too intrusive one cannot remain silent on the fact that the Proposals' coverage is too narrow and therefore "the number of differences between the laws of the Member States that may continue to worry traders [and consumers] will be greater under the current Proposals than they would have been had the CESL been adopted".[96] More specifically, the Proposals leave, unfortunately, outside the scope of their application controversial issues that were in actual need of regulation at EU level, considering the varying, and at various instances opposing positions of national laws regarding these matters, such as the necessary requirements for the formation of a contract, the time for the conclusion of a contract, the effect of a mistake, as well as the right to damages.[97] These omissions can be regarded as a missed opportunity of the European Commission to eliminate legal barriers regarding cross border transactions.

[94]Ibid, p. 25.

[95]Supra n14; Regarding the United Kingdom see for example UK Ministry of Justice (2012).

[96]Beale (2016), p. 25.

[97]The latter will be discussed in detail within this section.

4.2 *Different Content: A Complex Duo*

Apart from the issues totally omitted from their content, reading through the Proposals one realises that several of their actual provisions depart furthermore from the corresponding provisions found in the pCESL. More importantly, one notes that the two Proposals, interestingly, appear at certain instances, to diverge, unjustifiably, additionally in between them. Based on these initial observations this chapter will focus, in parallel, on the key features of the Proposals[98] *vis à vis* the pCESL and *vis à vis* one another, if applicable.

Conformity Criteria Within the pOSD and pDCD

Two Partly Different Sets of Conformity Criteria

Regarding the issue of conformity with the contract, Articles 4 to 8 of the pOSD appear to follow closely Articles 99–105 of Annex I of the pCESL. Interestingly the pOSD follows "a number of novelties"[99] found in the pCESL yet with certain modifications. Firstly, Article 4(1) of the pOSD, in line with Article 99(1)(a) of Annex I of the pCESL, requires goods to conform to the content of the contract. More specifically, according to this Article "the seller shall ensure that, in order to conform with the contract, the goods shall, where relevant: (a) be of the quantity, quality and description required by the contract. . .". "Likewise, only precontractual statements which are 'an integral part of the contract' [would be]. . .binding on the seller".[100] Secondly, according to Article 7[101] of the pOSD "goods must be free from any right of a third party". However, the Proposal does not proceed, similarly as the pCESL in Article 102(2) of Annex I, to answer the "incidental question of which intellectual property law should govern the issue of whether the goods. . .are free from or cleared of such rights or claims".[102] Furthermore, Article 8 of the pOSD, following Article 105 and consequently Article 142 of Annex I of the pCESL, introduces a detailed set of provisions regarding the relevant time for establishing non-conformity, including rules on whether the goods were installed by the seller or under the seller's responsibility. Lastly, the pOSD[103] requires that goods "meet both the "subjective" and "objective" conformity requirements at the time of the conclusion of the contract unless the consumer knew of the specific condition of the goods and the consumer *expressly*[104] accepted this specific

[98] Supra n18.
[99] Smits (2016), p. 9.
[100] Manko (2016), p. 5.
[101] Following Article 102 of Annex I of the pCESL.
[102] Schuller and Zenefels (2013), p. 597.
[103] Article 4(3) of the pOSD.
[104] Emphasis added.

condition when concluding the contract".[105] Although this improved[106] formulation is taken again from the pCESL[107] one must admit that the pOSD version strengthens the position of the consumer as it requires not only that the latter was aware and has accepted the defect, as it is the case with the pCESL, but also that he has done so explicitly.

On the other hand, the criteria for the conformity of the digital content with the contract can be found in Article 6 of the pDCD. Although Article 6(1) of the pDCD, containing the contractual criteria, can be seen as resembling Article 4 of the pOSD, as well as Articles 99(1) and 100 (a) of the pCESL, save that the pDCD encompasses various innovative "features that are specifically relevant to digital content, such as "functionality, interoperability and other performance features such as accessibility, continuity and security", and also updating",[108] this does not appear to be the case for the statutory criteria found in Article 6(2). More specifically, Article 6(2) reads "to the extent that the contract does not stipulate, where relevant, in a clear and comprehensive manner, the requirements for the digital content under paragraph 1 the digital content shall be fit for the purposes for which digital content of the same description would normally be used including its functionality, interoperability and other performance features such as accessibility, continuity and security...". Reading this Article one realises that the European legislator brings forward a substantially weaker conformity test regarding these statutory requirements rendering them automatically as subsidiary criteria for ascertaining conformity[109] in contrast to Article 5 of the pOSD and Article 100(b) of the pCESL. More specifically in the latter Articles both contractual and statutory criteria must be met for the goods or digital content to conform to the contract as they are regarded as cumulative. Interestingly as Loos (2016)[110] points out "the primacy of subjective over objective criteria can lead to problems: the supplier can in fact escape from the minimum requirements set by the Digital Content Directive by mentioning only very limited usage possibilities, potentially hiding that information in standard contract terms or among an abundance of other information provided to the consumer".

More importantly, "if this is indeed meant by the Commission, it means that the conformity regime will be spread out over three different directives with partly diverging rules: the Consumer Sales Directive for face-to-face sales, the future Online and Distance sales directive for distance contracts and the future Digital

[105] Beale (2016), p. 16.

[106] Compared to the one found in the CSD.

[107] Article 99(3) of Annex I of the pCESL reads "In a consumer sales contract, any agreement derogating from the requirements of Articles 100, 102 and 103 to the detriment of the consumer is valid only if, at the time of the conclusion of the contract, the consumer knew of the specific condition of the goods or the digital content and accepted the goods or the digital content as being in conformity with the contract when concluding it".

[108] Beale (2016), p. 20.

[109] Manko (2016), p. 18.

[110] Loos (2016), p. 20.

Content directive for the supply of digital contents".[111] In practice, such a scenario will be highly problematic and unsatisfactory for two main reasons. Firstly, it would weaken the position of the consumer buying digital content *vis à vis* the position of the consumer buying tangible goods, as Article 4(3) of the pOSD renders as invalid any agreement derogating from the conformity requirements set out in its content unless the consumer knew of the specific condition of the goods and had expressly accepted it when concluding the contract. Secondly, the parallel application of both sets of criteria might pose difficulties in practice in cases that combine the sale of both goods and digital content in a single transaction. One can therefore ask why has the European legislator proceeded with the formation of two sets of partly diverging rules? Why weren't the two conformity tests merged into one as it was the case under the pCESL combining in it content both contractual and statutory criteria?

Reversal of the Burden of Proof: Raising Significantly the Level of Consumer Protection?

Despite certain similarities found between the Proposals and the pCESL regarding the issue of conformity, a fundamental difference exists regarding the presumption for non-conformity found within these three legislative documents.

More specifically, according to Article 105(2) of Annex I of the pCESL, "in a consumer sales contract, any lack of conformity which becomes apparent within *six months*[112] of the time when risk passes to the buyer is presumed to have existed at that time…"

In contrast, Article 8(3) of the pOSD reads that "any lack of conformity with the contract which becomes apparent within *two years*[113] from the time indicated in paragraphs 1 and 2 is presumed to have existed at [that]…time". According to Recital 33 of the pOSD, this change is proposed "in order to ensure higher awareness of consumers and easier enforcement of the Union rules on consumer's rights in relation to non-conforming goods". Although this is not a warranty, in practice, "with the exception of extreme cases, evidence contrary to the presumption will be very difficult for the seller to assemble, so the rebuttable presumption will, in point of fact, be almost equivalent to full and absolute warranty coverage"[114] for two years. This important alteration coupled with the fact that the Proposal is a maximum harmonisation measure can be argued to raise significantly the level of consumer protection within the EU.

Furthermore, according to Article 9(1) of the pDCD "the burden of proof with respect to the conformity with the contract at the time indicated in Article 10 shall

[111] Smits (2016), p. 9.

[112] Emphasis added.

[113] Emphasis added.

[114] Gomez (2002), p. 69.

be on the supplier". According to the Explanatory Memorandum of the latter "this reversal of the burden of proof *is not limited in time*[115] as digital content is not subject to wear and tear".[116] Although this can be argued to be overall fair,[117] raising again significantly the level of consumer protection, from a legislative perspective this permanent reversal creates again a theoretical asymmetry between the two Proposals with possible practical implications. More specifically, considering that the notion of embedded digital content is not crystal clear,[118] problems will emerge as to whether the non-conforming digital content shall be regarded as an integral part of the good on which it was installed or not. In practice, if the answer is a positive one that would mean that the shift of the burden of proof for non-conformity would be restricted to two years while if the answer is a negative one the shift would be a permanent one.[119] This is, again, highly unsatisfactory.

Remedies Available for the Buyer Within the pOSD and pDCD

Regarding the remedies available to the consumer, in contrast to Article 106 of Annex I of the pCESL that provides a free choice to the consumer between repair, replacement, withholding of performance, termination, reduction of price and damages, the pOSD and the pDCD employ instead a hierarchy of remedies.

Remedies for Non-conforming Goods Purchased at a Distance

Interestingly the pOSD follows the traditional hierarchy of remedies found in the CSD. More specifically, examining Articles 9 and 11 of the pOSD it becomes clear that in case of a lack of conformity the consumer has two remedies primarily available, namely that of repair and replacement, whereas the remedies of termination and reduction of price play solely a secondary role.

[115] Emphasis added.

[116] pDCD, Explanatory Memorandum, p. 12.

[117] Although it has been argued by Loos (2016) that for digital content supplied on a DVD or CD the burden of proof should be restricted to six months or two years. The author of this chapter does not agree with such an approach as it would lead to further legislative fragmentation and practical difficulties regarding the supply of the same digital content for the same price online and over a DVD or CD.

[118] See Sect. 3.4.

[119] Once must not forget that in practice further problems will be created as according to Article 5 (3) of the CSD "unless proved otherwise, any lack of conformity which becomes apparent within *six months* of delivery of the goods shall be presumed to have existed at the time of delivery unless this presumption is incompatible with the nature of the goods or the nature of the lack of conformity".

Repair and Replacement

Regarding repair and replacement, the pOSD follows the pCESL approach[120] in that the seller has the obligation to take back the goods at his own expense.[121] Yet, based on the important Court of Justice of the European Union ('CJEU') rulings *Weber/Putz,*[122] published a few months before the release of the pCESL, the pOSD moves one step further, in Article 10(2), to propose that when the consumer had installed the goods according to their nature and purpose, before the lack of conformity became apparent, the seller is obliged to either remove the defective goods and to reinstall the repaired or replacing goods or to compensate the consumer for the costs thereof. Furthermore, following again the wording of the pCESL,[123] the pOSD reads in Article 10(3) that "the consumer shall not be liable to pay for any use made of the replaced goods in the period prior to the replacement". This rule derives once more from the ruling of the CJEU in *Quelle*[124] decided in the context of the CSD. Looking at these provisions, one cannot but admit that the European legislator clearly aims to increase consumer protection at EU level. Yet, one cannot remain silent on the fact that various questions remain unanswered as to the practical application of these provisions. Firstly, a washing or drying machine that has broken down 19 months after being originally bought shall be replaced with a new washing or drying machine or could be simply replaced with another one used, approximately, for the same time? Secondly, as Loos interestingly asks, after receiving the replacing good, is the consumer entitled to invoke a remedy for a fresh two-year period or is he just covered for the remainder of the original two-year period?[125]

Termination

As it has been aforementioned, the remedy of termination is considered as a secondary option for the consumer within the pOSD. Apart from this shift, the pOSD differs from the pCESL regarding this remedy in that it allows the consumer to terminate, additionally, for the first time, in case of minor defects.[126] Although the meaning of the term "minor" is omitted from the content of the Proposal, this does not bear any real significance as in practice any lack of conformity will allow the consumer to terminate the contract. Furthermore, although the Proposal sets out in Article 13(1) that termination shall take place by notice, similarly to what it is

[120]Found in Article 112(1) of Annex I of the pCESL.

[121]Article 10(1) of the pOSD.

[122]CJEU, *Gebr. Weber GmbH v Jürgen Wittmer* (C-65/09) and *Ingrid Putz v Medianess Electronics GmbH* (C-87/09), Joined cases C-65/09 and C-87/09, Judgment of 16 June 2011.

[123]Article 112(2) of Annex I of the pCESL.

[124]CJEU, *Quelle AG v Bundesverband der Verbraucherzentralen und Verbraucherverbände,* Case C-404/06, 17 April 2008.

[125]Loos (2016), p. 12.

[126]Recital 29 of the pOSD.

provided in Article 118 of Annex I of the pCESL, the former does not provide any guidance as to when such a notice shall become effective, an issue that was, in contrast, tackled within the latter.[127] Such an omission can be argued to be quite important, as well as dangerous in creating divergences at national level considering the opposing expedition and receipt theories adopted by national laws regarding this matter.[128] The pOSD, in contrast to the pCESL,[129] provides detailed rules regarding the return of price and products following termination. According to Article 13(3)(a) and (b) of the pOSD the consumer shall return the goods, at the seller's expense, no later than 14 days from sending the notice of termination while the seller shall return the price paid no later than 14 days from receipt of the notice. This new provision can be argued to be problematic in that in practice the seller "may withhold payment repayment of the price until the consumer has returned the goods, burdening the consumer with the risk of the seller's insolvency or non-performance".[130] Such a provision thus "fails to achieve a fair balance of the interests at hand in case of termination of a synallagmatic contract due to a lack of conformity of the goods sold".[131]

Withholding of Performance

Furthermore, regarding the right to withhold performance although, following the paradigm of the pCESL, this is ascribed explicitly to the consumer in Article 9(4) of the pOSD, it appears that it also encompasses a subsidiary role alongside termination and reduction of price. Interestingly "one question for discussion is why the Proposal does not adopt the more nuanced rule of Art. 113 [p]CESL that provides more guidance on when the buyer is exactly allowed to withhold payment of the price".[132]

No Notification Duty

Following the paradigm of the pCESL[133] the pOSD abolishes the consumer's duty to notify the seller for lack of conformity. Conversely, the CSD gave the option to Member States, in Article 5(2), to provide that the consumer must inform the seller of the lack of conformity within a period of two months from the date on which he detected such lack of conformity. In practice, this meant that the consumer lost his

[127] Article 10 of Annex I of the pCESL.

[128] Smits (2015), pp. 59–61.

[129] The pCESL provides nothing more than a general, and vague, rule on this matter. More specifically according to Article 172(1) of the pCESL reads "where a contract is avoided or terminated by either party, each party is obliged to return what that party ("the recipient") has received from the other party".

[130] Loos (2016), p. 12.

[131] Notaries of Europe (2016), p. 2.

[132] Smits (2016), p. 12.

[133] Article 122 of Annex I of the pCESL provides a notification obligation for lack of conformity solely in sale contracts between traders.

rights in case he failed to provide the seller such notification. The abolition of this duty exemplifies the overall aim of the European legislator to increase the level of consumer protection.

Remedies for Non-conforming Digital Content

Mirroring the pOSD and the CSD, the pDCD brings forward, in Article 12, a hierarchy of remedies aiming at first instance to keep the contact intact.

Specific Performance

More specifically, according to Article 12(1) of the pDCD "in the case of a lack of conformity with the contract, the consumer shall be entitled to have the digital content brought into conformity with the contract free of charge [and within a reasonable time],[134] unless this is impossible, disproportionate or unlawful". Reading this provision one realises that the Proposal does not distinguish between the two traditional sub forms of specific performance found in the pCESL, as well as in the pOSD, that of repair and replacement. Some guidelines are yet provided within paragraph 36 of the Preamble of the Proposal which reads, *inter alia,* that "depending on technical characteristics of the digital content, the supplier may select a specific way of bringing the digital content to conformity with the contract, for example by issuing updates or requiring the consumer to access a new copy of the digital content". Yet, the omission of such examples from the main text of the Proposal shall not come as a surprise considering the variety of content and format regarding digital content contracts. More specifically, according to Mak (2016) "whereas an e-book or a movie file might be replaced, repair is harder to envisage. Malfunctioning software, on the other hand, could well be fixed through an update that repairs certain bugs. For problems with accessing data on cloud services. . .the specific performance type remedy would in that case be to restore access to the data. Seeing this diversity, it makes sense not to include specifications as to what a specific performance type remedy should look like for digital content contracts".[135]

Price Reduction or Termination

Similarly, as in the pOSD, the consumer may resort to price reduction, where the digital content is supplied in exchange for a payment of a price, or termination[136]

[134] Article 12(2) of the pDCD.

[135] Mak (2016), p. 24.

[136] Provided that according to Article 12(5) of the pDCD "the lack of conformity with the contract impairs functionality, interoperability and other main performance features of the digital content such as its accessibility, continuity and security where required by Article 6 paragraphs (1) and (2). The burden of proof that the lack of conformity with the contract does not impair functionality, interoperability and other main performance features of the digital content shall be on the supplier".

regarding non-conforming digital content only as a secondary remedy and provided that, according to Article 12(3), (a) the remedy to bring the digital content in conformity is impossible, disproportionate or unlawful; or (b) the supplier has not completed the remedy within a reasonable time; or (c) the remedy to bring the digital content in conformity would cause significant inconvenience to the consumer; or (d) the supplier has declared, or it is equally clear from the circumstances, that the supplier will not bring the digital content in conformity with the contract. Reading this exhaustive list of cases, where one may resort to these two secondary remedies, it becomes clear that this is not as exhaustive as it first seems to be. More specifically, one may question what is disproportionate and what is not. What does reasonable time mean? Furthermore, when would inconvenience be regarded as significant? These can be seen as vague notions that are left to be determined at national level thus opening up the possibility for divergences or even disagreements between national judges regarding their interpretation.

Regarding termination, the pDCD contains, in Article 13, detailed rules regarding the supplier's and the consumer's rights and obligations. More specifically, Article 13(1) reads that "the consumer shall exercise the right to terminate the contract by notice to the supplier given by any means". Yet, the pDCD, similarly to the pOSD, does not provide any guidance as to when a notice becomes effective, as it was the case under Article 10(3) of Annex I of the pCESL, which stated that "a notice becomes effective when it reaches the addressee, unless it provides for a delayed effect", thus adopting the receipt theory.[137] Some more detailed provisions could therefore be included. Interestingly, compared to the rules found in Chapter 17 of Annex I of the pCESL regarding restitution, some tailor made rules can be found in the pDCD regarding the termination of contracts for non-conforming digital content. More specifically, one could mention the supplier's duty to refrain from using the consumer's personal data[138] and his duty to provide to the consumer technical means to retrieve all content,[139] as well as the consumer's duty to stop using the digital content or making it available to third parties[140] and his duty to return the digital content that was supplied on a durable medium.[141] Yet, one cannot remain silent on the fact that in practice it is difficult or, even impossible, to monitor whether the supplier has actually stopped using the consumer's data as a whole or whether the consumer has copied, illegally, the digital content and has therefore not stopped using it.

[137] Smits (2015), pp. 59–61; Fauvarque-Cosson (2016), p. 13.

[138] Article 13(2)(b) of the pDCD.

[139] Article 13(2)(c) of the pDCD.

[140] Article 13(2)(d) of the pDCD.

[141] Article 13(2)(e) of the pDCD.

Damages: ABSENCE of a General Right to Claim Damages

Apart from repair, replacement, withholding of performance, termination and reduction of price, Article 106 of Annex I of the pCESL if the consumer had an immediate right to claim damages. Looking at the Proposals one realises that again they appear to follow a different approach both *vis à vis* the pCESL and *vis à vis* one another.

No Right to Claim Damages for Non-conforming Goods

Interestingly the consumer's right to claim damages in case of lack of conformity with the contract is not regulated by the pOSD at all. According to the Explanatory Memorandum, "the proposal leaves provisions on the consumer's right to receive compensation for the losses caused by such lack of conformity to national laws".[142] Yet, this statement is far from clear for two main reasons.

Firstly, neither the Preamble nor the text of the Proposal includes any explicit reference to the right of the consumer to claim damages according to national law. In practice, although Article 1(4) explicitly leaves rules, on the consequences of the *termination*[143] of a contract to national contract laws, this provision seems to refer to damages that are caused by termination[144] and not damages as a remedy for lack of conformity as such. Furthermore, the decision of the European legislator to employ maximum harmonisation coupled with the wording of Article 9 can be argued to bring forward an exhaustive list of remedies for the consumer.[145] More specifically, it is clear that initially the consumer can request solely repair or replacement. Moving on if repair and replacement are, *inter alia*, impossible, unlawful and significantly inconvenient the consumer has again solely two supplementary remedies, these being reduction of price and termination. Therefore, one may easily ask where does a potential right to damages actually fit into the hierarchy of remedies proposed by Article 9? Although in the implementation of the CSD many Member States, including Austria, Belgium, France and Germany,[146] did not adopt the two-stage hierarchy of remedies, allowing furthermore consumers to bring a claim for damages instead off, or as well as, a claim for repair, replacement, reduction of price and termination this possibility was available because of the minimum harmonisation character of the specific directive. This is

[142]pOSD, Explanatory Memorandum, p. 3.

[143]Emphasis added.

[144]An example of damages that are caused by termination is the case in which "the consumer decides to terminate the contract, but is only able to purchase the similar product elsewhere at a higher price. The trader will have to consult the specific national laws to establish the extent to which he is obliged to compensate the consumer for such damages" Smits (2016), p. 14; See also Fauvarque-Cosson (2016), p. 16.

[145]Loos (2016), p. 13.

[146]Schulte-Nölke and others (2008), p. 699.

not the case for a maximum harmonisation legislative instrument like the pOSD. Clearly, the European legislator needs to provide an express reference to national law within the content of the Proposal if damages may indeed be claimed at national level as a primary or supplementary remedy.

Yet, moving one step further one may question why the European legislator has not followed the example of the pCESL to grant to consumers the possibility to obtain damages at European level specifically considering the varying, as well as, at many instances, contrasting national approaches regarding this matter.[147] This omission can be regarded, again, as a missed opportunity.

Limited Right to Claim Damages for Non-conforming Digital Content

On the other hand, reading Article 14 of the pDCD, one realises that, regarding digital content contracts, the consumer has an additional right to the ones presented in Article 12 of the pDCD, namely that of claiming damages. According to this Article, "the supplier shall be liable to the consumer for any economic damage to the *digital environment*[148] of the consumer caused by a lack of conformity with the contract or a failure to supply the digital content". According to Article 2(8) of the pDCD, "'digital environment' means hardware, digital content and any network connection to the extent that they are within the control of the user". Furthermore, according to the Explanatory Memorandum of the Proposal "Article 14 establishes a right to damages *restricted to cases*[149] where damage has been done to the digital content and hardware of the consumer...".[150]

Reading Article 14, in conjunction with Article 2(8) and the Explanatory Memorandum, one cannot remain silent on the fact that the wording of this Article brings forward a restrictive nature of the right to damages "merely point[ing] up the absence of any more general right to damages".[151] More specifically, it appears that the Proposal does not cover consequential damage. This contradicts the earlier position of the pCESL regarding this matter. More specifically, Article 159(1) of Annex I of the pCESL, regarding the right to damages, reads, "a creditor is entitled to damages for *loss*[152] caused by the non-performance of an obligation by the debtor, unless the non-performance is excused". According to Article 2(c) of the Regulation of the pCESL, ""loss" means economic loss and non-economic loss in the form of pain and suffering, excluding other forms of non-economic loss such as impairment of the quality of life and loss of enjoyment". Reading this definition, it can be claimed that the pCESL gave to the notion of loss, a notion not expressly

[147] Smits (2015), pp. 209–228; Prastitou (2012) pp. 96–121.

[148] Emphasis added.

[149] Emphasis added.

[150] Explanatory Memorandum of the pDCD, p. 13.

[151] Clive (2016), p. 1.

[152] Emphasis added.

found to exist at all in the consumer *acquis,* an autonomous European legal meaning encompassing, in contrast to the pDCD, both an economic and non-economic element.

Based on the above remarks the position of the Proposal regarding this matter can be seen as, at least, problematic. One may claim that although it can be easily understood why non-economic loss in the form of impairment of the quality of life and loss of enjoyment has been excluded, as it was the case for the pCESL,[153] "it is quite wrong to exclude liability for all other losses".[154] This limited right "would of course have harsh consequences for consumers that were probably not intended by the Commission's proposal".[155] In practice, "while suppliers could be held liable if his or her digital content contained for example viruses or malware and thereby caused damages to the consumer's other software, consequential damages like those arising from third parties retrieving the consumer's online banking passwords would not (and could not) be covered, even if those were foreseeable for the supplier".[156] Additionally, the same result would be achieved in a case where a hacker, because of a bug contained in a computer's newly bought software, gains access to a consumer's computer and steals photos and other personal data.[157] As an unfortunate result both economic and non-economic consequential damage could easily occur that would remain outside the spectrum of this article. As Beale (2016) fairly comments "there is no need to give the digital content industry blanket immunity for loss other than the consumer's digital environment".[158]

The next question that comes to one's mind is whether this right can be extended at national level by national legislators. According to Article 14(2) of the pDCD, "the Member States shall lay down detailed rules for the exercise of the right to damages". Yet, does this refer to a right to damages for losses other than those to the digital environment or, following the wording of Article 14(1), solely to the detailed conditions of the exercise of the right to the digital environment's economic damage? The Proposal seems quite ambiguous regarding this matter and does not appear to provide a clear answer to this question. More specifically, although according to Recital 10 "Member States should. . .remain free to provide rules for

[153]In the case of the pCESL, it can be argued that the European legislator was heavily influenced by academics regarding this matter. More specifically Simon Whittaker in his article (Whittaker (2008), p. 114) criticised that there was "an entirely unjustified substantive breadth to the central definition of loss [in the Draft Common Frame of Reference and Expert Group Feasibility Study]". More specifically, he argued that the CJEU in the case of *Leitner* granted damages for loss of enjoyment, as the Package Travel Directive's concern was "to protect consumers in connection with tourist holidays, where loss of enjoyment is particularly important. Its reasoning was therefore, very specific to its context; the decision should certainly not be used to justify a generalisation of the size attempted by the definitions found in the DCFR".

[154]Beale (2016), p. 24.

[155]Spindler (2016), p. 21.

[156]Ibid, p. 21.

[157]Mak (2016), p. 27.

[158]Beale (2016), p. 24.

the detailed conditions for the exercise of rights, such as the right to damages to the extent not covered by the Directive", Recital 44 reads "the principle of the supplier's liability for damages is an essential element of the contracts for supply of digital content. To increase consumers' trust in digital content this principle should thus be *regulated at Union level*[159] to ensure that consumers do not suffer a detriment if their hardware or software is damaged by digital content which is not in conformity with the contract...However, it should be for Member States to lay down the detailed conditions for the exercise of the right to damages". Yet, one must not forget that the Proposal aims at full harmonisation.

4.3 Comments

Based on the above analysis, one realises that apart from differences in form and in scope, the two Proposals diverge significantly from the pCESL regarding their content.

As it has been exemplified, the content of the Proposals appears narrow leaving outside its scope of application controversial issues that are in need of regulation at European level considering the substantial differences existing at national level regarding these matters. One of the most important examples of this argument is the total omission of a right to damages, within the pOSD, and a right to damages other than loss to the consumer's digital environment, within the pDCD. This is disappointing as it will lead to national legislative asymmetries and consequently, in certain Member States, to a reduction of consumer protection.

Furthermore, substantial differences have been observed both between corresponding provisions of the two Proposals, as well as between the Proposals and the pCESL that at certain instances can be argued to raise, whereas in others can be argued to reduce the level of consumer protection. More importantly, these theoretical asymmetries between the two Proposals can be seen, as inevitably leading to practical inconsistencies.

More specifically, although the pOSD presents an improved conformity test that can be argued to strengthen the position of the consumer as compared to his position in the pCESL, this does not appear to be the case for the pDCD. Interestingly as it has been noted, although the latter encompasses various innovative digital contractual conformity features, a weaker test regarding statutory requirements is introduced. Such a theoretical asymmetry can be argued to be problematic. Similarly, although in both the pOSD and pDCD the reversal of the burden of proof, elevated to two years and forever, respectively, can be argued to raise consumer protection, one may interestingly ask whether such an asymmetry is necessary.

Furthermore, the hierarchical approach of remedies followed in both the pOSD and the pDCD, in contrast to the pCESL, regarding the consumer remedies for

[159] Emphasis added.

non-conforming goods or digital content can be argued to reduce consumer protection in certain cases. More specifically, from a commercial point of view, it can be claimed that by "giving the supplier at least one opportunity to cure the non-performance or defective performance can be a cost-effective solution. It means that consumer-buyers will not have to look for another supplier—a transaction costs argument—and it benefits businesses because they will be able to continue the contract and (in many cases) still make a profit".[160] Yet, as it can been seen this is solely to the benefit of the supplier. What about the consumer? In practice, this hierarchical approach can be argued to weaken the position of the consumer, *vis à vis* his position in the pCESL. Interestingly, although it has been argued that from a legislative perspective "adopting a similar regime [to the hierarchy of remedies that applies to consumer sales contracts on the basis of the CSD rather than to the free choice of remedies provided in the pCESL] for digital content can make the rules appear more consistent and familiar to businesses and consumers"[161] this might not always appear to be the case in practice as one must not forget that the CSD is a minimum harmonisation directive. More specifically, because of this minimum harmonisation character many Member States like Greece, Lithuania and Portugal were allowed to make all the remedies available alongside one another within their transposing legislation.[162] Furthermore, in the United Kingdom, according to the Consumer Rights Act 2015, that consolidates in one place fundamental consumer rights[163] including, *inter alia*, the provisions of the CSD, if the goods delivered are not in conformity with the contract, the consumer has an additional immediate short term right to reject[164] the goods and terminate the contract without first having to seek repair or replacement. Thus if the pOSD and pDCD are adopted in their current form in many Member States legislative fragmentation will occur, rather than legislative consistency, as regarding face to face sale of goods contracts these Member States will be allowed to keep intact their more consumer friendly rules, where for distance sale of goods contracts and digital content contracts they will have to follow strictly the provisions of the pOSD and pDCD, thus reducing consumer protection. Such problems would not have occurred had the pCESL been adopted.

[160] Mak (2016), p. 25.

[161] Ibid, p. 25.

[162] Schulte-Nölke and others (2008), p. 675.

[163] Giliker (2016), p. 2.

[164] Sections 20 and 22 of the Consumer Rights Act 2015.

5 Concluding Observations: There Is Still Way to Go for a Truly Digital European Contract Law

This chapter aims to examine the extent to which the pOSD and the pDCD have moved away from the withdrawn pCESL and the extent to which they appear to form an adequate replacement for the rebirth of a digital European contract law. Whilst the foregoing has not covered every aspect of the Proposals, *vis à vis* the pCESL, various conclusions can easily be drawn regarding the matters examined.

Based on the above analysis it has become clear that the European Commission has actually moved far away from the failed pCESL project in relation its form, its scope and its content. In practice, it appears to have move so far away that the two Proposals can be characterised as two brand new legislative initiatives, opening up a new chapter in the process of Europeanisation, rather than as an altered pCESL.[165] More specifically, looking at the Proposals' form, scope and content one might claim that this "moving away", firstly, from unification to total harmonisation, secondly, from B2C and B2B just to B2C transactions, thirdly, from solely cross—border contracts to both cross border an domestic contracts, fourthly, from on, off and distance sale of goods transactions solely to distance sale of goods transactions and, lastly and most importantly, from an "almost complete law of contract"[166] just to the regulation of the issues of conformity and remedies, these can be much more easily compared with the traditional consumer law directives, like the CSD, rather than with the failed pCESL. Consequently, despite their theoretical importance, these Proposals "from the point of view of anyone interested in the development of a more principled and coherent European contract law...are profoundly disappointing...back to the bad old days of itsy-bitsy rules on particular topics".[167]

More importantly, do these new Proposals form the adequate replacement for the rebirth of a truly digital European contract law? The pCESL was withdrawn as its content was regarded as too broad and problematic. Moreover, its efficiency as a legislative instrument and the competence of the European Union to enact it were under question. Although the problems faced by the pCESL can be seen as inexistent in the Proposals unfortunately, despite their innovative digital look, especially regarding the pDCD, which covers, *inter alia*, digital services contracts, the supply of "free" digital content and the termination of long terms contracts the Proposals do not remain without problems.

Initially, it has become clear that problems appear to exist when these two legislative instruments are examined *in parallel*[168] *vis à vis* the pCESL. More specifically, regarding their form, the idea of introducing two full harmonisation

[165] Supra n16.

[166] Beale (2016), p. 25.

[167] Clive (2016).

[168] Emphasis added.

directives is not as unproblematic as it seems, at first instance, as it opens up the possibility of fragmentation of EU law, as well as of the reduction of consumer protection at national level. Furthermore, in relation to their scope, regarding the pOSD, following a sectorial approach and leaving behind on and off premises sales of goods transactions, can be argued to generate great problems in practice, where regarding the pDCD, the complex notion of "embedded digital content" needs to be better worked out. Additionally regarding their content, one might easily ask why "a more elaborated set of provisions, also covering other aspects of the consumer sales contracts"[169] has not been proposed? On a related note the incomplete hierarchical approach followed in both Proposals regarding consumer remedies, excluding a general right to damages, can be argued to lower significantly the level of consumer protection. Lastly, various notions and phrases found in both Proposals need to be reformulated, as, as they currently stand open up, again, the possibility of practical inconsistencies at national level.

More importantly, the above analysis has shown that major difficulties exist when these two legislative instruments are examined *together*[170] *vis à vis* the pCESL. More interestingly, key theoretical asymmetries appear to exist between the Proposals, including, *inter alia*, the sectorial approach followed by the pOSD, applying only to distance sale of goods transactions *vis à vis* the comprehensive approach ascribed to the pDCD, applying additionally to on and off premises transactions. Furthermore, the weaker conformity test found in the pDCD, regarding statutory requirements, in contrast to the pOSD where both contractual and statutory criteria must be met for the goods to conform to the contract, as well as the difference between the two years presumption for non-conformity found in the pOSD against the unlimited in time corresponding presumption traced in the pDCD. Lastly, one must not forget the absence of a right to damages within the pOSD *vis à vis* the limited right for any economic damage to the digital environment of the consumer found in the pDCD. More importantly, significant inconsistencies will be encountered in practice, because of these theoretical asymmetries, if the two Proposals are *applied together,*[171] especially considering the unclear notion of embedded digital content that complicates even further the relationship between the two Proposals.

Therefore, one could claim that this new chapter of Europeanisation of digital contract law must be revised before becoming officially part of the *acquis communautaire*. The scope and provisions of the pDCD and the pOSD should be examined further and should be aligned as far as this is possible, to prevent traders and consumers from having to deal with unnecessary divergences between the two sets of legislative provisions. One could even claim that the two Proposals should be transformed into one,[172] firstly, "in particular because – upon acceptance – the

[169]Smits (2016), p. 8.

[170]Emphasis added.

[171]Emphasis added.

[172]Clive (2016).

Member States are likely to implement them together into their national laws"[173] and, secondly, considering that owing to the hybrid nature[174] of various goods "tangible goods and digital content are no longer two worlds apart".[175] What is definite is that although this appears to be new start for digital European contract law there is still way to go for actually achieving a truly digital European contract law....

References

Arroyo Amayuelas E (2016) The idea of an optional contract code. In: Twigg Flesner C (ed) Research handbook on EU consumer and contract law. Edward Elgar, Cheltenham/Northampton, pp 463–486

Basedow J and others (2011) Policy Options for Progress Towards a European Contract Law: Comments on the issues raised in the Green Paper from the Commission of 1 July 2010, COM (2010) 348 final. Max Planck Private Law Research Paper No. 11/2

Beale H (2016) Scope of application and general approach of the new rules for contracts in the digital environment: In: Depth analysis. European Parliament - Policy Department for Citizen's Rights and Constitutional Affairs PE 536.493

Clive E (2016) The proposed new digital single market contract law Directives. European Private Law News, Edinburgh. http://www.epln.law.ed.ac.uk/2016/01/19/the-proposed-new-digital-single-market-contract-law-directives/. Accessed 30 Dec 2016

Dalli H (2016) Contracts for the supply of digital content and for the online and other distance sales of goods. European Parliamentary Research Service. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/528827/EPRS_BRI(2016)528827_EN.pdf. Accessed 30 Dec 2016

Dannemann G (2013) Choice of CESL and conflict of laws. In: Dannemann G, Vogenauer S (eds) The common European sales law in context. Oxford University Press, Oxford, pp 21–81

Eidenmueller H and others (2012) The proposal for a regulation on a common European sales law: shortcomings of the most recent textual layer of European contract law. Juristenzeitung, pp 269–289

Fauvarque-Cosson B (2016) The new proposal for harmonised rules for certain aspects concerning contracts for the supply of digital content (termination, modification of the digital content and right to terminate long term contracts). In: Depth Analysis. European Parliament - Policy Department for Citizen's Rights and Constitutional Affairs PE 536.495

Fuchs A (2011) European contract law: the way forward. ERA Forum 12(1):1–5

Giliker P (2016) The Consumer Rights Act 2015 – a bastion of European consumer rights? Leg Stud. doi:10.1111/lest.12139

Gomez F (2002) Introduction. In: Bianca MC, Grundmann S (eds) EU sales directive: commentary. Intersentia, Antwerp, Oxford, New York, pp 53–78

Hesselink M and others (2007) The legal basis for an optional instrument on European contract law. Centre for the Study of European Contract Law Working Paper Series No. 2007/04. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1091119. Accessed 30 Dec 2016

James S (2011) European contract law: doubling up. https://www.cliffordchance.com/briefings/2011/10/european_contractlawdoublingup.html. Accessed 30 Dec 2016

[173] Smits (2016), p. 9.

[174] Encompassing a mixture of tangible and digital elements.

[175] Wendehorst (2016), p. 4.

Kuipers JJ (2011) The legal basis for a European optional instrument. Eur Rev Priv Law 19 (5):545–564

Kurcz B (2001) Harmonisation by means of directives. Eur Bus Law Rev 12(11/12):287–307

Lando O (2011) On a European contract law for consumers and businesses - future perspectives. In: Schulze R, Stuyck J (eds) Towards a European contract law. Sellier European Law Publishers, Munich, pp 203–216

Law Commission and the Scottish Law Commission's advice to the UK Government (2011) An Optional Common European Sales Law: Advantages and Problems. http://www.lawcom.gov.uk/wp-content/uploads/2015/03/Common_European_Sales_Law_Advice.pdf. Accessed 30 Dec 2016

Loos M (2016) European harmonisation of online and distance selling of goods and supply of digital content. Centre for the Study of European Contract Law Working Paper Series. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2789398. Accessed 30 Dec 2016

Low G (2012) Unitas via diversitas, Can the common European Sales Law harmonize through diversity? Maastricht Faculty of Law Working Paper. http://ssrn.com/abstract=1991070. Accessed 30 Dec 2016

Mak V (2016) The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content – In Depth Analysis, European Parliamentary Research Service – PE 536.494. http://www.epgencms.europarl.europa.eu/cmsdata/upload/a6bdaf0a-d4cf-4c30-a7e8-31f33c72c0a8/pe__536.494_en.pdf. Accessed 30 Dec 2016

Manko R (2015) Contract law and the Digital Single Market: Towards a new EU online consumer sales law? In-Depth Analysis, European Parliamentary Research Service – PE 568.322. http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/568322/EPRS_IDA(2015)568322_EN.pdf.Accessed 30 Dec 2016

Manko R (2016) Contracts for online and other distance sales of goods. European Parliamentary Research Service. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577962/EPRS_BRI(2016)577962_EN.pdf. Accessed 30 Dec 2016

Micklitz HW, Reich N (2012) The Commission Proposal for a "Regulation on a Common European Sales Law (CESL) – Too broad or not to broad enough? EUI Working Paper Law 2012/04. http://cadmus.eui.eu/bitstream/handle/1814/20485/LAW_2012_04_ERPL_03.pdf?sequence=3&isAllowed=y. Accessed 30 Dec 2016

Notaries of Europe (2016) Position Paper on the proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods (COM (2015) 635) and a Directive on certain aspects concerning contracts for the supply of digital content (COM (2015) 634) http://www.notaries-of-europe.eu/files/position-papers/2016/Contract-Law-CNUE-Position-Paper-11-03-16-en.pdf. Accessed 30 Dec 2016

Prastitou T (2012) Interpretation asymmetries: an obstacle to the harmonised application of European contract law. PhD Thesis, University of Bristol

Schuller C, Zenefels A (2013) Obligations of sellers and buyers. In: Dannemann G, Vogenauer S (eds) The common European sales law in context, interactions with English and German Law. Oxford University Press, Oxford, pp 581–611

Schulte-Nölke H and others (eds) (2008) EC Consumer Law Compendium - Comparative Analysis, Updated Version. Universität Bielefeld. http://ec.europa.eu/consumers/rights/docs/consumer_law_compendium_comparative_analysis_en_final.pdf. Accessed 30 Dec 2016

Schulte-Nölke H (2007) EC law on the formation of contract – from the common frame of reference to the "Blue Button". Eur Rev Contract Law 3(3):332–349

Smits JM (2015) Contract law: a comparative introduction. Edward Elgar, Cheltenham/Northampton

Smits JM (2016) The new EU proposal for harmonised rules for the online sales of tangible goods (COM (2015) 635): Conformity, lack of conformity and remedies. Maastricht European Private Law Institute Working Paper Series. https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2731811. Accessed 30 Dec 2016

Spindler G (2016) Contracts for the supply of digital content – Scope of application and basic approach – Proposal of the Commission for a Directive on contracts for the supply of digital content. https://polcms.secure.europarl.europa.eu/cmsdata/upload/22d59110-9445-4058-b889-418572bf4071/Prof%20Spindler%20-%20Contracts.pdf. Accessed 30 Dec 2016

Twigg Flesner C (2011) Good bye harmonisation by directives, Hello Cross – border only regulation? - A way forward for EU consumer contract law. Eur Rev Contract Law 7 (2):235–256

Twigg Flesner C (2015) CESL, cross-border transactions and domestic law: why a dual approach could work (although CESL might not). Eur Rev Priv Law 23(2):231–249

UK Ministry of Justice (2012) A Common European Sales Law for the European Union – A proposal for a Regulation from the European Commission - The Government Response. https://consult.justice.gov.uk/digital-communications/common-european-sales-law/results/cesl-government-response.pdf. Accessed 30 Dec 2016

Van derWeide J, DeTavernier P (2012) Common European Sales Law and EU-Competence: A Never Ending Game? http://leidenlawblog.nl/articles/common-european-sales-law-and-eu-competence-a-never-ending-game. Accessed 30 Dec 2016

Wendehorst C (2016) Sale of goods and supply of digital content – two worlds apart? In Depth Analysis. European Parliament - Policy Department for Citizen's Rights and Constitutional Affairs PE 556.928

Whittaker S (2008) The draft common frame of reference – An assessment. Ministry of Justice, London, United Kingdom

Chapter 7
European Union Information Law and the Sharing Economy

Catherine Easton

Abstract The sharing or collaborative economy, including prominent platform-based businesses such as Uber and Airbnb, harnesses online technology to match service providers and users. The EU has identified this sector as providing wide-ranging opportunities for growth, while acknowledging its potential to disrupt existing regulatory frameworks and, in this way, create risks for service providers and users alike. This chapter focuses specifically on the information law-related aspects of the sharing economy. In a move to support certainty in the area and to clarify its own position, the EU has recently published its agenda on the collaborative economy. This policy document is analysed in the light of its implications for EU information technology law and policy. Areas such as intermediary liability, data protection, ratings systems and the use of algorithms are analysed to draw conclusions on the effectiveness of the EU's regulatory approach and to make predictions for the future development of law and policy.

1 Introduction

This chapter examines key issues of European Union (EU) Internet law in relation to the growth of the so-called sharing economy. It analyses the position of platforms such as Airbnb and Uber in legal areas such as data protection, intermediary liability and the use of algorithms. The position of the EU as a regulator in this specific online sphere will be evaluated, in particular its stance as outlined in the recently published "European agenda for the collaborative economy",[1] with predictions made in relation to future reforms and the evolving nature of this sector.

[1]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European agenda for the collaborative economy COM(2016) 356 final {SWD(2016) 184 final} (EU Agenda on the Collaborative Economy).

C. Easton (✉)
Lancaster University, Bailrigg, Lancaster LA1 4YW, UK
e-mail: c.easton@lancaster.ac.uk

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_7

The rise of the sharing economy is a global phenomenon and one that the EU, as a global economic entity, has recognised that it needs to address with strategically implemented law and policy. Services are commodities that can be traded across a wide range of markets based on peer-to-peer access. While the potentially revolutionary nature of this shift has yet to be determined, these new business methods based on collaboration have had a widespread economic, cultural and societal impact. Botsman and Rogers (2010)[2] highlight the transformative, beneficial aspects of what they see as the future of commodity exchange. Others point towards the ability of this economic interaction to discover new connections and drive down prices.[3] What these new business methods have in common is the use of technology to establish, develop and aggregate links between parties and, potentially, lead to a more sustainable use of resources.[4] However, these shifts have been criticised for by-passing regulations, minimising employment protection and creating ever-evolving risks for providers and users alike.[5]

Given the breadth of potential disruption and the diversity of the services and commodities that can be shared, EU and local Member State regulators have been forced to make a growing number of regulatory responses on a piecemeal basis. However, there was a need for more strategic measures to develop a cohesive approach to regulation. In September 2015 the European Commission initiated a consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy.[6] The results were drawn upon to produce the European Commission's Agenda for the Collaborative Economy,[7] which aims both to support this growing market and to provide clarity for businesses, end users and policy makers alike. This chapter analyses these initiatives to evaluate the sharing economy from the perspective of the challenges these new forms of doing business create for EU Internet Law. Relevant law and policy will be tackled on a thematic basis, covering issues relating to intermediary liability, data protection, ratings systems, verification of users, and the use of algorithms.

[2]Botsman and Rogers (2010), p. 11.

[3]Allen and Berg (2014), pp. 13–16.

[4]Daunoriene and others (2015), p. 837.

[5]Goudin (2015), p. 16.

[6]https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud Accessed 20 July 2016.

[7]COM(2016) 356 final.

2 Defining the Online Sharing Economy

The decentralised nature of the Internet has, since its introduction, allowed for unprecedented real time, cross border interaction between end users. While these tech-enabled peers have long been able to create content and communicate, it is in the last few years that commercial enterprises have been able to take these interactions to a higher level to disrupt existing markets. Added to this, the growth of smartphone and portable mobile device ownership has allowed for easier access to online services.

Kennedy (2016)[8] highlights that the sharing economy is closer to that of commodity exchange markets than true sharing. A socio-technical practice is not solely based on reciprocal actions but usually holds an expectation of some form of compensation. The European Parliament's 2015 report into the sharing economy[9] highlights the lack of consensus on the terminology used. It itself opts to use "sharing economy" defined as:

> The use of digital platforms or portals to reduce the scale for viable hiring transactions or viable participation in consumer hiring markets (i.e. 'sharing' in the sense of hiring an asset) and thereby reduce the extent to which assets are under-utilised.[10]

Whereas, the European Commission refers to the "collaborative economy" and holds as its definition: "*a complex ecosystem of on-demand services and temporary use of assets based on exchanges via online platforms*",[11] the European Agenda[12] expands upon this and defines this sector as:

> business models where activities are facilitated by collaborative platforms that create an open marketplace for the temporary usage of goods or services often provided by private individuals

In the website accompanying her academic work, Botsman (2015) provides a dictionary of commonly used terms relating to the sharing economy.[13] This defines the collaborative economy as one that bypasses traditional intermediaries; it continues to outline terms such as "gig economy", where jobs are broken down into smaller tasks or "gigs" that are performed for a specific time, and the "on demand economy" which matches providers to users at the exact time a need arises. Tellingly, reciprocal sharing is only a factor in a small number of sites and a key characteristic of the sector in question is that it is delivered over platforms; it could, therefore, be better defined as a "platform economy". Banning (2016) argues that

[8] Kennedy (2016), pp. 461–474.

[9] Goudin (2015), p. 10.

[10] Ibid, p. 11.

[11] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Upgrading the Single Market: more opportunities for people and business. COM (2015) 550 final.

[12] COM (2016) 356 final, p. 3.

[13] Botsman (2015).

defining this sector as based upon "sharing" could mask strong commercial interests, highlighting her concern:

> that the web and Internet more generally celebrate a culture of sharing while exploiting what can be seen as the best impulses of humanity, the affective and altruistic *esprit de corps* based on common human experience, to fuel the growth of digital neoliberal capitalism.[14]

However, with the acceptance that there are numerous facets to its operation, this chapter uses "sharing economy" as a blanket term to refer to the use of online technology to facilitate peer-to-peer access to goods and services, usually for monetary consideration.

Attention has been drawn to certain key players in the field, owing both to their own publicity and to instances in which their use has clashed with more traditional forms of local regulation. Uber, a car-sharing firm was founded in 2009 and, put simply, provides an app to allow users to a car journey and drivers using their own vehicles respond to this. At the end of 2015, it was valued at US $62.5 million[15] and operated in over 400 cities.[16] Airbnb, an accommodation-sharing website, was founded in 2008 and uses its website and related apps to connect hosts with end users in search of space to rent. Others have used similar methods across a wide variety of services such as: home and office task provision,[17] garden and home tool sharing[18] and pet sitting.[19]

What these companies have in common is that they are facilitators not producers. Uber is a car-focused company that does not own cars and Airbnb does not rent its own rooms to tourists. This position has allowed for the circumvention of traditional, localised forms of regulation and has led to conflict with sector-specific regulators. Uber has been sued for providing illegal services in France[20] and, after a number of court cases, has been banned in Spain.[21] Airbnb has come into conflict with numerous property regulations across the globe and, for example in June 2016, San Francisco's Board of Supervisors voted to impose $1000 fines on Airbnb for every listing in the area that had not registered according to local regulations.[22] While the impact of these new ways of doing business raises complex, often localised, legal issues, the EU has taken strategic steps to examine, at a wider level, the interaction between the law and the role that technology plays to sustain these business models.

---

[14]Banning (2016), pp. 489–503.

[15]Isaac and Picker (2015).

[16]https://www.uber.com/cities/ Accessed 8 Sept 2016.

[17]https://www.airtasker.com/ Accessed 8 Sept 2016.

[18]https://www.openshed.com.au/ Accessed 8 Sept 2016.

[19]https://dogvacay.com/ Accessed 8 Sept 2016.

[20]Labbe (2016).

[21]Uber (2016).

[22]Benner (2016).

2.1 European Union Policy and the Use of Technology to "Share"

A 2013 report for the European Commission[23] linked the emergence of the sharing economy to both a lack of trust in large companies because of the 2008 economic crisis, and the prevalence of and ease of access to technology. It goes on to indicate that an essential factor in the success of these models is public trust in the technology supporting the interactions and transactions themselves. If its position is that these new ways of doing business are beneficial to economic growth, then the EU needs a strategy to develop the online environment in a way that develops and sustains consumer trust.

At a wide level, initiatives taken by the EU relating to the sharing economy link squarely back to the creation of a strong, sustainable Single Market and, when targeting the sharing economy, the overarching Single Market Strategy[24] and the Digital Single Market Strategy[25] include reciprocal references, highlighting complementary interaction. The latter Strategy, developed by Andrus Ansip, Vice-President on the Digital Single Market, seeks to address the challenges and opportunities of an increasingly online marketplace within the remit of free movement principles. It accepts that a number of fragmentation threats and barriers to trade exist uniquely in the online environment and seeks to place the EU at the forefront of the global digital economy. While accepting that the subsequent Single Market Strategy will provide details, it states:

> The rise of the sharing economy also offers opportunities for increased efficiency, growth and jobs, through improved consumer choice, but also potentially raises new regulatory questions.[26]

The Digital Single Market Strategy[27] itself outlines the prediction that the sharing economy has the potential to increase global revenues to 300 million euros by 2025. Research is referenced to indicate that a third of respondents to a survey covering 15 EU countries stated that their participation in the sharing economy is likely to rise in the next twelve months.[28] While using the term "collaborative", it includes a section on enabling the balanced development of the sharing economy. It highlights a perceived lack of regulatory certainty in the areas of "consumer protection, taxation, licensing, health and safety norms, social security and employment protection". It complements the on-going work on the digital

[23]Dervojeda and others (2013), p. 2.

[24]European Commission (2015).

[25]Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM (2015) 192 final.

[26]COM(2015) 550 final, par. 3.3.1.

[27]COM (2015) 192 final.

[28]IPSOS (2015).

environment with an aim to produce guidelines on the interaction between EU and national law. The goal is that they will go further to work towards the production of guidelines for international best practice, identify regulatory gaps and develop strategies for on-going monitoring of this fast-moving sector.

As business models develop, so too does empirical research into consumer attitudes to and use of sharing economy services. Positive factors pushing users towards the services include value, local and global sustainability, enjoyment of the use of technology, and the creation of a community. Barriers to their use include a lack of trust in both the technology itself and other people, concerns that the product or service will be substandard, and the perceived or actual difficulties of using the technology itself. Tussyadiah and Pesonen's (2016)[29] research on US and Finnish users of accommodation sharing websites found that the two nationalities reported both economic and social reasons for using the services. Social factors included the forging of relationships, supporting community cohesion and enhancing sustainability. They concluded that this focus on the socially responsible nature of the economic model could extend its attraction beyond those merely wanting to save money. It is likely that this will be a factor that is exploited by sharing economy platforms. If so, then an outward semblance of adherence to ethical practices will be crucial. Furthermore, supporting the all-important end user trust will be achieved by the platforms and the EU creating an appropriate regulatory environment that develops consumer confidence while also allowing platform-based businesses to innovate and grow.

2.2 *The Nature of an Information Society Service*

The Internet enables the collaboration of service provider and end user. A crucial aspect of a sharing economy platform's interaction with EU law is how it is defined in relation to the services provided. If, as could happen in rare cases, the platform provider is also the supplier of the resources relating to the underlying service, for example, cars then it may not be classified purely as an information service and enjoy the legal framework relevant to such services. Article 4 of the E-Commerce Directive[30] tasks Member States with ensuring that information services should "*not be made subject to prior authorisation or any other requirement having equivalent effect*". The classification of a sharing economy platform is, therefore, critical to the imposition of potential entry standards into a relevant marketplace with its associated sector-specific regulations. The Directive's definition of an information society service[31] is a service "*normally provided for remuneration, at*

[29]Tussyadiah and Pesonen (2016), p. 14.

[30]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive), OJ L 178/1.

[31]E-Commerce Directive, Recital 17.

a distance, by electronic means. . .and at the individual request of a recipient of services". To fulfil this crucial distinction there is, therefore, a need to distinguish the information service aspect of a sharing economy platform with that of the underlying service itself.

The EU Agenda on the Collaborative Economy[32] accepts that a determination of the status of a platform has to be carried out on an individual basis and gives a list of three factors to be considered. Firstly, whether the platform sets the price of the service is considered or not. An approach in which the underlying service provider has a choice in adopting the price recommended by the platform would lead toward a finding that the platform is not providing the underlying service. Secondly, any contractual terms set by the platform will be examined to determine the extent of any mandatory, fixed instructions relating to the relationship between the service provider and the end user. Finally, the assets used in providing the service are examined and, if these are owned by the platform, then it is less likely to be deemed a mere information service. All of these factors need to be considered in determining the status of the platform itself on a case-by-case basis.

3 Intermediary Liability

In keeping with the focus of this chapter on the information aspects of the sharing economy, this section will cover intermediary liability from the perspective of a business' ability to manage the information shared on its network. In relation to the sharing economy, an examination of intermediary liability can extend to wide-ranging aspects of consumer protection, employment law and local sector-specific regulation. However, the following discussion will cover specifically the relationship between the platform and those using it to share information in, for example, reviews and profiles. What will be discussed is the position of online service providers in relation to the information transmitted across their service. This type of liability of intermediaries is addressed and limited by the EU's E-Commerce Directive, and this has been fundamental to the Internet's growth into a global, interactive marketplace.

At a basic level, an information society service is not liable for information transmitted when it acts as a "mere conduit"[33] or a host that does not initiate or modify the communication or select who receives the transaction.[34] Information services are also protected from a general obligation to monitor the information they transmit or store.[35] These principles were created in the early years of the Internet's development when services were usually small to medium enterprises

[32]COM (2016) 356 final {SWD(2016) 184 final}p. 6.

[33]E-Commerce Directive, Article 12.

[34]Ibid, Article 14.

[35]Ibid, Article 15.

that could not do business without a level of protection.[36] Nowadays online businesses such as Google, Amazon and Facebook are among commercial entities with the highest global turnover and undertake an increasingly wide range of activities. Because of this, the EU has initiated a consultation on Online Platforms,[37] which elicited responses on, among other issues, the current and future nature of the intermediary liability regime.

Sharing economy platforms have come into prominence at this time when the nature of the liability regime is evolving. A sharing economy platform when it hosts its users' profiles and reviews acts as a host and generally will not be liable for any potentially illegal content that appears in this information. This is subject to the platform not having actual knowledge of the illegal activity and, when such knowledge is gained, taking expeditious action to remove the information. With the Internet developing as a marketplace, these general limitations have been further defined by case law. The Court of Justice of the European Union case *L'Oreal v eBay*[38] focused on a trademark dispute because of users employing the auction site to sell unauthorised products. While the Article 14 hosting limitations applied in the first instance, further questions arose relating to eBay's selling of links to these products and the use of purchased search engine placements to drive potential buyers to the products. The Court saw these extra steps taken by eBay as affecting their intermediary position and held that the limitations could be waived if the information service:

> was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful[39]

This concept of the "diligent operator" sees the court accepting that there are circumstances in which the E-Commerce Directive's wide-ranging limitations may not apply. This has led to a reliance upon self-regulatory measures to demonstrate diligence. The Communication on Online Platforms[40] highlights that a number of online platforms have raised concerns that the move towards self-regulatory regimes would lead to the loss of their limited liability status. Clear guidance is called for to provide platforms with more certainty in relation to how any self-regulatory measures they take interact with the intermediary liability limitations.

After its consultations, the European Commission has decided not to change the intermediary liability regime but to undertake a programme based upon

[36]Guadamuz (2014), pp. 312–366.

[37]Supra, n6.

[38]CJEU, *L'Oréal SA and Others v eBay International AG and Others*, C-324/09, Judgment of 12 July 2011.

[39]*L'Oréal SA and Others v eBay International AG and Others*, par. 124.

[40]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM (2016) 288 final (Communication on Online Platforms).

"*a sectorial, problem-driven approach to regulation*".[41] What is fundamental is a need for a more coordinated oversight of self-regulatory mechanisms and the European Commission sets forth an aim to determine whether guidance on voluntary measures should be developed.

The maintenance of the online intermediary liability status quo is welcome news for sharing economy platforms as it leaves them to develop as they have been, relying upon limited liability as long as they demonstrate a reasonable level of diligence. However, they should expect the EU to initiate a review of sharing economy-specific rules and guidance on how best to manage self-regulatory oversight of the legality or otherwise of the information shared by their users.

4 Data Protection

The EU has recently undertaken a wide-ranging reform of its data protection laws, culminating in the adoption in April 2016 of the General Data Protection Regulation (GDPR).[42] One of the main reasons put forward for this modernisation was the need to update the framework to address the challenges of new technology. With sharing economy platforms reliant on the collection and sharing of data, and the maintenance of service provider and user profiles, there are a number of the reforms that could have a fundamental impact on the sector. Data and meta-data shared by users with the platforms can reveal a wide-range of personal information. This can be contained in personal profiles but also is gathered in relation to location, shopping preferences, health and availability. This collection of data can affect service users and providers alike. The information collected could be put to use within the platform to manipulate the behaviour of users and, outside of the platform, it could comprise a commercially-lucrative asset. Furthermore, platforms may be put in the position of needing to share personal data with outside agencies if stricter rules are provided for verifying the identity of service providers and users.

The GDPR's updated basic definition emphatically demonstrates that sharing economy platforms process many types of personal data:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[43];

[41] COM (2016) 288 final, p. 9.

[42] Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1.

[43] Ibid, Article 4(1).

Sharing economy platform providers are data controllers when they determine "*the purposes and means of the processing of personal data*"[44] when they collect information online to match a service user to a provider of, transport, accommodation or other service. This leads to a position in which they have to fulfil a wide range of duties placed upon them. The reforms also create new responsibilities for data processors, defined as the "*natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".[45] In particular, through the Article 32 responsibilities relating to the security of processing, both controller and processor are charged with implementing appropriate measures to ensure a risk-appropriate level of security. For sharing economy platforms this leads to a situation in which complex agreements need to be developed with any data storage or cloud technology providers they may use to provide their service. The key will be in defining clear roles and responsibilities, with transparency for end users a crucial factor in gaining and sustaining end user trust.

The GDPR heralds a stronger focus on the rights of data subjects. Importantly, the notion of consent has been strengthened to require the need for "*a clear affirmative act*"[46] that goes beyond "*silence, pre-ticked boxes or inactivity*". Furthermore, the consent needs to cover all potential processing activity for a stated purpose; if there are a number of purposes then this explicit consent needs to be given for all of these. This means that a platform provider is under a requirement to gain further consent if it wishes to use data gathered for the initial use of a service for other purposes not stated in gaining the initial consent. Further detail is provided on whether a processing activity is new; where the Article 23 security and public interest restrictions do not apply a list of factors to be considered are given.[47] These are: any potential link between the initial collection purpose and the new purpose, the context in which the data collection occurred, the nature of the personal data itself, the consequences of the further processing, and whether safeguards are provided or not. In practice, this means that a platform focuses on facilitating travel services could not then either sell on data to another business or expand its own business into areas such as insurance provision, leisure marketing or health, for example, based on the initial data collected for travel. This will lead to strategic drafting of consent clauses in wide terms or a greater number of consent points throughout the platform's relationship with the end user and service provider. This, however, could potentially contribute to consent fatigue, what the UK Information Commission's Office terms the "disturbing irritation"[48] of repeated consent requests.

[44]Ibid, Article 4(7).

[45]Ibid, Article 4(8).

[46]Ibid, Recital 32.

[47]Ibid, Article 6(1)(a).

[48]Bourne (2015), p. 1.

The regulation increases the fines available for infringements with two levels of penalties reaching up to €20,000,000 or, in relation to undertakings, 4% of global turnover if this is higher. New timescales for notification of data breaches have been provided with controllers now needing to inform the relevant supervisory body of a breach within 72 hours of discovery.[49] Processors need to inform controllers of breaches "without undue delay" once aware of a breach.[50] The new law contains a number of measures intended to address the realities of technology development. These include the need, in certain circumstances, to carry out a data protection impact assessment,[51] paying attention to wider organisational and developmental measures to minimise risk. Similarly, the regulation enshrines the concept of data protection by default that, in essence, requires data controllers to take appropriate steps to embed strategies to support data protection principles throughout the creation and use of a technology. Further detail is given in relation to what these steps could entail:

> minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.[52]

These wider regulatory measures aim to help technology creators fulfil the legal responsibilities placed on them by the GDPR as a whole. Sharing economy platform creators seeking to sustain economic development will need to engage with these practices, not only to comply with the law but also to develop the on-going trust of increasingly empowered end users.

The reforms enshrine a number of concepts that aim to strengthen end user rights with an emphasis on supporting control and facilitating transparency. A right to data portability has been introduced[53] in which a data subject has a right to access his or her own data processed lawfully[54] by automatic means; linked to this, a request can be made that the data is transferred to another data controller.[55] Interoperability is key to effective transfers and data controllers are encouraged to support the storage of data in formats that support easier transfers.[56] The provision[57] recognises that the right to data portability depends upon the technical feasibility of any measures but, at a minimum level, personal data needs to be stored in a "commonly used and machine-readable format".[58] In relation to the sharing

[49]Regulation 2016/679/EU, Article.33(1).
[50]Ibid, Article 33(2).
[51]Ibid, Article 35.
[52]Ibid, Recital 78.
[53]Ibid, Article 20.
[54]Ibid, Article 6(1).
[55]Ibid, Article 20(2).
[56]Ibid, Recital 68.
[57]Ibid, Article 20.
[58]Ibid, Article 20(1).

economy, a very good or excellent reputation on a platform is a commercially lucrative asset and service providers and users invest heavily in their maintenance. Because of this, data portability has been highlighted as being crucial to preventing consumer "lock-ins" and essential in supporting competitive practices.[59] However, platform providers need to see this as a priority in gaining sector-wide provider and user confidence and, in particular, collaborate to achieve the required level of interoperability.

Further strength is given to end users with the right to request that reasonable steps are taken to rectify inaccurate data and complete incomplete data.[60] The right of erasure[61] heralds a new level of end user control over the retention and storage of personal data. Subject to certain conditions, the data processor on receiving a request needs to erase personal data with no undue delay. If the data has been made public then the original data controller needs to take feasible, reasonable measures to inform subsequent processors of the need to comply with the request and avoid any links to or copying the data. The manner in which this new right is implemented could have a significant impact on the development of more sophisticated ratings systems. The need to support transparency in the reciprocal ratings system, as discussed below, has been identified as a policy concern after the European Commission's consultation on online platforms.[62] However, transparency and veracity in relation to customer and service provider reviews will need to be balanced with a data subject's ability to request the erasure of data. Wide-scale removal of ratings-linked data could have a significant effect on the economic and social value of platforms' reliance on reputational reviews.

5 Reputational Systems

A typical sharing platform aims to facilitate a transaction between an end user and a service provider. Technology's ability to aggregate and simplify feedback has led to reputational systems taking an increasingly influential role in consumer decision-making.[63] A key characteristic of the sharing economy is the way in which this technology is employed to enable the potential quality of the service providers and the users themselves to be assessed.

In relation to the quality of the service, reputational systems are crucial to developing and sustaining trust between users and providers and towards the platform itself. Allen and Berg deem them a pivotal factor in the bottom-up governance approach that draws upon market forces to "*develop and implement*

[59]Bureau Europeen des Unions de Consommateurs (2016).

[60]Regulation 2016/679/EU, Article 16.

[61]Ibid, Article 17.

[62]COM (2016) 356 final, p. 10.

[63]Li and Hitt (2008), pp. 456–474.

bottom-up governance, utilising and making information available that only the consumers can provide".[64] However, the use of technology in this way does not always achieve neutral results; indeed, an asymmetry in the information can lead to warped perceptions of services and even platforms themselves. Early work on online ratings systems[65] found that users were reluctant to give negative feedback unless in exceptional circumstances, that ratings were used both to retaliate negatively and to enhance reputations; and that those with bad ratings were able to change identities to erase negative profiles. Additionally, in these collaborative marketplaces, end users as guests, passengers, service users also receive ratings from those providing the services. This can lead to discrimination arising; for example, research has found that African Americans have a lower acceptance rate to Airbnb listings[66] and Uber drivers can be rejected simply on the way they look.[67] There is potential for the platforms themselves to address these issues by identifying those who give negative ratings for a particular group and manipulating their search results to penalise those making persistent discriminatory choices. This, however, would need strategic, potentially commercially damaging, action being taken by the platforms to address the negative aspects of their users' decisions.

In many platforms, service providers are able to reject a user without providing a reason, with Airbnb hosts rejecting potential guests in 49% of cases.[68] In this way, a semi-complicit situation may develop in which users and service providers are reluctant to provide negative reviews out of fear of receiving a low reciprocal rating. To address this, platforms such as Airbnb elicit hidden feedback from each party before it is revealed. Nosko and Tadelis's (2015)[69] work highlights "reputational externalities" in which one negative experience can lead a user to make negative assumptions about all service providers on a platform. Furthermore, they identify the potential for inbuilt positive biases to occur if a user leaves a platform after a substandard experience and does not leave a review. Added to this is the phenomenon of incentivised reviewing which is growing on retail platforms such as Amazon.[70] This sees users given products or discounts in exchange for giving a review. The deal is openly stated in the review itself and the reviewers have full autonomy over their comments but early research shows that incentivised reviews were four times less likely to be critical.[71] These practices may potentially be taken up by sharing economy platforms and, if so, could have a negative effect on consumer trust.

[64]Allen and Berg (2014), p. 29.
[65]Resnick and others (2000), pp. 45–48.
[66]Edelman and others (2016), p. 17.
[67]Harman (2014).
[68]Fradkin (2015), p. 4.
[69]Nosko and Tadelis (2015), pp. 1–14.
[70]Gibb (2016).
[71]Reviewmeta (2016).

Despite these potential asymmetries, the EU Agenda on the Collaborative Economy gives similar weight to rating and reputational systems as they do to existing consumer protection mechanisms and holds that they:

> can contribute to higher quality services and potentially reduce the need for certain elements of regulation, provided adequate trust can be placed in the quality of the reviews and ratings.[72]

This indicates an approach that places technology-mediated interaction in a position where it, to a certain level, replaces the need for strong, centralised regulation. However, a January 2016 European Parliament-commissioned report,[73] while predicting the wide reach sharing economy platforms will have on economic and social life, warns of the potential dangers of exclusion. Users with lower ratings could find themselves removed from the site and barred from re-entry to try to rebuild a reputation. The report also raises concerns about the potentially socially disruptive practice of frivolous or malicious reviews. In contrast with some of the market-driven approaches, regulation is recommended with potential legal options including full regulation of ratings systems, a qualified right to reset a rating and the provision of "gateway" or "rehabilitation" communities in which reputations can be rebuilt to an appropriate level to re-enter the original platform. Such legal responses would need to be drafted with full co-operation from the sites themselves and be neutral enough to encompass the wide range of available systems. Currently, intrusive regulation could have negative effects on this developing market. However, with increasingly sophisticated systems and the growing potential for inequalities to develop, light-touch regulation may be needed to develop and sustain consumer confidence.

6 Verification

To place service providers with users, technology is used to verify the identity of both parties. Some sharing economy platforms have promoted these technology-driven checks as being more dependable than those existing "off-line", as Airbnb founder Brian Chesky stated in 2013:

> Well it turns out that cities can't screen as well as technologies can screen. Companies have these magical things called reputation systems.[74]

However, initial reliance solely on technology-facilitated self-regulated ratings systems has now given way to more platforms employing centralised scrutiny, with Airbnb subsequently introducing identification verification requirements. Similarly, Uber carries out background checks on its drivers but, in an April 2016

[72] COM(2016) 356 final, p. 4.
[73] Goudin (2015), pp. 29–30.
[74] PandoMonthly (2013).

settlement to a case brought in California, have been ordered not to advertise these as "the gold standard" or to state that their cars are "the safest ride on the road".[75] In this case, California District Attorneys presented evidence that Uber's systems had failed to detect the criminal convictions of 25 of its drivers.

While these extra checks are carried out by some platforms, as outlined above, a large amount of weight is given to the ability of ratings systems to develop trust between the parties. In the report on the EU consultation on platforms and the collaborative economy[76] concerns were raised that sharing platforms' rating systems could give the impression that they have carried out checks on, for example, the safety of accommodation when this is not part of the service they provide.[77] The nature of the platforms' responsibilities to carry out technology-facilitated verifying checks on their services needs to be made clear to users, perhaps alongside the development of best practice standards on an industry-specific basis. A fine balance needs to be drawn as, as highlighted by the EU Agenda on the Collaborative Economy,[78] the more action a platform takes in verifying the specific quality of services, the more likely they are to be found to be providers of the actual service itself. This creates a tension for EU regulators who have indicated an aim to support sharing platforms, as they provide "an important contribution to jobs and growth,"[79] while recognising the need to regulate to protect end users.

7 Algorithms

Key to the success and growth of the online sharing economy has been the ability to harness ever-widening data sets to match service providers with users. The ability to store and analyse large data sets is constantly improving, leading to ever-expanding data sets upon which to base economic decisions.[80] Sharing economy platforms employ sophisticated algorithms to fulfil the roles that would have previously been occupied by managers taking decisions on pricing and the matching of providers and users. With these decisions now, in the main, undertaken by an algorithm, there is no need for direct contact between, for example, service providers as distributed car or property owners and a human manager. One high-profile example of this in action relates to the car-sharing platform Uber's use of surge-pricing in which an increased demand for services in one area leads to its algorithms increasing prices for others nearby.[81] This, however, does not consider

[75] Hern (2016).
[76] European Commission (2016) par. 5.2.6.3.
[77] Ibid.
[78] COM (2016) 356 final.
[79] Ibid, p. 2.
[80] Fradkin (2015), p. 31.
[81] UberEstimator (2016).

the reasons behind the surge, and the company was criticised when its prices rose to four times the normal rate after a siege in Sydney in 2014.[82] The company claims that this practice has been suspended during subsequent emergencies but this indicates the need for human input to override the negative impact of the blanket implementation of algorithmically determined decisions.

A key issue for regulators when faced with the predominance of algorithms is a lack of transparency that creates difficulties in determining whether decisions are being made on a fair basis. Indeed, Banning (2016)[83] provides a scathing critique of the opaque nature of the technology behind the public-facing interface of a "sharing" platform. At a wide level she sees end users, service users and providers alike, as being manipulated by algorithms that "*induce, cue and co-construct realities*"[84] to support commercial interests. This is reflected in Noulas and others' (2015)[85] work that highlights that the system for ride sharing rating could become more sophisticated and responsive to the realities of human interaction, and include data based on "*support for the disabled, driver politeness or cleanliness*". Similarly, Lee and others (2015)[86] research examines algorithmic management in the ride-sharing platforms Uber and Lyft. They found that, while the algorithm aimed to motivate human behaviours, it did not address the wider motivations of drivers in their reactions to, for example, surge pricing and the ratings systems. The data-driven systems were centred on economic considerations and did not consider the rates at which the drivers worked or the human interactions with passengers. Yet again, the opaque nature of the computer-based systems was highlighted with conclusion that:

> Transparency in how the surgepriced area was computed in real-time could improve workers' trust toward the algorithmic information.[87]

How such transparency is achieved is yet to be determined. The sheer quantities of data and the sophisticated machine learning tools involved in their analysis makes it increasingly more difficult for regulators, even when they have access to data, to determine the impact of its use. Martens (2016) highlights potential information asymmetries and the need for independent regulators with "autonomous technical expertise"[88] to delve beneath the technical complexities and opaque practices fuelled by the use of these increasingly sophisticated systems.

[82]BBC News (2014).

[83]Banning (2016), pp. 489–503.

[84]Ibid p. 499.

[85]Noulas and others (2015), p. 18.

[86]Lee and others (2015), pp. 1603–1612.

[87]Ibid p. 1610.

[88]Martens (2016), p. 45.

8 Conclusions

The EU Agenda on the Collaborative Economy[89] brings some clarity to the position of the EU as a regulator in the face of the boom in sharing economy platforms. It is apparent from the report, however, that this sector is deemed crucial to economic development and any regulatory measures need to achieve a balance between protection of users and supporting commercial growth. An example of this can be seen in the EU's position to maintain the current regime of intermediary liability, while aiming to create guidance on self-regulatory actions. New technology-focused laws in wide areas such as data protection will, however, affect the development of these business models. This is particularly apparent in relation to the newly-introduced rules on the right to data erasure and their potential impact on reputational ratings systems. The ratings systems themselves have been identified as constituting a healthy self-regulatory environment that minimise the need for top-down regulatory action. As Koopman and others (2014) state:

> Markets, competition, reputational systems, and ongoing innovation often solve problems better than regulation when we give them a chance to do so.[90]

However, increased reliance upon algorithms and ratings systems can lead to information asymmetries that are difficult to identify and address. Indeed, the technology-fuelled nature of these platforms is problematic for the EU to tackle as they:

> shape their innovations in a manner that creates ambiguity in terms of which higher-level institutions apply to them.[91]

This is reflected in the responses to the EU Consultation on the regulatory environment for platform as conclusions were drawn that:

> the regulatory system is not suited to new business models, and that it is difficult for public authorities to collect evidence in the fast-moving environment.[92]

Because of the penetration of these businesses and their highly technical nature, one suggestion has arisen for the creation of a new sector-specific regulator to work alongside existing authorities such as the EU Data Protection Supervisor.[93] This would need to have access to effective resources and skills to probe the technology-specific aspects of these developing businesses. This approach, however, is not one that the EU currently indicates it is considering. The decision taken not to change fundamentally the regulatory environment relating to platforms but to work with the industry to create sector-specific guidelines indicates a cautious response that leaves the way open for more intrusive measures if deemed necessary. In relation

[89]{SWD(2016) 184 final}.

[90]Koopman and others (2014), p. 19.

[91]Elert and Henrekson (2016), pp. 95–113.

[92]European Commission (2016), p. 26.

[93]Martens (2016), pp. 44–46.

to, for example, ratings systems and intermediary liability, there is the possibility for guided self-regulatory solutions to increase consumer confidence and protection. The extent to which these could be effective depends strongly upon the sector's willingness to co-operate and, in particular, provide transparent information about the wider effects of the technology employed.

References

Allen D, Berg C (2014) The sharing economy: how over-regulation could destroy an economic revolution. Melbourne: Institute of Public Affairs. https://ipa.org.au/portal/uploads/Sharing_Economy_December_2014.pdf. Accessed 17 Aug 2016

Banning M (2016) Shared entanglements – Web 2.0, infoliberalism and digital sharing. Inform Commun Soc 19(4):489–503

BBC News (2014) Uber 'truly sorry' for price rise during Sydney siege BBC.co.uk December. http://www.bbc.co.uk/news/technology-30595406. Accessed 9 Sept 2016

Benner K (2016) Airbnb in disputes with New York and San Francisco. NYTimes.com. http://www.nytimes.com/2016/06/29/technology/airbnb-sues-san-francisco-over-a-law-it-had-helped-pass.html. Accessed 9 Aug 2016

Botsman R, Rogers R (2010) What's mine is yours: the rise of collaborative consumption. Harper Collins, New York

Botsman R (2015) The sharing economy: dictionary of commonly used terms. Collaborativeconsumption.comhttp://www.collaborativeconsumption.com/2015/11/12/the-sharing-economy-dictionary-of-commonly-used-terms/. Accessed 12 Sept 2016

Bourne I (2015) Consent: some basic questions of policy and approach Information Commissioner's Office Meaningful Consent. http://www.meaningfulconsent.org/reports/mcde_report_bourne01.pdf?f=reports/. Accessed 8 Sept 2016

Bureau European des Unions de Consommateurs (2016) The Collaborative Economy BEUC Position April. http://www.beuc.eu/publications/beuc-x-2016-030_gbe_collaborative_economy_beuc_position.pdf. Accessed 22 Aug 2016

Daunoriene A, Drakš A, Snieškac V, Valodkien G (2015) Evaluating Sustainability of Sharing Economy Business Models 20th International Scientific Conference Economics and Management (ICEM-2015)

Dervojeda K, Verzijl D, Nagtegaal F, Lengton M, Rouwmaat E, Netherlands PWC, Monfardini E, Frideres L, Luxembourg PWC (2013) The Sharing Economy Accessibility Based Business Models for Peer-to-Peer Markets Business Innovation Observatory

Edelman B, Luca M, Svirsky D (2016) Racial discrimination in the sharing economy: evidence from a field experiment. Am Econ J Appl Econ. http://www.benedelman.org/publications/airbnb-guest-discrimination-2016-09-16.pdf. Accessed 25 Sept 2016

Elert N, Henrekson M (2016) Evasive entrepreneurship. IFN Working Paper No. 1044. Available at SSRN: https://ssrn.com/abstract=2513475

European Commission (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Upgrading the Single Market: more opportunities for people and business {SWD(2015) 202 final} {SWD(2015) 203 final}

European Commission (2016) Synopsis Report on the Public Consultation on the Regulatory Environment for Platforms. Online Intermediaries and the Collaborative Economy. https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-environment-platforms-online-intermediaries. Accessed 8 Sept 2016

Fradkin A (2015) Search frictions and the design of online marketplaces. http://andreyfradkin.com/assets/SearchFrictions.pdf. Accessed 13 Sept 2016

Gibb S (2016) Incentivised reviews are warping Amazon's product star ratings, report says. The Guardian 20th September. https://www.theguardian.com/technology/2016/sep/20/incentivised-reviews-amazon-product-star-ratings. Accessed 11 Sept 2016

Goudin P (2015) The Cost of Non-Europe in the Sharing Economy European Parliament. January 2016

Guadamuz A (2014) Development in internet liability. In: Savin A, Trzaskowski J (eds) Research handbook on EU Internet law. Edward Elgar, Cheltenham, pp 312–366

Harman G (2014) The sharing economy is not as open as you might think. The Guardian.com 12 November, https://www.theguardian.com/sustainable-business/2014/nov/12/algorithms-race-discrimination-uber-lyft-airbnb-peer. Accessed 14 Sept 2016

Hern A (2016) Uber's 'safe ride fee' becomes 'booking fee' after $25m settlement over rider safety. The Guardian.com. https://www.theguardian.com/technology/2016/apr/07/uber-driver-background-check-lawsuit-passenger-safety-california. Accessed 22 Aug 2016

IPSOS (2015) ING International Survey: What's mine is yours - for a price. Rapid growth tipped for the sharing economy June. http://www.ezonomics.com/ing_international_survey/sharing_economy_2015. Accessed 15 Aug 2016

Isaac M, Picker L (2015) Uber Valuation Put at $62.5 Billion After a New Investment Round. NYTimes.com December, http://www.nytimes.com/2015/12/04/business/dealbook/uber-nears-investment-at-a-62-5-billion-valuation.html?_r=1. Accessed 08 Sept 2016

Kennedy J (2016) Conceptual boundaries of sharing. Inform Commun Soc 19(4):461–474

Koopman C, Mitchell M, Thierer A (2014) The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change. Mercatus Research. http://mercatus.org/sites/default/files/Koopman-Sharing-Economy.pdf. Accessed 9 Sept 2016

Labbe C (2016) French court fines Uber, execs for illegal taxi service.Reuters.com Thursday June 9th, http://www.reuters.com/article/us-france-ubertech-court-idUSKCN0YV1DQ. Accessed 11 Sept 2016

Lee M, Kusbit D, Metsky E, Dabbish L (2015) Working with machines: the impact of algorithmic and data-driven management on human workers. In: CHI '15 proceedings of the 33rd annual ACM conference on human factors in computing systems, pp 1603–1612

Li X, Hitt LM (2008) Self-selection and information role of online product reviews. Inform Syst Res 19(4):456–474

Martens B (2016) An economic policy perspective on online platforms. JRC Technical Reports European Commission. https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/economic-policy-perspective-online-platforms. Accessed 8 Sept 2016

Nosko C, Tadelis S (2015) The limits of reputation in platform markets: an empirical analysis and field experiment. NBER Working Paper Series, 20830. doi:10.3386/w20830 http://faculty.haas.berkeley.edu/stadelis/EPP.pdf. Accessed 8 Sept 2016

Noulas A, Salnikov V, Lambiotte R, Mascolo C (2015) Mining open datasets for transparency in taxi transport in metropolitan environments. EPJ Data Sci 4:23

Pando Monthly (2013) Brian Chesky defends the legality and safety of Airbnb Youtube. https://www.youtube.com/watch?v=cNsFe7cRShc&list=UUgHogDu1ewdkkWZjfKIuKXQ&index=4. Accessed 12 Sept 2016

Resnick P, Kuwabara K, Zeckhauser R, Friedman E (2000) Reputation systems. Commun ACM 43(12):45–48

Reviewmeta (2016) Analysis of 7 million Amazon reviews: customers who receive free or discounted item much more likely to write positive review. ReviewMeta.com http://reviewmeta.com/blog/analysis-of-7-million-amazon-reviews-customers-who-receive-free-or-discounted-item-much-more-likely-to-write-positive-review/. Accessed 11 Sept 2016

Tussyadiah IP, Pesonen J (2016) Drivers and barriers of peer-to-peer accommodation stay – an exploratory study with American and Finnish travellers. Curr Issues Tour. doi:10.1080/13683500.2016.1141180

Uber (2016) Why Barcelona has no Uber. February 22nd https://newsroom.uber.com/spain/mwc16-en/. Accessed 9 Sept 2016

Uber Estimator (2016) Surge Pricing. http://uberestimator.com/uber-surge-pricing. Accessed 9 Sept 2016

Chapter 8
Product Liability and Digital Products

Geraint Howells, Christian Twigg-Flesner, and Chris Willett

Abstract This paper examines the topical question as to whether non-tangible products such as apps and other software not supplied on a tangible medium (should) qualify as products under EU Product Liability Directive. It addresses the relevant questions posed by the European Commission, which has recently announced an evaluation of the said Directive with the aim of its adaptation to the digital age. The article draws a crucial distinction between information (whether in tangible or non-tangible form) that should not lead to liability and tangible or non-tangible products which are not confined to mere information provision and whose defects may cause material harm. The latter must be considered as falling within the Product Liability Directive, which is eligible to reasonable interpretation achieving this aim.

1 Introduction

We are in the age of digital products[1] and information.[2] Instead of looking at physical maps, we use Google maps (other brands are available). Instead of buying records, CDs or books, we download versions or recover them from a cloud. We buy or use programmes that do everything for us from running a bath, controlling

[1] Murray (2016).

[2] Castells (2010).

G. Howells (✉)
City University of Hong Kong Law School, Tat Chee Avenue, Kowloon, Hong Kong
e-mail: ghowells@cityu.edu.hk

C. Twigg-Flesner
School of Law, University of Warwick, Coventry CV4 7AZ, UK
e-mail: c.twigg-flesner@hull.ac.uk

C. Willett
School of Law, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, UK
e-mail: cwillett@essex.ac.uk

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_8

the heat in the house to operating our car. In the future, even driving may be automatically controlled by computers. Computers are now able to interact and give each other instructions.[3] The key technology is now the intellectual property in software. The European Union ("EU") is focusing its consumer and private law initiatives around the digital agenda.[4] Just as this paper was being finalised the EU announced an evaluation of the EU Product Liability Directive[5] with the major driver being its adaptation to the digital age.[6] In particular, it asks:

- whether apps and non-embedded software or the Internet of things (IoT) based products are considered as "*products*" under the Directive;
- whether an unintended, autonomous behaviour of an advanced robot could be considered a "*defect*" according to the Directive;
- how the strict liability for damages between the different participants in the IoT is allocated, in particular in case of connected objects or sensors relying on each other that are not necessarily under the control of a single *producer*.

There has always been a process in product design, but the original product designer is insulated from strict product liability if not also a producer. Liability is channelled to the seller of the final product in sales law and the producer (in most cases) is liable under strict product liability. With digital products, the writing of the programme blurs the line between design and final product. The code produced can be delivered to a consumer who produces their own product with a 3D printer.[7] In commercial supplies, the final product can be in intangible form. The digital product can be either a product in its own right or incorporated into a final product without the need for an intermediate manufacturer. The question is whether such an intangible product can be a product imposing liability under the Product Liability Directive. This is at one level a technical question of interpretation. Under the present wording of the Directive, are intangible products covered? There are also the broader policy debates about whether they should be covered, which if answered positively, may lead on to discussion of whether the current wording can be adequately applied to intangible products.

[3]For example, computer can give instructions to another computer through a software that collects instruction from human users.

[4]Commission Staff Working Document A Digital Single Market Strategy for Europe—Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe, COM (2015) 192 final.

[5]Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products [1985] OJ L210/29.

[6]European Commission (2016) Evaluation of the Directive 85/374/EEC concerning liability for defective products. http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_grow_027_evaluation_defective_products_en.pdf. Accessed 24 Oct 2016.

[7]Howells and Willett (2016).

This paper starts by reviewing current law on whether intangible goods are to be treated as products. It will be noted that much of this is in relation to sales law where different considerations may apply. It will also be suggested that many of the distinctions drawn to justify treating digital products as goods have been rather artificial excuses to find liability. It will eventually be argued that the real distinction is not between physical and intangible products, but between information in physical or non-tangible form, and products whether tangible or non-tangible whose defects cause material harm.

2 Existing Law

2.1 Importance of Durable Medium

The early discussion on liability for digital products centered on whether intellectual property, mainly software, was covered by sale of goods legislation. One approach used by the courts was to distinguish between software supplied on a durable medium i.e. compact disc and computer programmes that were simply downloaded. The physical nature of the disc encouraged some commentators and judges to treat the former as products. Sir Iain Glidewell in *St Albans District Council v International Computers Ltd.*[8] drew a parallel between software supplied on a disc and an instruction book which would be part of the goods and therefore considered that a disc containing instructions should be treated as goods; although in the instant case the programme was actually loaded by an employee of the company rather than being supplied. This decision followed the Australian authority *Toby Constructions Products Pty Ltd v Computa Bar (Sales) Pty Ltd,*[9] which held that a computer system as a whole that includes both hardware, software, installation and software would be treated as "goods". In the United States, *Advent Systems Ltd. v Unisys Corporation*[10] had held software was "goods" within the Uniform Commercial Code's definition. The Court had assumed that such software was always contained in a physical medium; as it would have been at that time. Most recently, the Mercantile Court in London held that computer software qualified as "goods" under the Commercial Agents (Council Directive) Regulations 1993.[11] HHJ Waksman QC concluded, "there is no reason to require the product to be tangible or a "chattel" in the traditional sense, especially when installed so as to operate in a physical (i.e. hardware) environment.[12]

[8][1996] EWCA Civ 1296, 4 All ER 481.

[9][1983] 2 NSWLR 48.

[10]925 F.2d 670 (3rd Cir. 1991).

[11]SI 1993/3053.

[12]*Software Incubator Ltd v Computer Associates* [2016] EWHC 1587 QB 68.

The reliance on the software being in a physical medium has always seemed something of an excuse to invoke liability without addressing the core issue of whether software should on substantive policy grounds be treated as goods. In the common law systems you might have thought it would have been possible for the courts to be more flexible and willing to recognise *sui generis* contracts with obligations corresponding to those arising e.g., in the sale of goods?[13] However, the courts seemed to need to find it fell within the sale of goods code. They were probably hesitant to address the daunting task of defining a set of implied terms for software. Therefore whilst the approach of finding a rationale based on a durable medium is understandable given the tools the courts were working with, it has become an even more untenable distinction as technology has developed. If you have the option of downloading from a CD or from a cloud, it seems irrational to apply different regimes depending upon your choice. Now that software is usually simply downloaded, the relevance of this distinction has faded. However, it was crucial in denying sale of goods protection in the Australian case of *Gammasonics Institute for Medical Research Pty Ltd v Comrad Medical Systems Pty Ltd.*[14] However, it is and always has been a shaky distinction; for instance, why should there be liability for software supplied with hardware, but no liability if a newer version was subsequently supplied.[15]

2.2 Bespoke Goods

In some respects, a more logical distinction sometimes drawn turns on whether software is standardised or bespoke. The off-the-peg software might be equated with a mass produced product. Bespoke products can be viewed as an individualised service. However, as the Court noted in *Advent Systems Ltd. v Unisys Corporation*, "The fact that some programs may be tailored for specific purposes need not alter their status as 'goods' because the Code definition includes 'specially manufactured goods'." The distinction between bespoke and standardised products might be one that could be defended because customer has potentially more input into custom made goods and also the producer, who might be considered to be providing something akin to a service, has less chance to spread his risk.[16] However, as regards manufacturing defects, a producer making several bespoke products can still spread the general risks of manufacturing defects. The law of sale or product liability does not normally exclude bespoke goods.

[13]For example, the Supreme Court in the *PST Energy 7 Shipping LLC and another v O W Bunker Malta Limited and another* [2016] UKSC 23, which held that the sale of bunkers was not on terms used a sale of goods contract, but rather a *sui generis* contract.

[14][2010] NSWC 267.

[15]Koch (2016).

[16]Zammit and others (1987), Weber (2012), Prince (1980).

2.3 Legislative Approaches

Under CISG, there have been similar debates about whether digital products should be treated as goods.[17] In that context, judicial attempts to interpret the wording flexibly to adapt to technological change may be justified out of a necessity of broadening the scope of an international sales regime that is almost impossible to update.

With so much uncertainty, the logical options would be for the legislator to decide whether digital products were goods. Indeed, some commentators where critical of the EU's failure to address digital products fully when making a proposal for an optional instrument a Common European Sales law.[18] One country that did address this is New Zealand. It simply clarified in its Consumer Guarantees Act 1993 that goods would include computer software.[19] Bradgate could not find any evidence that this had caused any particular problem.[20] The new Australian Consumer Law also includes computer software within the definition of goods.[21]

The modern approach in sales law has, however, been to recognise digital goods as a separate category. The United Kingdom has enacted a separate regime for digital products in its Consumer Rights Act 2015[22] and the EU has now proposed a similar regime.[23] In the context of quality defects, this makes sense as digital products may not fit easily into the traditional sales regimes. For example, programmes will typically have bugs and remedying them is a normal expectation. Thus, both the standards of conformity, satisfactory quality and fitness for purpose, may need to be finessed and the language of remedies may need to be changed as programmes are patched rather than repaired or replaced and it is hard to reject a programme that has been downloaded.[24]

A question we will return to later is whether the EU directive's product liability regime can deal with digital goods or needs to be amended. Giving a hint to future discussions, our feeling is that most issues can perhaps be addressed by reasonable interpretation. As the only remedy is damages, this makes the differences between

[17]Green and Saidov (2007).

[18]Guibault and others (2011).

[19]Section 2(1) states "'Goods':

(a) means personal property of every kind (whether tangible or intangible), other than money and choses in action; and
(b) includes—(vi) to avoid doubt, water and computer software."

[20]Bradgate (2010).

[21]Competition and Consumer Act 2010. sch 2, section 2, following *Gammasonics Institute for Medical Research Pty Ltd v Comrad Medical Systems Pty Ltd* [2010] NSWSC 267, there is a difference in the treatment between consumer and commercial goods in Australia.

[22]Consumer Rights Act 2015, Chapter 3.

[23]Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM (2015) 634 final.

[24]Schulze (2016), Howells and Willett (2016).

products less crucial. The key question remains whether there should on policy grounds be strict liability for digital products. Only if that is answered positively is there a need to discuss whether to create a separate regime or simply to decide if digital products should be classed as products so the strict liability regime applies.

2.4 Digital Products Are Certainly Already Covered When Comprised in a Final Product

The fierce debates over whether digital products are goods or not seem rather strange given that the final producer will be liable for such digital products embedded in his product. Just as the producer is liable for errors in instruction booklets that render his product defective, a producer of a physical product will certainly be liable for damage caused because of an error in the digital product (software) embedded in the physical product. For example, a bug in a car's software might cause brakes to respond more sluggishly than they should, extending the breaking distance and causing a serious accident. Alternatively, thinking about the future, if a self-driving car has a fault in the software that causes it to drive erratically and injure a passenger or by-stander, the car will be condemned as defective. The question of whether the faulty software programme is a product in its own right attracting strict liability or is only subject to negligence liability is relevant as to (a) whether the injured person has a separate of action under the Product Liability Directive against the producer of the component software and (b) whether the car producer can rely on the directive to join the software component manufacturer as a defendant.

This still leaves the question of whether the software is a product in its own right that is capable of attracting strict product liability. The liability choice is between a negligence standard or strict liability. The software might be equated to a service that normally attracts negligence type liability or the programme writing might be seen to have produced a product. An example will be taken from the IofT. Here physical devices are often less significant than the software. For example, consider the situation where a software on a central heating control has a flaw that causes the central heating system to shut down. In sub-zero temperatures this might cause pipes burst and damage the house as a result. The flaw would be very much in the software. This might no longer be an integrated part of the boiler controls. Instead, it might be an app on a phone. Such a scenario squarely raises the issue of liability for software.

2.5 Distinguishing Software from Information

By analogy, this also raises the question of whether physical products that provide information should attract strict liability. For instance, should a map that fails to

indicate an obstacle or a chemistry book that provides the wrong proportions for an experiment give rise to strict liability? Whilst the physical book or map is undoubtedly a product, does the strict liability extend to the content? And, if not, why not?

Some argue that once information in code or writing is materialised in goods such as a CD or a book it should be treated at goods within the scope of the legislation.[25] Borghetti cites a French first instance case imposing liability for the content of a book.[26] However, he notes that the liability was in negligence. In Denmark in 2007, the Maritime and Commercial Court had relied on the Product Liability Act to impose liability on a public agency that published a nautical chart that indicated the incorrect water depth due to information disappearing when old maps were digitalised. The Supreme Court found in favour of the publisher without determining whether the chart was a product.[27]

However, it seems instinctively wrong to treat pure information as products subject to strict liability. Where information is being provided the negligence approach of only imposing liability where responsibility is accepted seems more appropriate. One cannot imagine a lawyer or doctor writing advice on the Internet would accept liability for all harm caused. We certainly would not like to be liable based on any advice in this article. Information is provided to allow the receiver to become better informed so they can make a judgment, but unless in particular circumstances responsibility is taken, it is not subject to negligence liability. It seems a large leap therefore to impose strict liability. The situation may be different where the digital product not merely informs, but also performs a task. Thus, a programme might direct how a car is driven or how much medicine should be delivered to a patient and here the digital product is performing the task without human intervention. It is acting like a product and policy considerations may favour liability.[28]

2.6 What the Legislation Provides

In the first instance, this is an interpretative question. Does the wording of the Directive cover intangible products such as software? Only when that question is answered, is there a basis for assessing whether the current law is correct and determining whether any amendments are necessary. Therefore, the wording of the Directive is a good starting point. Article 2 of the Product Liability Directive provides that 'product' means all movables. It also includes electricity. The mention of movables and the need to specifically mention electricity has led many commentators to consider this excluded incorporeal property such as digital

[25]Triaille (1993).

[26]Borghetti (2004) *citing* TGI Paris (1986) 28 May 1986 RTD civ. 552, note Huet J.

[27]Holle and Møgelvang-Hansen (2016).

[28]Alheit (2001).

products.[29] Although, it has also been suggested the inclusion of electricity might suggest a "slightly reduced corporality requirement."[30] There has been a debate as to whether other incorporeal products are excluded. The majority of judges in the United States[31] and commentators have come down in favour of the exclusion of intangible products,[32] but significantly, some have made an exception for software.[33] The most crucial debate centres on whether software is a product.[34]

The only country to have addressed this issue directly in its implementing legislation is Belgium, which restricts the definition of product to tangible movables, thus excluding software.[35] Whether this is in line with the Directive is debatable. The European Commission believes that the Directive applies to software programmes.[36] Some argue that "software is effectively a material good since it cannot exist without material support and it could not have material effects if it were truly immaterial."[37] Others argue the use of software leads to visibility and thus a certain degree of corporality.[38] This way of viewing software as tangible goods could explain why, while holding that only tangible goods are covered by the text, software is nevertheless covered. However, this reliance on a material medium is outdated and the equation with writing does not fit into a scheme that excludes liability for pure information. We also do not think this question should be determined by some metaphysical debate as to whether code or the pulses sent over the internet contain some physical matter.

There is a need to find a sound policy base for viewing software as products. As we have noted, relying on the fact that software was supplied on or in a durable medium has become unhelpful, as commonly software is simply made available for downloading. A more rational distinction might turn on whether software is standardised or bespoke. There might be some value in equating off the peg software with a mass produced product and viewing bespoke products as an individualised service. The same rationales for strict liability might then apply to the mass produced standardised software. However, the problem with this approach is that artisan goods are not treated any differently to standardised products. However, it is true that the more individualised the programme the more it looks

[29]Ibid 200; Whittaker (1989).

[30]Magnus (2016) Supra n 15, p 245.

[31]Winter v G.P. Putnam's Sons, 938 F.2d 1033, 1036 (9th Cir. 1991); Gorran v Atkins Nutritionals, Inc., 464 F.Supp.2d 315, 325 (S.D.N.Y. 2006).; Way v Boy Scouts of Am., 856 S.W.2d 230, 239 (Tex. App. 1993).

[32]See, for example, Prince J Supra n16, pp 849, 852–855; Scott (1987), Stapleton (1989).

[33]Gemignani (1980–1981).

[34]Whittaker S Supra n 29; Supra n 28.

[35]The Law of 25 February 1991 concerning Liability for Defective Products, Art. 2.

[36]Answer of the Commission on 15 November 1988 to written question No. 706/88 [1989] OJ C144/42.

[37]Supra n 26.

[38]Supra n 30.

like a service. A more convincing distinction is between software, which undertakes actions itself, and software that produces information that is then acted upon by a person. The latter sort of information producing software requires human intervention to use it and arguably is similar in quality to the information found in a book or nautical map and so should not be subject to strict liability. So for instance, if a GPS system instructs you to drive off a cliff the actual decision to do so is not that of the GPS, but the driver who should have final responsibility. However, if software directly has a material effect, such as operating a life support machine or helping land a plane, then it seems valid to treat it as a product and subject it to strict liability. These are likely to be component parts for which the producer of the final product would be liable for in any event. The risk spreading rationale underpinning products liability applies equally to these products. When commercially supplied, software manufacturers should be responsible for physical damage caused by their products not providing the safety that can be expected.

The crucial policy decision should therefore be to class as a product software that is a final product and causes material damage or is a component of the product that makes it function autonomously to cause damage, but to exclude information in written or digital form from the strict product liability regime.

2.7 Wording

How is this policy to be achieved? Can this be achieved by a simple amendment clarifying that software is a product, or would that be too all embracing and capture information provision? It is submitted that such an amendment, along the New Zealand lines can work. If necessary, the distinction can be clarified in the recitals to make it clear that it only covers software that directly or because of its interaction with other products causes damage.

Borghetti favours the exclusion of intangible products because he believes it is hard to apply the terminology of the Directive to them.[39] However, he seems to be contemplating the problems of applying the wording to information. By contrast, he seems to accept software should be included because the Directive is "applicable to damage caused by software programmes, either because they are tangible items or because non-tangible property is already covered by the European text."[40]

For software, there may be some need to be flexible in how the Directive's terms are interpreted, but most of the concepts can cover the supply of software. A general problem is that the meaning and application of some of the broad concepts such as defectiveness are uncertain. This may be inevitable to some extent, but it would be helpful if there were some more clues as to the underlying policy that should inform the Directive's aim of "a fair apportionment of the risks inherent in modern

[39]Supra n 26.

[40]Ibid.

technological production."[41] However, this is no more the case for software than for other many other products such as pharmaceuticals.

Bugs and viruses are two issues likely to figure in software product liability litigation. It is certainly not uncommon for software to contain bugs. Users may expect to put up with some minor bugs, but a bug is less likely to be considered acceptable if it is serious enough to cause harm. Equally, software suppliers will not be liable for viruses if they can prove they infected the software after they had supplied it. The only exception being if the design of the software was defective because it in some way made it easily exposed to attack by viruses. Likewise, the development risks defence may assist producers if truly novel and unanticipated defects arose, but the application of that narrow defence will have to be worked out on a case-by-case basis. Thus if software is expressly included within the definition of product, the liability should be capable of being applied to it. For example, it should not be impossible to consider the software company a producer who manufactured the product, to determine when it was put into circulation or to apply the defectiveness standard to it. The standard of defectiveness makes it clear that the presentation of the product is a relevant factor. This allows the software manufacturer to massage the expectations of its product. However, there is an interesting question about the extent this is possible given exclusions of liability are not allowed.[42]

3 The Commission's Three Questions

As noted above, the Commission has recently posed three particular questions: whether apps and non-embedded software or the Internet of things (IoT) based products are considered as "*products*" under the Directive; whether an unintended, autonomous behaviour of an advanced robot could be considered a "*defect*" according to the Directive; how the strict liability for damages between the different participants in the IoT is allocated, in particular in case of connected objects or sensors relying on each other that are not necessarily under the control of a single *producer*.

Our answer to the first question, based on the discussion above, would be that apps and non-embedded software or the IofT based products should be considered products when they act as products by being able to cause material damage within the scope of the Directive. If they simply provide information on which others act, they should be outside the scope of the Directive.

The unintended, autonomous behaviour of an advanced robot could also be considered a "*defect*". It would not have "provided the safety which a person is entitled to expect".[43] A question posed to us recently was about the moral and

[41] Supra n 5, Recital 2.

[42] *A v National Blood Authority* [2001] EWHC QB 446, 3 All ER 289 (Burton J).

[43] Supra n 6, Art. 6.

liability issues arising if you programme a self-driving car to avoid hitting a child that ran into the road, but which then because of that choice ploughed into a group of people on the sidewalk and killed several bystanders. Our response is that there may be a need for moral discussions about how such algorithms are devised. However, the self-driving car is no different from a real driver faced with such a dilemma. If the car simply veered into the crowd, that would be a defect. However, making hard, but reasonable, choices cannot be a defect. If it veered off to avoid a dog then the standard of safety would be more clearly breached. However, it does raise the question how safe are we entitled to expect such products to be?

As for the connections between IoT products, this liability can be developed along the lines of existing case law that makes producers liable to ensure their products can be used safely with accessories.[44] Products will be defective if they fail to anticipate or provide safe means for their interconnection with products that is foreseeable. Again, the limits of liability will depend upon the application of the defectiveness standard and potentially the developments risk defence. If more than one product is defective and contributes to the damage that is a matter of causation that is left by the Directive to national law.[45]

4 Conclusion

In the sales context a separate category of conformity, rules are being created for digital goods. This is especially needed because of the need to fashion remedies to the digital context. For product liability, a distinction should be drawn between intellectual property which is information and should be subject to negligence law and software that can cause material damage and should fall within the Directive. The Directive should be amended to clarify this. With some ingenuity, the Directive can be applied to software like any other product. There has been less discussion of this issue in relation to product safety, but similar issues might arise. The fact the definition in the General Product Safety Directive[46] states a "product" shall mean "any product" without a restriction to movables may make it easier to ensure software is included.[47] However, this could be usefully clarified at the same time as any product liability amendment.

Acknowledgment Hong Kong (Professor Howells' work was supported by a grant from City University of Hong Kong Project No.9380074).

[44]In a German case, a manufacturer of a motorcycle was found liable in negligence for failing to supervise the accessories market. Parts made by another producer, but aimed at his products, rendered them dangerous: see VI ZR 65/86, NJW 1987, 1009.

[45]Supra n 5, Art. 8.

[46]Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance), OJ L11/4.

[47]ibid, Art. 2(a).

References

Alheit K (2001) The applicability of the ED product liability directive to software. Comp Int Law J South Afr 34(2):188–209

Answer of the Commission on 15 November 1988 to written question No. 706/88 [1989] OJ C144/42

Borghetti JS (2004) La responsabilité du fait des produits. Etude de droit compare, vol 423. LGDJ, citing TGI Paris (1986) 28 May 1986 RTD civ. 552, note Huet J

Bradgate R (2010) Consumer rights in digital products. A research report prepared for the UK Department for Business, Innovation and Skills, University of Sheffield. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31837/10-1125-consumer-rights-in-digital-products.pdf. Accessed 21 Sept 2016

Castells M (2010) The information age: economy, society and culture. Volume I: the rise of the network society, 2nd edn. Wiley-Blackwell, p xvii

Commission Staff Working Document A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe, COM (2015) 192 final

European Commission (2016) Evaluation of the Directive 85/374/EEC concerning liability for defective products. http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_grow_027_evaluation_defective_products_en.pdf. Accessed 24 Oct 2016

Gemignani M (1980–1981) Product liability and software. Rutgers Comput Techol Law J 8:173–204

Green S, Saidov D (2007) Software as goods. J Bus Law 161:164–167

Guibault L, and others (2011) The regulation of digital content contracts in the optional instrument of contract law. Eur Rev Priv Law 6:729–758

Holle ML, Møgelvang-Hansen P (2016) Denmark. In: Machnikowski P (ed) European product liability. An analysis of the state of the art in the era of new technologies. Intersentia, Antwerp-Cambridge, pp 155–172

Howells G, Willett C (2016) 3D printing: the limits of contract and challenges for tort. In: Twigg-Flesner C (2015) Conformity of 3D Prints – Can Current Sales Law Cope?. In: Schulze R, Staudenmayer D (eds) Digital revolution: challenges for contact law in practice. Nomos/Hart, pp 67–86

Koch B (2016) Austria. In: Machnikowski P (ed) European product liability. An analysis of the state of the art in the era of new technologies. Intersentia, Antwerp-Cambridge, p 111

Magnus U (2016) Germany. In: Machnikowski P (ed) European product liability. An analysis of the state of the art in the era of new technologies. Intersentia, Antwerp-Cambridge, p 245

Murray A (2016) Information technology law: the law and society, 3rd edn. Oxford University Press, Oxford

Prince J (1980) Negligence: liability for defective software. Okla Law Rev 33:848

Schulze R (2016) Supply of digital content. A new challenge for European contract law, Howells G (2016) Reflections on Remedies for Lack of Conformity in Light of the Proposals of the EU Commission on Supply of Digital Content and Online and Other Distance Sales of Goods. In: Alberto de Franceschi (ed) European contract law and the digital single market, Intersentia, pp 127–162

Scott A (1987) Software as "Goods": Nullum simile est idem. Comput Law Pract 3(4):133–136

Stapleton J (1989) Software, information and the concept of product. Tel Aviv Univ Stud Law 9:147–163

Triaille JP (1993) The EEC Directive of July 25, 1985 on liability for defective products and its application to computer programs. Comput Law Secur Rep 5:214–226

Weber L (2012) Bad bytes: the application of strict products liability to computer software. St. John's Law Rev 66(2):469–485
Whittaker S (1989) European product liability and intellectual products. Linear Quad Regul 105:125, 129
Zammit J and others (1987) Tort liability for high risk computer software. 1:2–3

Chapter 9
New Liability Patterns in the Digital Era

Rolf H. Weber and Dominic N. Staiger

Abstract The growth of new technologies such as robotics, online sales of goods and services and the creation new digital businesses has created a wide array of new risks and liabilities. In this context, the main areas of EU and US law including the various forms of liability are addressed and potential mitigation strategies proposed.

1 Introduction

The Digital Single Market (DSM) as proposed by the EU Commission in its "Digital Single Market Strategy" on May 6th, 2015 attempts to reform the digital ecosystem in Europe.[1] This development aims at bringing new offerings of goods and services, at changing the manner of business transactions, and at influencing the responsibility of the market participants. A particular focus is placed on the accessibility of digital goods from anywhere in the EU.

However, the respective liability issues have hardly been addressed in the Digital Single Market Strategy. Questions that have been raised are whether the distinction between contract and tortious liability is still suitable in the digital age and what potential consequences arise from the blurred concepts of goods and services. New "actors" such as robots add to the complex mix of technologies that challenge existing notions of contract and tort law.

Within the EU, most countries are based on the Roman civil law system and thus have a different understanding of contract and tort law than common law jurisdictions. In addition, the EU's consumer protection laws further effect contract laws.

Tortious product liability is generally an avenue that is pursued by a party injured by a product and can include a wide variety of damages and compensation. However, in most cases the issue is rather a defective good or service that the

[1] European Commission. Digital Single Market (2016).

R.H. Weber (✉) • D.N. Staiger
University of Zurich, Raemistrasse 74/38, Zurich 8001, Switzerland
e-mail: Rolf.weber@rwi.uzh.ch

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_9

customer wants to return and receive a refund for. These situations shall be governed by the proposed laws under the Digital Single Market Strategy.

Furthermore, technology has created new areas of liability within businesses and in their interaction with customers and other stakeholders. These risks are further aggravated by increasing compliance obligations under data and consumer protection laws. To deal with the additional liability, enterprises must understand the nature of the risks and implement appropriate measures to minimise exposure. Additionally, the risks associated with data and security breaches in the context of new technologies are constantly growing and thus require a refocusing of attention on how safety measures can be included in the design of products, as well as the IT systems in operation.

2 New Technologies

2.1 Internet of Things

The Internet of Things (IoT) has significantly evolved over the last decade starting with passive RFID devices to highly sophisticated networking compatible consumer products. These devices are part of every aspect of daily life as they monitor and control heating and cooling in houses, report traffic conditions through integrated systems in cars, as well as track fitness and movement patterns through mobile phones and wearables.[2]

Liability concerns with regard to the fast growing market of IoT devices, the so-called wearables, are based in data protection, product liability and potential disclosure of trade secrets.

The data protection dimension and potential for infringing privacy are one of the most prominent concerns raised in the context of the IoT. Wearables such as wristbands monitoring hearth rate, fitness levels and location allow a highly accurate assessment of a person's identity. Unfortunately, based on the nature of this product the technology has not been subject to as much protection as for example the health care sector or data in cloud environments. The insurance industry is very interested in gaining access to such IoT data as it allows adjusting the premiums based on the risk the customer presents. Thus, an unhealthy lifestyle will result in higher premiums as will fast driving. Naturally, consumers are concerned with the potential to discriminate based on IoT data, as well as the ability to sell this data to data brokers for third party use.

Nike recently faced the issue of its fitness app being non-compliant with Dutch data protection laws as it processed health data (the fitness of the user) without justification. Furthermore, the policies lacked clarity, as most customers would not have understood that the data is transferred abroad to the US. Thus, to bring its

[2]Eg Fitbit; Google NEST.

terms in line with the EU data protection framework Nike had to make the supply of height and weight information optional (the basis of the health data), inform the customers via email that the supply of this data was optional and acquire their consent for the retention of the data.[3] This example shows how easily data protection is infringed upon even by simple apps through which a user supplies information. In this regard, IoT devices pose an even greater risk as users are often not aware what data is collected and transferred to whom.

2.2 Robotics

A completely new area is initiated with the development of autonomous robots. Even if it is clear that robots are mechanical objects the legal notions applicable to them and the ensuing legal regimes are yet ill equipped to deal with them. As objects, robots fall under the broad definition of machinery pursuant the EU Machinery Directive 2006/42 and as they qualify as products intended for the consumer markets the General Product Safety Directive 2001/95 is applicable. Nevertheless, many provisions of these two Directives are not apt for robots; consequently, the question must be tackled to what extent (1) an analogous application is suitable and (2) the therein contained obligations can actually lead to a liability of the producer of robots.

The liability issues in the robotics environment appear to be even more complicated. The traditional notion of liability is based on the possibility to exert "control" (1) over his/her own behaviour, (2) over produced, offered or sold products, or (3) over actions for which he/she is responsible. However, robots are usually autonomous, i.e. the creator of the device has lost control and the machine is acting on its own sensory perceptions based on its code and self-learning abilities. However, from a philosophical viewpoint a robot does not fulfil the requirements of a moral agent to which moral responsibility can be described.[4] They are designed to carry out a task or achieve a result in the most efficient manner without any free will. A robot setting its own goals and being self-conscious is currently unfeasible and scientists argue whether such a robot could ever be designed.[5]

Theoretically, law knows the strict liability regime for "dangerous activities" of an undertaking; but it is highly doubtful that the simple fact of utilising a robot already constitutes a dangerous activity; the introduction of a strict liability regime would also heavily jeopardise the desired innovation incentives. Another approach consists in an increase of the liability burden of the owner of the robot, possibly combined with a liability cap, but the proof of negligence and causation might be very difficult in an individual case. A reversal of the burden of proof would also

[3]College Bescherming Persoonsgegevens (2015).

[4]Kapitan (1999).

[5]Hertzberg and Chatila (2008).

present a solution that could make it easier for an aggrieved party to bring a claim. However, the overall effect of such a rule could disincentivise the use of highly efficient robot devices and thus must be appropriately balanced against its overall economic effect.

A further solution would be the creation of a legal (electronic) personhood for robots to make them responsible for any damage they may cause leading to the problematic situation that robots are to be considered as autonomous agents. Consequently, none of these proposals convinces at first sight. Moreover, a new functional approach to liability rules appears to be warranted. Amongst others, the use of robots should require the implementation of an appropriate risk management strategy by their owners.

Two main research questions in relation to robotics and the law must be analysed to understand where the road is currently leading with regard to the applicable robotics laws. Firstly, the existing legal frameworks and their adequacy to regulate the highly complex subject matter of robotics and artificial intelligence must be determined. Secondly, the manner in which this technology affects social process and norms should be examined contrasting these developments to what the current framework achieves and what progress is necessary to bring the law in line with the expectations of society. Ultimately, with this information, a set of regulatory guidelines can be proposed to bridge the gap between robotics and the law.

Furthermore, the term robot is extensive and encompasses a vast array of devices. Thus, when approaching the subject of liability for a device and its actions one must first closely assess the specifics of the device in questions and the surrounding circumstances to determine what law is applicable and to what extent. In any case, robots will at the current technological state be subject to the will of a person be this the programmer or user as otherwise the usefulness of a robot would be lost.[6]

2.3 Miscellaneous Technologies

IoT such as Google Glass enable employees to record potential proprietary information at their workplace. This fact is further exacerbated by a constant decrease in size of such devices and the vast array of manufacturers adding new devices to the market.

Drones also present new challenges to regulators, as well as introduce new liabilities. These drones for example can be used for a wide range of purposes considering their capacity to carry items, as well as to record a wide range of digital and audio data. Local regulatory action has already been taken, limiting the use of such devices by the public as they pose significant security, as well as privacy issues. A few near

[6]Bertolini (2013).

collisions with airplanes have been reported. If such a drone collides with a plane, it could cause fatal crashes and create threats for aviation safety.

The commercial use of drones includes intentions of Amazon to deliver their parcels through this convenient method. Furthermore, drones can be used to assess the condition of crop growth to identify areas that need more fertiliser or pesticides. To conduct such assessment, drones fly over the area equipped with a broad-spectrum camera that captures the reflection of light from the crop, which is then used to determine their health.[7]

3 Legal Frameworks

3.1 EU Framework of Online Sales

In respect of electronic contracts in the EU, the basic framework has already been designed by the E-Commerce Directive 2000/31. The formation of electronic contracts and the results of failures in the formation are vaguely regulated and only minimal boundaries for interpretation by Member State courts are set. Previous attempts of harmonising the EU contract law have so far been unsuccessful which is why a less invasive approach to regulating digital contract law has been proposed only governing the essential liability provisions when dealing with consumers. This framework furthermore includes the Consumer Rights Directive, as well as the above-mentioned Directive on Online and Distant Sales.

In this context, for example the burden of proof of the goods' quality lies with the supplier for two years after delivery. In cases of digital content, this burden is never borne by the consumer. In relation to goods, even minor defects allow the consumer to terminate the contract and seek reimbursement when the supplier fails to repair or replace the good. This may lead to an accumulation of risk on the retailers' side, as they must grant more refunds and exchanges and are longer liable for the goods sold. Therefore, the Directive may have a negative effect on small businesses in cases in which the producer or wholesaler of the goods does not adjust its reimbursement policies ancillary to the Directive.

At any rate, risks in digital contract formation are mainly based in the used technology itself and are dealt with similarly in EU and US law. The fundamental problem concerns the allocation of the responsibility for the proper functioning of IT systems amongst the contract parties and the acknowledgement of a meeting of minds. For example, if a party relies on its own IoT (Internet of Things) data that party is usually liable for any costs or loss that occurs in the context of this data. The liability for digital content in a contractual relation can be assessed in line with the traditional legal rules. However, special tasks might become relevant if the burden of proof for the existence of a digital contract must be borne by a contract party.

[7] Eg PrecisionHawk (2016).

Consequently, certain adjustments of the legal framework appear to suffice in this context.

3.2 Supply of Digital Content

In addition to the provisioning of goods a Directive on certain aspects concerning contracts for the supply of digital content has been proposed which should harmonise some of the contractual aspects of digital content contracts.[8] One of the main obstacles to a fully integrated European market is the uncertainty of consumer rights on the national level. The Directive will instill the necessary confidence in buying digital content in another Member State. It shall also apply to digital content for which no price is paid as other performance may well have an effect on the economic interests of the consumer. In some regards, the Directive is groundbreaking as it grants consumers a wide range of benefits in particular with regard to their ability to access content from various locations.

The supply of digital content across the EU has also long been an issue as some service providers only serve select territorial markets. Under the proposal of new EU Digital Content Directive,[9] such a limited approach would no longer be possible, as the provider is required to supply the content anywhere in the EU. Any restrictions on access in another EU country would be unenforceable. The Digital Content Directive aims at encompassing all data-related content that potentially plays a role in connection with digital transactions, particularly data bases, social networks, electronic auction and trading platforms, blogging-environments or even streaming services for movies and data related to 3D printers.[10] The reason for this extensive definition can be seen in the attempt to cover not only the present technologies but also to cater for future developments to avoid not yet available digital content making an amendment of the Directive necessary in the near future.

This law will have significant effects on intellectual and copyright agreements throughout the EU and require licensing parties to reevaluate the currently used territorially based exclusive rights contracts. Such contracts would no longer be permissible in the EU, as the content offered in the home State of an EU citizen must made accessible to that customer when he or she is in another EU Member State. Any contractual provision to the contrary will be void as the Regulation is set to apply retrospectively to all contracts in force. However, a reasonable grace period is included in the draft aiming at giving content providers enough time to adjust to this new setting.

[8]Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law COM (2011) 635 final.

[9]Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of Digital Content COM (2015) 634 final.

[10]Weber and Oertly (2016).

3.3 Tortious Liability

Common law requires as basic elements of a negligence claim (1) a duty of care, (2) the breach of that duty, and a damage that is not (3) remote and (4) unforeseeable. Furthermore, the US allows so-called class actions in which all affected members of a class (the people affected by a product) can bring one single claim resting on the same elements. This allows for a splitting of the legal fees across all class members and thus incentives the litigation of these claims. In contrast, the EU civil law countries generally do not allow for such a class action and the payout for civil damages claims are generally very low compared to the US.

Data protection laws have increasingly gained importance over the last decade as enforcement action and the associated fines have risen. In particular, the new EU Data Protection Regulation (GDPR) and its liability provision of up to 4% of world-wide turnover will present challenges to companies processing personal data of EU citizens, as they must ensure compliance with a range of obligations. These include Privacy Impact Assessments to determine the risk of a processing operation, ensuring a justification for the processing and potential trans-border data transfers are applicable, as well as complying with data subject requests.

In some other fields, the legal framework needs more than just an adjustment or an amendment. The most eminent example concerns product liability as the scope of the regulation is no longer adequate, i.e. a new approach is needed to meet today's reality related to "goods" and "services" characteristics. The Product Liability Directive 85/374 is only applicable in case of (physical) goods; but the non-coverage of services can be hardly justified in the digital era. Therefore, legalistic differentiations between sales of goods and services in e-commerce markets must be abolished.

In the US, the legal framework for product liability encompasses three concepts. These require a manufacturing defect, a design defect, or a warning defect. Defects in this context are intrinsically excessive risks that occur in the use or to a certain extent the misuse of a product. With regard to robotic devices, the most applicable defect argument that could be made is the one concerning the design of the robot. In this case, it must be shown that the risk could have been reduced through a reasonable alternative design, considering the costs and benefits of such an alteration.[11] However, the real measure of liability is whether the risk was foreseeable thus, whether the programmer can foresee the action of a robot. Even if a robot has self-learning capabilities and is to a certain extent able to make autonomous decisions within a set framework of choices, it is still subject to its producer's instructions. Thus, these risks created by a robot are foreseeable and attract liability.[12] If at the time of production of the robot, the risk fell beyond existing scientific knowledge this will shield the producer from liability. However, based on the risks robots

[11] Owen, et al. (2007), p. 40 ff.

[12] *Feldman v Lederle Laboratories*, 479 A.2d 374 (NJ 1984).

create, an exception to the liability provisions or a reduction of liability does not seem warranted as otherwise the end-user would not be sufficiently protected.

Internet intermediaries are a new group of market participants that hardly find a corresponding function in the physical world. Apart from the "normal" well established contractual liability the crucial part of their activities lies in the non-contractual field, i.e. in the potential tortious liability for example in case of illegal disclosure of personal data or of access to illegal information stored on their systems or of non-compliance with copyright law by users of their platforms. In such a situation Articles 12–14 of the E-Commerce Directive apply with a step-regime of limited liability as concretised by court practice (Delphi case[13]). However, these limitations should be re-examined in light of new technologies and if necessary new exclusions developed in accordance with the technical nature of a party's tasks.

3.4 Laws Applicable to Children in the Online World

The protection of children has gained increased attention over the last decade as more children use websites and apps for education and gaming purposes. In the US operators of commercial websites, apps, and online services must provide notice and obtain parental consent before collecting personal information from children under the age of 13.[14] This applies to companies directly targeting or obtaining information about children with actual knowledge that the data is related to children or that the data comes from a service provided to children. However, the consent can be obtained from the school when the data is not used for commercial purposes.

Furthermore, the Federal Trade Commission and the EU Commission on Competition have wide reaching powers to investigate unfair practices, which also consist of gaining an advantage over competitors by not abiding the data protection standards.[15] Thus, it is advisable for enterprises as for schools to be transparent about the data they collect and how it is used. In this regard, the trend has been going towards regulation that places the burden on the companies to appropriately inform their costumers of the data collection and use. This principle is also contained in the GDPR.[16]

[13]ECHR, *Delfi AS v Estonia,* App No 64569/09, 16 June 2015.

[14]Children's Online Privacy Protection Act 15 U.S.C. §§ 6501–6506.

[15]European Commission, Enhancing competition enforcement by the Member States' competition authorities: Institutional and procedural issues, COM (2014) 453 final.

[16]EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1.

In Switzerland, a revision of the current data protection law is being prepared which aims at bringing the Swiss laws in line with the GDPR and addressing issues such as the protection of children in the online world.[17]

4 Future Legal Challenges

4.1 Liability for Robotic Actions

Under the existing laws in the EU, robots cannot be made responsible for any actions. This is based on the notion that robots are unable to "think" and act for themselves as there is always a person administering the commands to the machine.[18] Thus, only the manufacturer or owner of the robot should be held liable when the cause of the actions stemming from a robot can be traced back to either of them. In this situation, the general rules on causality and foreseeability apply, thus the action must have caused the damage and it must have been reasonably foreseeable. Product liability as a special category of tort may also attract strict liability, as well as cases in which the robot is classed as a dangerous device. However, this will depend on EU Member State law and is more akin to common law legal systems than the predominant civil law countries in Europe. The unclear rules in this regard present a significant degree of legal uncertainty for producers and users of robotic devices.

In particular, the medical field is increasingly relying on robotic devices to improve quality of operations. For example, surgical robots are used in cases in which the operation to be conducted is done on a smallest scale such as brain surgery during which robotic devices are maneuvered by a surgeon who is ultimately responsible for the operation. These operators must be specially trained to reduce risk, and to defeat any potential negligence argument an affected patient may raise. However, when there is a malfunction of the robot this will touch upon the product liability provisions which are often ineffective.[19]

Robots, similar to other less sophisticated IoT devices constantly collect and communicate various forms of information through their sensors. Once this data concerns individuals it will likely be subject to the EU General Data Protection Regulation as it allows for the identification of an individual in some direct or indirect way.[20] The obligations to ensure compliance mainly rest on the controller of personal data. This will most likely be the operator of the robotic device. However, when highly autonomous devices are used on a large scale in daily life

[17]Eidgenössisches Justiz-und Polizeidepartement EJPD (2014).

[18]See also Freytag U, Sicherheitsrechtliche Aspekte der Robotik, Sicherheit & Recht 2/2016, for a discussion of the rules and laws that should apply to robotics.

[19]Supra n 7.

[20]Supra n 16.

the determination for whom the device is processing data and for what purpose is sometimes hard to achieve.

The technology underlying robotic actions is very diverse starting with simple commands to sophisticated, fully integrated environments with cloud computing capabilities. Thus, the range of data protection challenges is also highly diverse. Privacy by Design can resolve some of these data protection issues by including data protection and data minimisation procedures at the development stage of the product that is included as a core concept in the GDPR.[21] Such procedures can include encryption, access controls and automatic deletion tools.

As a major part of the newest robotics technology is not developed in the EU but in the US and in other countries these devices will generally not be EU data protection ready and will present significant challenges for foreign developers when trying to enter the EU market. Thus, technology should be developed which enshrines the necessary data protection standards in the data creation of IoT devices such as robots. However, some challenges are hard to overcome. For example, when a robot is designed to respond to vocal commands but is not allowed to eavesdrop. In such a situation, the robot would be required to filter the audio signals received, determine whether it is given a command and immediately delete the data if it is not relevant to a command.

Companion and care robots are a new type of robots designed to support people in their daily lives. In doing so, they must be able to perform legal transactions to for example acquire the basic goods required by their human companion. Furthermore, they may be essential in assisting and caring for elderly people that creates additional risks with regard to an inadequate execution of their functions. During the provisioning of their services they collect data on the individual they are a caregiver for, i.e. not only personal data but also sensitive data that includes health information is stored by the robot.

Thus, new patterns for the emerging new liability challenges must be created encompassing (1) proposals for amendments to existing regulations if the emerging technologies can be handled with the traditional tools, as well as (2) thoughts developed to find future-oriented concepts that can tackle to questions raised in the introduction. In light of the growing amount of artificial intelligence (AI) (apart from the mechanics of robots), a legal personhood for such software based agent may be warranted. This agency however must be registered and accessible to third parties intending to contract with the AI in order to identify the limits set to the AI's abilities to enter into contracts on behalf of its principal.[22]

Another approach to the issue of liability would be the issuance of compulsory third party liability insurance for certain robotic devices. However, this may add unnecessary cost to the use of robots and lead to unintended market effects.

[21] General Data Protection Regulation, Article 23.

[22] Allen and Widdison (1996).

4.2 Cross-Device Tracking

Various technologies are currently used to identify individuals, which all attract some form of data protection liability, as well as liability based on a duty of care.

Probabilistic methods aim at determining the likelihood of a person applying a device by considering access patterns such as (1) the use of a personal computer in the morning and evening when a person is not at work and (2) the use of mobile device during the day. In most cases, cookies are used to identify the devices. By adding deterministic methods such as website, logins to the mix a person becomes fully identifiable.

The Digital Advertising Alliance (DAA) has published its new revised guidance on transparency and control to data used across devices in November 2015.[23] In this guidance, the DAA highlights the need to inform the consumer that the data collected from one browser may be linked to other devices and that the consumer has the option of limiting such collection and use. However, the use of data collected from a device on another device, which is not connected to that device, is prohibited, as well as the use of the data of another device on the consumer's device. Furthermore, the data collected from a device is not being transferred to a non-affiliate third party.

Notice and transparency are a central element of the DAA guidance focusing on the need to inform the costumer of all aspects relating to cross-device practices in the applicable privacy policy of the enterprise. As most users do not read the privacy policy, easy to understand icons and information relating to cross-device tracking must be provided on the website. Automatic plugins that enable the limitation of objection of the consumer to the tracking must be supported as they provide an effective means of enforcing consumer choice. These plugins can also be used to inform a user of any privacy settings of a site that are not compatible with the pre-set privacy level allowing a choice whether to agree to the privacy policy or leave the site. This opt-out function should be applied to all linked devices thus all devices belonging to a specific individual.

In addition to the broader DAA framework, other organisations such as the Network Advertising Initiative set strict standards as to the information policies and choices that must be granted by their members to website users. Essentially, the identification of browsers and devices has been conducted for a long time and allows for targeted advertisement and the displaying of user specific content. In contrast, the newer cross-device linking allows for much more knowledge and surveillance of the individual concerned as once a person is identifiable across his or her devices, tracking and behavioural patterns can be recorded with great precision. Additionally, the linking of data allows the identification of further information that would otherwise not have been available.

[23] Digital Advertising Alliance (2015).

4.3 Regulators and Security Breach Litigation

An important part of any compliance strategy is to identify which regulator is responsible for which oversight measures. This will enable a targeted discussion on potential liability issues and the implementation of measures that comply with the specific requirements of the local regulator. In this context, prioritisation of privacy and security tasks are key to ensuring the most effective risk reduction strategy based on the available resources.

In the US, the Federal Trade Commission oversees any action relating to data and security breaches affecting consumers. Often, high fines are imposed on companies that fail to ensure the security of their customer data including personal, as well as financial data (credit cards). Furthermore, Attorney Generals across the US are increasing their prosecution of such matters.[24] The Federal Communications Commission also recently fined Cox Communications for a security beach affecting 61 customers in the amount of 595,000 USD.

The issue in a class action for a privacy breach is to show damages that are required prerequisite for the success of such a claim.[25] Often the information disclosed carries the potential for abuse but seldom can a traceable use be presented coinciding with subsequent damage at time of the class action against the company from which the disclosed data originated. Additionally, damages based on time expended to monitor personal data, as well as a loss of a bargain were no reduction of the value of the purchased goods has occurred, are not accepted by the courts in being sufficient to prove an injury.[26]

Security Breach Litigation One of the most prominent security breaches in recent time has affected the US retailer Target from which costumer and credit card information was stolen. The case was brought in the Minnesota Federal Court, and consolidated 33 lawsuits.[27] Ultimately, a settlement was reached in the amount of 10 million USD. The judge pointed out that this was a favourable outcome in light of the novel level and the complexity of the issues involved which would have resulted in a long legal procedure. Already up to this point, the legal fees amounted to 6.75 million USD. The challenge in this case was the barred negligence claims based on a lack of economic loss, the ambiguity of security breach notification statutes and the issues surrounding the unjust enrichment argument based on the fact the customers would not have shopped at Target unless their data was safe. The most promising arguments were raised in the context of consumer protection law.

[24]For example, in a New York case in January 2016, the matter was settled by the AG under the condition that the geo-location data will be encrypted, as well as a fine of 20,000 USD paid, because of a failure to inform customers of a breach.

[25]Pisciotta v Old National Bancorp, F.3d WL 2389770 (7th Cir. 2007). Only damages sought were credit monitoring measures that are not recognised in Louisiana as a compensable damage.

[26]In re: SuperValu, Inc., Customer Data Security Breach Litigation, Court File No. 14-MD-2586 ADM/TNL.

[27]In re: Target Corp. Customer Data Security Breach Litigation, MDL No 2522 (D. Minn).

Another retailer, the luxury store Neiman Marcus, was also subject to a hacker attack in 2013 during which potentially 350,000 credit cards were exposed of which over 9200 incurred in fraudulent charges. A class action was brought, however, the Federal Court determined that the class and individual lacked standing. This decision was overturned on appeal. In its judgement, the court analysed the reasoning in Clapper requiring the injury to have occurred or be "certainly impeding".[28] The 9200 plaintiffs who had fraudulent charges were later reimbursed, thus, their loss was the time spent in sorting out the matter. Furthermore, they could only proof the loss of the credit card data not the stealing of their identity. As for the other parties, which had not yet suffered a loss, the Court acknowledged the costs of the monitoring of their credit score and account, as well as the time necessary to mitigate the fraudulent charges on their accounts. In Clapper,[29] the court highlighted that standing to bring a claim could be present based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm. Importantly, the court agreed with the reasoning in Adobe stating that requiring the plaintiffs "to wait for the threatened harm to materialize in order to sue" would create a different problem as "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."[30] Based on the sustained fraudulent charges on the credit cards the pleading standard of "fairly traceable" was met although other disclosures such as through the Target data breach may also have caused the loss.

The issue for companies is the fact that the remedial action in informing its customers of the breach and supplying monitoring services were taken as evidence to establish the injury at the pleading stage of the procedure. This may act as a deterrent for companies to be proactive about security breaches and to take mitigating measures.

In the EU, the risk of litigation on privacy issues has so far been fairly low as most EU Member States do not recognise class actions thus every affected individual has to bring their own case. This is slowly changing as Germany recently passed an amendment to various laws in February 2016 that allows for the bringing of actions by consumer protection associations against companies violating the German data protection law. However, as Germany does not have a class action lawsuit such as the US, this law allowing for an action on behalf of a group of affected individuals was limited to business models that focus on the commercialisation of personal data leaving out the processing for purposes of entering, executing or terminating a contract.[31]

[28]ACLU v Clapper No 13-cv-03994 (S.D.N.Y.).

[29]Clapper v. Amnesty International, 133 S. Ct. at 1150 n.5 (2013).

[30]In re: Adobe Sys., 2014 WL 4379916, at 8 n.5.

[31]Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts BGBl (2016).

Special Aspects of Consumer Data Consumer reporting agencies are central providers of information to businesses in the US, as well as in Europe. However, in Europe the data collection is much more limited than in the US. The recent case of Robins v. Spokeo Inc. before the US Supreme Court, Robin's information had been wrongly recorded in the Spokeo database. He filed a class action against Spoeko in Federal Court for violation of the Fair Credit Reporting Act. To succeed in an Article III[32] proceeding the plaintiff must plead injury in fact. This requires an invasion of a legally protected interest that is concrete and particularised and actual or imminent, not conjectural or hypothetical.[33] In its judgement, the Court highlighted that the concreteness requires the injury to be "de facto, that is, to actually exist".[34] However, as the court wanted to avoid a 4 to 4 split it handed the case down for re-evaluation based on the narrow argument that the lower Court had only focused on the particularity of the injury not its concreteness.

5 Liability Mitigation Strategies

Reducing the risk and thus the level of potential liability for an enterprise are key themes in a compliance strategy. With regard to the liability of robot devices and other automated products companies should assess the risks that are inherent in the design of the technology and proactively take steps to reduce the risk. However, as not all risks can be totally reduced the customer must be made aware of any residual risk, as well as how this can be further reduced through the appropriate use of the device. Following industry standards in product design and testing will also reduce the risk of being subject to liability.

Additionally, internal procedures and security policies should be designed and implemented alongside employee privacy training. Furthermore, a team could be set up to deal with requests from data subjects such as request for access to ones own personal data[35] or general complaint handling relating to personal data processing. This will enable a quick solution to most concerns preventing complaints to data protection authorities or negative publicity. In other cases, a quick assessment should be conducted and controversial or litigation prone issues should be transferred to the Chief Legal Officer immediately.

[32]The Constitution of the United States.

[33]Lujan v Defenders of Wildlife, 504 U.S. 555, 560, pp 7–11.

[34]Spokeo, Inc. v. Robins, Docket No 13–1339, 2.

[35]The following countries currently grant such rights: Australia, China, HK, Japan, Malaysia, Singapore, Canada, US (HIPAA), S. Africa, Austria, Belgium, Denmark, Finland, France, Germany, Italy, Norway, South Africa, Spain, Sweden, Switzerland, The Netherlands and the United Kingdom.

5.1 Enterprise Risk Management

Furthermore, the internal risks must be addressed through appropriate Enterprise Risk Management (ERM) including training of staff, as well as technical safeguards. One staff training per year is seen as sufficient for staff that do not carry out any specific privacy related tasks. However, most privacy breaches occur in a very unspectacular setting such as a work colleague looking into the screen of another or views documents lying on the table.[36] According to a 2015 study, the cost of such a breach based on negligence by the employees amounts to 145 Euro per record.[37]

Mobile devices brought into the company by employees are also a great risk for the security of confidential information. Information shared through the device may be vulnerable such as Emails, other messages or documents when the employee installs unauthorised applications on the device which have not been screened for security risks by the IT department. Thus, effective guidelines and training are core factors of a company's risk minimisation strategy. However, the ease of access to confidential business information coincides with the risks of unwanted disclosure. Essentially, both have to be balanced against each other finding the middle ground between enabling business growth and efficiency whilst ensuring the maximum security of the data.

Personal data should only be made available to staff which requires it as a prerequisite to carry out their job functions. Thus, personal, as well as sensible, data should only be communicated on a need to know basis. The same procedures must also apply to any subcontractors.

5.2 Privacy Compliance

Privacy Impact Assessments (PIA) are an important step in identifying potential privacy issues and developing mitigation strategies for them.[38] Such PIA are now required under the GDPR as part of the mandatory measures when processing personal data of EU citizens. It should include answers to the following questions:

(a) What data is being collected?
(b) Is the data regulated?
(c) Why is it being collected?
(d) Where is it being collected?
(e) Where is it being stored?
(f) How is it protected?
(g) Who will access it?
(h) When will it be destroyed?

[36]Information Week Dark Reading (2015).
[37]Ponemon Institute (2015).
[38]Weber (2012).

These PIA should be conducted in regular intervals assessing all of the company's processing operations, as well as when a new service or processing operation is to be added.

Once the necessary information is known strategies can be developed to address potential risks such as through appropriate contractual provisions for the processing of the data. These include rules on what happens to the data when a merger or acquisition takes place, as well as when another party processing the data is responsible for a breach or the deletion of the data. Maintaining control over the data is key in ensuring the enforceability of any obligations that may materialise down the line.

5.3 Notice and Choice

Most service providers insert the appropriate provisions into their contract informing customers of their extensive power to use various types of data collected during the service offering or acquired from third parties. However, the FTC Chairwoman Edit Ramirez highlighted that customers do not read these policies nor are they able to understand their scope or precise meaning. Thus, future information policies must enable clear notice and choice by the customer. The EU General Data Protection Regulation has enshrined such an approach into the new EU framework of data protection by requiring clear and plain language. Notice provisions or pop-ups on mobile devices should be designed so that the customer knows what information is provided and that he has the right to object. Furthermore, the effects of an objection to the usage of a service should also be made available. This will reduce the potential liability for processing operations that carry a high risk from a data protection and privacy viewpoint based on the argument of voluntary assumption of the risk.

A lab study by Carnegie Mellon[39] has shown that a label approach as used for nutrition information on packaging is highly effective in conveying the necessary data protection information at a glance and easier to understand than a long legal text. As privacy sensitive product can be sold at a premium, enterprises must understand not only the burden of privacy but also the benefits a transparent and conservative privacy strategy can have on a business.

A further step in the notice provisions would be the taking of a mandatory but simple true/false test before being able to approve a company's terms of service or privacy policy. Such a question could for example be "Can the company sell the data it collects about you to another company?" By requiring the consumer to answer 2–5 simple questions he or she will become aware of the major aspects of the data processing and the rights granted to the company. Thus, this could serve as an enforcement tool in meeting the new GDPR standard for consent that requires

[39]Kelley, et al. (2010).

knowledge of the processing and an understanding of the risks for the data subject to effectively give consent to a processing operation.[40]

6 Outlook

The rise of new technologies and a growing complexity of existing technologies have resulted in a steady increase in risk associated with them. Previously, the risk surrounding IT and other technologies were seen by executive boards as an ancillary matter. Today, they present a significant business risk that needs to be accounted for in daily operations. In this context, the role of General Counsels, as well as the Chief Information Officer, has evolved to include more complex interactions between the law and technological challenges. Often clear-cut rules on the use and inherent technological risk do not exist in novel electronic services or fully automated goods. Thus, a multidisciplinary approach incorporating all aspects of the business and the associated risks will enable enterprises to bridge the gap between their business interests and the rising risks associated with their operations.

References

Allen T, Widdison R (1996) Can computers make contracts? Harv J Law Technol 9(1):26–52
Bertolini A (2013) Robotsas products: the case for a realistic analysis of robotic applications and liability rules. Law Innov Technol 5(2):214–247
College Bescherming Persoonsgegevens (2015) A Investigation Nike+Running App. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_dpa_investigation_nike_running_app.pdf. Accessed 20 May 2016
Digital Advertising Alliance (2015) Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices. http://www.aboutads.info/sites/default/files/DAA_Cross-Device_Guidance-Final.pdf. Accessed 20 May 2016
Eg Fitbit. https://www.fitbit.com/de. Accessed 03 Nov 2016
Eg PrecisionHawk (2016) http://www.precisionhawk.com/. Accessed 7 Nov 2016
Eidgenössisches Justiz-und Polizeidepartement EJPD, Normkonzept zur Revision des Datenschutzgesetzes 29.10.2014
European Commission, Enhancing competition enforcement by the Member States' competition authorities: Institutional and procedural issues, COM (2014) 453 final. http://ec.europa.eu/competition/antitrust/legislation/swd_2014_231_en.pdf. Accessed 7 Mar 2017
European Commission (2016). Digital Single Market. https://ec.europa.eu/digital-single-market/node/78515. Accessed 3 Nov 2016
Freytag U Sicherheitsrechtliche Aspekte der Robotik, Sicherheit & Recht 2/2016
Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts BGBl 2016, Part I Nr. 8, 23. February 2016, Article 3 (2)(dd)
Google NEST. https://nest.com/. Accessed 3 Nov 2016

[40]Staiger (2017).

Hertzberg J, Chatila R (2008) AI reasoning methods for Robotics. In: Siciliano K (ed) Handbook of Robotics, Part A/9.1. Springer, p 208

Information Week Dark Reading (2015) A Hidden Insider Threat: Visual Hackers. http://www.darkreading.com/vulnerabilities---threats/a-hidden-insider-threat-visual-hackers-/a/d-id/1323602. Accessed 20 May 2016

Kapitan T (1999) The free will problem. In: Audi R (ed) Cambridge dictionary of philosophy, 2nd edn. Cambridge University Press, Cambridge, p 326

Kelley PG, Cesca LJ, Bresee J, Cranor LF (2010) Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf. Accessed 7 Mar 2017

Owen DG, Montgomery JE, Davis MJ (2007) Product liability and safety: cases and materials. Statutory supplement, 5th edn. Foundation Press, p 40 ff

Ponemon Institute (2015) Cost of Data Breach: United States and Germany sponsored by IBM. http://www-03.ibm.com/security/data-breach/. Accessed 20 May 2016

Staiger DN (2017) Data protection compliance in the cloud. University of Zurich, Zurich

Weber R (2012) Can Data Protection be Improved Through Privacy Impact Assessments? In JusletterIT 12. September 2012

Weber R, Oertly D (2016) E-Commerce and Sharing Economy in Der Europäischen Union: Ein vertragsrechtlicher Überblick, Jusletter IT, N 28

Part III
Intellectual Property Law in the Internet Era

Chapter 10
The Portability of Copyright-Protected Works in the EU

Tatiana-Eleni Synodinou

Abstract This chapter deals with the nascent concept of portability in European copyright law. Two facets of EU portability are explored, with the emphasis on their interaction with copyright law. First is the data portability right in Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data; and second is the Proposal for a regulation on ensuring the cross-border portability of online content services in the internal market.

The data portability right established by the Data Regulation appears *prima facie* as a mechanism linked purely to personal data protection and with no relation with copyright law. Nonetheless, the new right slightly interferes with established copyright principles, and mainly with rules governing the control of use of copyright-protected works in social media, and with EU database copyright protection. On the other hand, the proposed regulation on ensuring the cross-border portability of online content services in the internal market openly and directly challenges copyright law regulation, with a focus on the limitations established by the new portability mechanism on the principle of copyright territoriality and on the protection of copyright as a human right. Although these two EU portability mechanisms interface differently with copyright law, they can be seen as the expression of a new perception of the control of use of works in European copyright law, which introduces certain flexibility in relation to the use of data, services, and applications. Motivated by the EU digital single-market priorities and dogmas, the two EU portability mechanisms appear to promote a vision of a more user-friendly EU copyright law. Nonetheless, this shift is embryonic and mainly symbolic because of the elusiveness and deficiencies in the enforcement of the emergent EU portability norm.

T.-E. Synodinou (✉)
Law Department, University of Cyprus, Panepistimiou Avenue 1, Aglantzia, 2109 Nicosia, Cyprus
e-mail: synodint@ucy.ac.cy

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_10

1 Introduction

The year 2016 has undeniably been a year when portability has been a very topical subject. A new data portability right was finally established in the long-debated and awaited Data Regulation (GDPR), while somewhat unexpectedly, a proposal for a regulation on ensuring the cross-border portability of online content services in the internal market was introduced. Through these regulatory pillars, the rather vague technical concept of portability came to be expressed in a more specific legal form, within what are probably the two most laborious sectors of EU Internet law: personal data protection and copyright law. Even though the portability formulas in these two regulatory instruments present significant differences as regards their aims, justifications, scope and content, both interact with EU digital copyright law, albeit to a dissimilar degree and at a different level.

The two portability formulas aim to regulate different facets of the question of portability. In the Data Regulation, the aim of the new portability right is to provide a remedy for specific functional restrictions, which impede the smooth transfer of users' personal data from one online environment to another. Thus, portability appears in substance as a question of format interoperability. Portability is established as a data subject's right, while at the same time it serves competition law goals, and mainly the prevention of data being locked into a specific platform or of a "switching cost". In this context, portability appears to have a rather discreet interface with copyright law. On the other hand, the proposed Regulation's[1] portability mechanism aims primarily to limit the copyright law-based territorial restrictions that hamper lawful consumers' cross-border access to copyright-protected content in another Member State. Here, the interaction of portability with copyright law is direct, as portability is established as a lawful subscriber's privilege to enjoy copyright- and related rights-protected subject matter across the EU, regardless of the territorial restrictions imposed by copyright holders.

In light of the above, the question that could be logically raised is whether it is methodologically appropriate or reasonable to deal with the two portability formulas together. Furthermore, that of whether a common legal conceptual core of portability is coming into being, because, as we shall show, in both cases portability

[1] See: Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market (2015) and European Parliament legislative resolution of 18 May 2017 on the proposal for a regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market (2017a). For an in depth analysis of the Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market (2015) see: Synodinou (2016) EU Portability Regulation: in-depth analysis of the Proposal. On 21 March 2017 the text agreed during the interinstitutional negotiations on Cross-border portability of online content services in the internal market (2015/0284 (COD) (rapporteur: *Jean-Marie Cavada*) was adopted in the JURI committee andon 18 May 2017 it was approved by the EU Parliament. The draft law still needs to be formally approved by the EU Council of Ministers. See: European Parliament (2017b), Watching online films and TV while abroad, Press Release, 18 May 2017.

appears to be the expression of a flexibility policy which interferes with established copyright and related rights interests, while ultimately the two forms of portability promote EU internal market principles and priorities.

This chapter provides a thorough exploration of these two EU portability mechanisms, with the emphasis on the interference of portability with well-established rules and principles of copyright law, which in this way serves as an essential logical link for analysing both mechanisms together.

Taking as a reference point the divergent features of the two portability formulas, the chapter is divided into two main parts. In Part One, the implications of the Data Regulation's portability on copyright law will be examined (Sect. 2). These repercussions appear mainly on two levels: at a content level in relation to copyright-protected content containing personal data and at a structural level in relation to the interference of the data portability right with the database copyright protection of the structure of an information asset containing personal data. In Part Two, the analysis will focus on the emergence of portability in European Copyright law (Sect. 3). Here the key issue is that of how the emerging portability privilege is challenging the principle of copyright territoriality and specifically whether it appears as a negation or, conversely, as a confirmation of that principle. In this context, it is crucial to examine the legal nature of the proposed Regulation's portability formula, which appears to be an intriguing amalgam, inspired both by mainstream copyright law logic and by consumer law interests. Furthermore, the provisions of the proposed Regulation will be scrutinised to better delineate the impact of portability on the protection of copyright law as a property right.

2 Implications of the Data Regulation's Portability Right on Copyright Law

2.1 The New Data Portability Right and Control of the Use of Copyright-Protected Works in Social Media

Data portability has made a dynamic entrance into the European legal landscape, in Article 20 of Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

According to this provision, where the processing of personal data is carried out by automated means, the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and to transmit this data to another controller without hindrance from the controller to which the personal data has been provided. That right should apply where the data subject provided the personal data based on his or her consent, or where such processing is necessary for the performance of a contract. Recital 68 provides more information about the scope of

application of the new right. It should not apply where processing is based on legal grounds other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of personal data is necessary for compliance with a legal obligation to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.[2]

The justifications of the GDPR's portability right are mainly two-fold. Firstly, the human rights argument to strengthen the data subject's control over his or her own data,[3] and secondly the competition and consumer law interest to prevent the problems of "lock-in" or high switching costs that appear when consumers find it costly or technically difficult to move from one service provider to another.[4]

The data portability right therefore appears to be a powerful tool for a consumer who wishes to migrate his or her personal data from one online platform to another. For example, the portability right could enable a Facebook or Instagram user to take his profile, together with all the personal data posted by him, to Twitter or Snapchat, or more generally, it could permit every user of a cloud storage service to migrate his personal data to another cloud service.[5] At the same time, competition is also enhanced. Competitors might be able to interest consumers in their own services more easily, as consumers will not hesitate to change service providers because of the inconvenience they will encounter in creating their profile and the history of their interactions from scratch. Finally, the motivations for the new right might be less altruistic than they might *prima facie* seem. The data portability right aims to regulate the profitable market in personal data, which is the main source of revenue for information technology companies operating on the Net, by making it easier for newcomers and start-ups to share a part of the tremendous wealth of personal data currently being exploited by Internet giants. In this way, if effectively applied, it could contribute to the World Wide Web's decentralisation efforts.[6]

The right applies only in relation to personal data and not to every type of content. Thus, *prima facie* it does not appear to significantly interfere with content protected by copyright law. However, overlaps will arise, mainly in cases where copyright protection and the protection of a data subject's image as personal data concur. Thus, while an original photograph or a video showing a person will fall within the scope of application of both the portability right and of copyright protection, the transfer of raw information about a data subject will only be subject to the data portability right.

[2]Recital 68 of the GDPR.

[3]Fialova (2014).

[4]Swire and Lagos (2013). For an analysis of the risk of lock in and of high switching costs in cloud computing services, see: Sluijs et al. (2012).

[5]Engels (2016).

[6]See, for example, the Solid ("social linked data") project of the inventor of the Web, Tim Berners-Lee. See: Weinberger (2016).

Indeed, in terms of the interface between the protection of a person's image and copyright law, this relationship is seen as primarily antagonistic, as image rights are traditionally exercised as external limits to copyright law.[7] In general, the clash between the portability right and copyright law is encapsulated in the classic controversies surrounding the coexistence of personal data protection and image rights with copyright law. Even though the conflict usually arises when a person's image is reproduced, adapted and/or communicated to the public by the copyright holder without that person's consent,[8] the opposite situation may also occur. In that case, the individual who is represented in a still or moving image communicates the copyright-protected work representing him or her without the copyright holder's authorisation.

While from the perspective of copyright law such an unauthorised use constitutes a copyright law infringement, the conflict will mainly be resolved on a case-by-case basis through the balancing of the individual's right to his or her image and personal data, and the protection of the copyright holder's property. In this context, the question of the author's authorisation is crucial. The issue is often not straightforward, as the majority of social networking sites introduce clauses in the terms of use of their services requiring users to grant to the network and to its affiliates a non-exclusive royalty-free and permanent licence to use their content.[9]

Using a copyright-protected work in a way that interferes with the rights granted by copyright law may be legitimate if it is done on the grounds of a copyright exception or a copyright licence or contract. The ambit of the contractual right to use a work is dependent on the terms of this contractual relationship, which can be closely or loosely regulated by the national copyright law applicable to the contract.[10] In principle, the acquisition of specific consent for migrating a copyright-protected work to another platform appears to be a necessity in continental law jurisdictions, where the principles of strict interpretation and of specialty in copyright contracts prevail. Nonetheless, in certain cases, the courts might adopt a more flexible interpretation of copyright contracts in light of the application of general principles of contract law, such as that of good faith, as regards the digital reproduction and communication of works via the Internet.[11] For example, even though under strict copyright law terms, "retweeting" or "sharing" a photo on Facebook without the author's authorisation might constitute unauthorized communication to the public, "retweeting" and "sharing" are functions which are part of

[7]For this question see: Synodinou (2014).

[8]See: Tribunal de grande instance de Paris, Ordonnance de référé, Virginie G/Juan F., 10 janvier 2013. Available: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3590. See also: "Right of Publicity Trumps Artistic Freedom of Expression." The 1709 blog. Available: http://www.the1709blog.blogspot.co.uk/2013_01_01_archive.html.

[9]Cahen (2012).

[10]Indeed, the parties can chose the law governing the contract (Art. 3 par. 2 of the Rome I Regulation). See: de Werra (2012).

[11]See for example: Cour Cass, 1re civ., 30 mai 2012, pourvoi n° 10-17.780, Sté Corbis sygma c/M. X.· CA Paris, 4e ch. A, 28 févr. 2007, Propr. intell. n° 24, p. 327, obs. A. Lucas.

the essence of Twitter's and Facebook's services,[12] which the author who first publishes his or her photo on these social networks might be deemed to have implicitly authorised when accessing these services and accepting their terms of use. On the other hand, the same flexibility will not normally apply when publishing a photo found on Twitter on another social network, platform or online medium without the author's authorisation. This has been cleared affirmed in the US in the case Agence France Presse v Morel, where it was found that the licence to use their content granted by Twitter users to Twitter and its partners and affiliates, when accepting the terms of Twitter's use, does not extend to the unauthorised use of such content by other Twitter users. Furthermore, the latter cannot be considered as third-party beneficiaries who are able to enforce Twitter's terms of use for their benefit.[13]

Especially in relation to the application of the data portability right, the main question will not be whether a copyright-protected work was first reproduced and published on an online platform, but that of whether migrating this work to another platform, medium or service will be covered by the initial author's authorisation. This will often be a matter of interpretation. If the author of a photograph showing a person gave authorisation for the publication of this photo generally on the Internet or on social media, migrating the photo from Facebook to a similar online platform will be covered by the initial authorisation. Nonetheless, the collision of the portability right with copyright law cannot be excluded if the author's or other rightholder's authorisation has been given only for use in a specific social media outlet or online platform, or only in a specific context. In that case, the migration and publication of the photograph, and its use on another platform could constitute copyright infringement by the data subject or even by the online service provider, in the event of direct transfer to another platform.

Furthermore, collision might arise in the event of works of multiple authorship, if authorisation to migrate the content has not been granted by all the authors. While the Regulation refers to the case where the migrated content is related to more than one data subject,[14] no similar provision exists for works of multiple authorship. Classic copyright law rules will apply and migration will require the authorisation of all the authors or rightholders. On the other hand, the pure migration of the data to another platform by the user himself, simply for storage purposes, might be

[12]Grondin (2013).

[13]Agence France Presse v Morel, United States District Court, S.D. New York, January 14, 2011, 769 F.Supp.2d 295 (2011). Available: http://www.nysd.uscourts.gov/cases/show.php?db=special&id=256· Agence France Presse v Morel v Getty Images, 10 Civ 02730 (AJN) (SDNY Jan 14 2013). Available: http://www.leagle.com. See also: Klawansky, R.

[14]Recital 68 ("Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation").

considered as being covered by the private copy exception,[15] provided that no communication of the data to the public takes place. If the migration is carried out directly by the data controller to another online platform, the classic copyright law controversy of who has made the copy arises. Even if CJEU case law does not exclude the possibility that the private copy exception applies when a copy is made by a third party for the benefit of the user,[16] the specific features of each online platform's services must be examined to establish whether the reproduction of a work in the cloud can be covered by the private copy exception.

2.2 *The Portability Right: Neutralisation of the Database Copyright Protection?*

A much more complicated and contentious question is the harmonious concurrence of the new data portability right with the copyright protection of the information systems to which portability applies. The data portability does not concern vague and unorganised masses of data, but personal data, presented either as raw or copyright-protected information, which are part of the sophisticated information systems of social media and online platforms.

These systems function on complex internal information structures and algorithms, which are protected by intellectual property law and trade secrets. In this context, the service provider's obligation to provide the data in a structured, commonly used, machine-readable format, and the data subject's right to transmit this data to another controller without hindrance seem to imply a standard of communication—i.e. interoperability—between the information systems of the two service providers. Consequently, the right to data portability is fully guaranteed only if the information systems of the initial service provider and the provider to whom the data will be migrated are compatible. This will typically be the case with open standards. On the other hand, the right would be difficult to enforce in the case of closed proprietary standards, whose structure and technical characteristics remain hidden, as the company that created them calls for their protection by intellectual property law. As we shall show, the Data Regulation has opted for a compromise solution, which appears to be more of a Pythian oracle than an effective regulatory choice promoting data portability.

[15]For such an interpretation see: Cartoon Network, LP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008). It was found that Cablevision, by selling access to a system that automatically produces copies of TV programmes on command, has been assimilated to a store proprietor who charges customers to use a photocopier on his premises. Therefore, the copy in the cloud service is deemed to have been made by Cablevision's subscribers and not by Cablevision.

[16]Copydan Båndkopi v Nokia Danmark A/S, Case C-463/12, Judgment of 5 March 2015.

Online Platforms and EU Database Law

The broad definition of the concept of personal data enables the data portability right to apply to a vast amount of personal information kept and processed by information-service providers: content containing personal data that is posted and stored, the user's profile and list of connections and friends, but also more importantly the entire history of the user's communications, acts and interactions (messages sent and received, history of reactions to other users, history of purchase, history of searches, etc.). Therefore, much or even the entirety of the internal structure of online platforms, social media and other information-society services might be compromised by the service providers' obligation to provide the personal data concerning their users in a structured, commonly used and machine-readable format.

From a purely copyright law perspective, these information systems might fall within the broad definition of a database, which is established in the Database Directive, and consequently, they could be protected by database copyright and the database *sui generis* right. Database copyright law protects the original structure (the "skeleton") of the database,[17] while the database *sui generis* right protects the corpus of the data (the "body" of the database).

Specifically, according to Article 1 par. 2 of the Directive, 'database' shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. The criterion of independence was interpreted by the ECJ in the landmark Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP) case,[18] where it clarified that independent materials within the meaning of Article 1(2) of the directive are those which are separable from one another without their informative, literary, artistic, musical or other value being affected, and consequently, they have an autonomous informative value. In the case of Freistaat Bayern v Verlag Esterbauer GmbH,[19] which concerned the qualification of a map as a database, the Court was asked to elucidate whether geographical data extracted from a topographic map in order that a third party may produce and market another map retains, after extraction, sufficient informative value so as to be held to be 'independent materials' of a 'database' within the meaning of the definition of a database in Article 1(2) of the Directive. The CJEU affirmed its technologically neutral and teleological perception of the concept of a database, and held that it is irrelevant whether the separable pieces of geographical information in the map significantly or completely lose their individual informative value once they have

[17]See Recital 15 of the Database Directive ("(15) Whereas the criteria used to determine whether a database should be protected by copyright should be defined to the fact that the selection or the arrangement of the contents of the database is the author's own intellectual creation; whereas such protection should cover the structure of the database;").

[18]Case C-444/02, Judgment of 9 November 2004.

[19]Case C-490/14.

been extracted. What matters is the value of these pieces of information to the users of sub-products of the initial database made by third parties. The evaluation of the informative value of the materials should be flexible and consider the collective informative value of the reused pieces of information. Accordingly, the Court asserted that not only an individual piece of information, but also a combination of pieces of information could constitute 'independent material' within the meaning of Article 1(2) of Directive 96/9. To reach this conclusion, the Court interpreted the concept of "informative value" liberally by disconnecting it from common value standards, such as the purpose, the principal intended use or the use that would be made by a typical user of a collection such as a topographic map. It seems that for the Court, it is sufficient that the subsequent reuse of the data has a certain independent commercial value,[20] and that the independence of the data is linked to the potential of an autonomous commercial exploitation after its extraction from the "database".

The Court's approach is based on the axiom that even a sole piece of information either taken separately or combined with other pieces can have an autonomous informative value. This broad interpretation of the concept of a database could easily permit the qualification as databases of the vast majority of the Internet's precious information assets, such as websites, blogs, information portals, online platforms and online social networks. For example, all of the users' personal information stored and displayed individually on Facebook could easily qualify as independent works, data or other materials, which are arranged in a systematic or methodical way and are individually accessible by electronic or other means. Interestingly, the application of the data portability right, which allows migration of the data to another platform, where the platform's users will use the data for the same, similar or even completely different purposes, supports this approach.

Certainly, the qualification of an online social network, of a platform, or more generally of an Internet information asset as a database does not automatically trigger database copyright protection. The protection will be awarded only if the database, because of the arrangement or selection of its content, is original in the sense that it is the author's own intellectual creation.[21] The EU "author's own intellectual creation" originality criterion has been one of the emblematic fields of EU copyright law, where the CJEU has demonstrated real interpretative activism and audacity. The interpretation of this criterion, especially in the field of information assets (such as computer programmes and databases), has led to a conception of originality based on the author's free creative choices, which can be ascertained only if the author's choices are not dictated by technical considerations, rules and

[20]For the assessment of the independence of the data on the grounds of purely economic criteria, see: Beutler (1996).

[21]Article 3 par. 1 of the Database Directive.

constraints.[22] The application of this criterion in the case of databases was further scrutinised by the CJEU. As the Court pointed out, the intellectual effort and skill involved in creating this data are not relevant for assessing the eligibility of this database for protection by that right, while it is also irrelevant whether the selection or arrangement of this data includes the addition of important significance to such data or not. Furthermore, the significant labour and skill required for setting up this database cannot as such justify such protection if they do not express any originality in the selection or arrangement of the data that that database contains.[23]

The attempts to satisfy this criterion in the case of online information assets must consider their multi-layered and complex structure. Indeed, the way in which the data is visible to its users is often just the tip of the iceberg. Electronic databases are composite information assets, which are often the combined result of a structural organisational intervention on two levels: an internal (i.e. not visible to the user) and an outer (i.e. visible, which is often the result of the user's search) intervention. During the process of constructing an electronic database, the author may take a series of actions and options characterised by much more creative choices than those made by the creator of a non-electronic database. The overall organisation of both the physical and the logical presentation model of the database is broken down into a series of choices concerning respectively the design, the form, (type, number) and the physical placement of the database's files, subfolders and other components to which the individual information sets will be attached (physical model) and the virtual, user-friendly presentation of the logical relationships and correlations between the database's elements (logical model).[24] Thus, electronic databases, just like every information system, are structured on a combination of three separate structural subsystems: a data storage system, a calculation or organisation system, and an information transmission system. The merger of these three subsystems into an organised group forms each information system, so that the individual features of each subsystem can now serve the general operation of the whole.[25]

[22]Case C-604/10, Football Dataco Ltd and others v Yahoo! UK Ltd and others, 1 March 2012. See par. 38 ("As regards the setting up of a database, that criterion of originality is satisfied when, through the selection or arrangement of the data which it contains, its author expresses his creative ability in an original manner by making free and creative choices (see, by analogy, Infopaq International, paragraph 45; Bezpečnostní softwarová asociace, paragraph 50; and Painer, paragraph 89) and thus stamps his 'personal touch' (Painer, paragraph 92).") and par. 39 ("*By contrast, that criterion is not satisfied when the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom (see, by analogy, Bezpečnostní softwarová asociace, paragraphs 48 and 49, and Football Association Premier League and Others, paragraph 98*").

[23]Football Dataco Ltd and others v Yahoo! UK Ltd and others, op.cit.

[24]The physical and the logical model are two different ways of presentation-registration of the components of the content of a database: the first corresponds to the real way of storing data and is not visible to the user, while the second is a user-friendly presentation based on the logical relationships between the data and does not correspond to their actual storage mode.

[25]According to Bilon, the Simon's three-part classification applies to every information management system. See: Bilon (1993), Simon (1974).

The creativity of the database's author might therefore be manifested at two different levels, either in combination or alternatively: an inner and an outer intervention. On the one hand, the meticulous design of the internal database's files, which constitutes the internal structure of the database that is not visible by the end user, and precedes any form of data storage, requires creative choices. This internal structure is very important for the commercial success of the database largely because it is responsible for the speed of access to the database content. On the other hand, creativity will also be expressed in relation to the external structure of the database: texts, tables and other structural interfaces that form the logical structure of the database, search tools, user interaction points, graphical representations, etc. These outer elements externalise the expression and presentation of the database information system, and at the same time, they ensure its smooth operation. Consequently, the complex information set resulting from the overall design of the database could constitute an original author's own intellectual creation and be protected by database copyright, provided that the author's creative choices are freely made and not dictated by technical or functional restrictions.

Given the complexity of modern online information assets, the originality of their structure will usually not be difficult to affirm. Nonetheless, in relation to interactive online databases, such as social networking platforms, where the database content is not arranged and selected by the author or the maker of the database, but is uploaded by the end users, another question might arise because of CJEU's ascertained preference for a separation of the phase of creation of the database content from the phase of construction of the database. Indeed, as stated in Football Dataco, the concepts of 'selection' and of 'arrangement' of the database content refer respectively to the selection and arrangement of data, through which the author of the database gives the database its structure. By contrast, these concepts do not extend to the creation of the data contained in that database.[26] The database prototype on which the CJEU built this interpretation is the gathering of pre-existing data and their inclusion and organisation within the database's structure. As stated by the Court, it is apparent from Recitals 9, 10 and 12 of the Database Directive that its purpose is to stimulate the creation of data storage and processing systems, to contribute to the development of an information market against a background of exponential growth in the amount of information generated and processed annually in all sectors of activity, and not to protect the creation of materials capable of being collected in a database.[27]

Does this inevitably mean that the substantial prerequisite of an "arrangement or selection of the database content" is absent from interactive online platforms, which are mainly fed by the gathering of user-generated content in a later phase? This is

[26]Par. 32.

[27]See Case C-604/10 paragraph 34· See also the ECJ decisions: C-46/02 Fixtures Marketing, 2004, ECR I-10365, paragraph 33 Case C-203/02 The British Horseracing Board and Others [2004] ECR I-10415, paragraph 30· Case C-338/02 Fixtures Marketing, 2004] ECR I-10497, paragraph 23 ·Case C-444/02 Fixtures Marketing, [2004] ECR I-10549, paragraph 39.

certainly not the case, as it is irrelevant for awarding database copyright protection how, when and by whom the content is included in the database, if the internal and external structure of the database is there. On the other hand, it is equally certain that the intellectual effort or even the originality expressed by the users when generating this content (images, video, private and public conversations, slogans, etc.) will not be considered when granting the database protection.

However, if the data controllers' information systems are protected by copyright law, does this mean that the data portability right is introduced as a new external limitation on their copyright protection? Further, in positive terms, how does this limitation interfere with the protection of these information systems as the property of their rightholders? To answer this question, the exact content and scope of the portability right must be analysed, with a view to exploring how the new right interferes with established proprietary rights and with the data controllers' freedom to conduct their business.

The Delicate Symbiosis of the Portability Right and Database Copyright Law on the Internet

The portability right enables an individual to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and to transmit this data to another controller without hindrance from the initial data controller. Article 20 par. 2 further provides that the data subject, in exercising his or her right to data portability, shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The core of this provision lies in the required technical characteristics in relation to the data format. As it is clearly stated, a data controller shall provide the data in a structured, commonly used and machine-readable format. In the eyes of a simple user who has uploaded his or her data in a popular data format such as PDF or GIF, the obligation might *prima facie* appear as a fairly anodyne task for the data controller. Nonetheless, the provision expressly stipulates that the data format must be "machine-readable". Machine-readable data is data in a format that can be automatically read and processed by a computer.[28] Unlike human-readable formats, which are formats that can be read by a human, machine-readable data must be structured data. It is noteworthy that the most popular file formats for documents (PDF, Word) and bitmap images (GIF, JPEG, PNG, BMP) are unstructured, and therefore cannot meet the technical standard imposed by the Regulation. The Regulation's decision to impose this demanding technical standard is understandable because unstructured documents are unsuitable vehicles for data, as they are designed to be displayed on a screen or printed, rather than to be processed programmatically.[29] Machine-readability is usually understood as making meaningful

[28]For this definition see: http://opendatahandbook.org/glossary/en/terms/machine-readable/.

[29]Source: http://schoolofdata.org/2013/10/21/know-your-data-formats/.

structure explicit, while most machine-readable formats make their structure completely transparent.[30] Simply put, machine-readability, together with the condition of providing data in a common readable form is a hint towards proposing the use of open formats, instead of closed and proprietary ones.[31] On the other hand, rightholders of Internet information assets usually seek to prevent their data being human-readable to prevent their competitors screen-scraping their services and automatically capturing their data.[32] Even more significantly, the innovative nature and the success of these information systems are strongly linked to the secrecy of their internal design and information structure.

In light of the above, the controller's obligation to provide the data in a structured, commonly used and machine-readable format might be interpreted as an obligation to provide the data in interoperable open-standard formats. If this is the true meaning of the provision, then the data portability right will bring radical changes in the way the data is stored and processed on the data controller's information system, whose internal structure has to comply with the Regulation's requirements. Accordingly, a copyright-protected online platform's database will need to be modified to integrate open-standard data formats with a view to making the data portability right workable and effective. To take matters even further, any new platform has to be designed in a way that permits portability to work, thus limiting the creative freedom of the authors of its structure. Nonetheless, the Regulation, as a compromise, does not go that far, and this is clearly stated in Recital 68. Pursuant to this provision, "*the data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible*". Furthermore, data controllers are only encouraged and not obliged to develop interoperable formats that enable data portability. This provision, in conjunction with par. 4 of Article 20, which provides that the portability right shall not adversely affect the rights and freedoms of others, empties the data portability right's technical standard of the substantial core of its meaning.

So, is the data portability right just an empty shell, whose application and enforcement is dependent on the goodwill of the copyright holders of online platforms, social networks and other Internet information assets? If so, speaking in terms of a "right" appears rather misleading. Certainly, the symbolic significance

[30]Source: http://schoolofdata.org/2013/10/21/know-your-data-formats/.

[31]According to Wikipedia, "proprietary format is a file format of a company, organisation, or individual that contains data that is ordered and stored according to a particular encoding-scheme, designed by the company or organisation to be secret, such that the decoding and interpretation of this stored data is only easily accomplished with particular software or hardware that the company itself has developed. The specification of the data encoding format is not released, or underlies non-disclosure agreements. A proprietary format can also be a file format whose encoding is in fact published, but is restricted through licences such that only the company itself or licencees may use it".

[32]Source: http://www.infoworld.com/article/2925041/big-data/make-your-data-both-human-readable-and-machine-readable.html.

of the portability "right", such as it stands in its present form, is much weightier than its real impact. As defending an interpretation of Article 20, which openly contradicts Recital 68, appears paradoxical, another option would be to make the data portability mechanism work through the introduction of a new specific data portability exception to database copyright law, and a new lawful user's unwaivable data portability right. Such an exception would clearly enable the lawful user of a database whose original structure is protected, to migrate, and thus to reproduce, database content containing his or her personal data to another database, by imposing on the database copyright holder the obligation to provide the personal data concerning the user in a structured, commonly used and machine-readable format.

From a pure copyright law angle, this solution might appear much more secure, because instead of taking the form of an external limitation on copyright law, data portability would enter into the well-established set of rules and principles of copyright law, and would then be better circumscribed and "controlled". Furthermore, the very specific scope of such an exception, which would serve only the Data Regulation's portability mechanism, might facilitate its introduction, as the latter will somehow be disconnected by the bigger and thorny debate concerning the advent of an interoperability exception or an exception for standards in copyright law.[33]

On the other hand, such a choice might undoubtedly be considered as heretical from an author-centred copyright law point of view. Indeed, as Carine Bernault notes, generally in relation to the question of the introduction of the interoperability issue within copyright law, such steps may pose a risk of watering down the specific nature of copyright law, as copyright is no longer merely an acknowledged right granted to the creator of a work and intended to protect his or her interests, but it also becomes a way of remunerating investment, and a tool for regulating markets and structuring relationships between competitors.[34] Furthermore, in contrast to the Software[35] and the Information Society Directive's interoperability mechanisms,[36] it would be the first time in EU copyright law that the interoperability privilege is directly granted to an end user. However, the whole edifice of EU database copyright and *sui generis* protection appears to be a deviation or a "foreign body" within classic copyright law, and the addition of such a corrective mechanism, which would enable Article 20 of the Data Regulation to regain a meaning, cannot be seen as a substantial mutation of classic copyright law principles. Furthermore, the restricted scope of its application—i.e. only to copyright-protected content containing personal data—in conjunction with the concurrent application of the three-step test, makes the new right appear less intrusive and menacing for database copyright ownership than it might at first seem.

[33]For the last question see: Koelman (2006).

[34]Bernault (2012).

[35]Article 6.

[36]Article 6 par. 4.

3 The Emergence of Portability in European Copyright Law

The portability of copyright-protected works and other protected subject matter has also emerged in another context, as a means of materialising the primordial Digital Single Market strategy's goal of access to online content services for consumers from wherever they are located in the European Union. The proposal for a Regulation on ensuring the cross-border portability of online content services in the internal market establishes an obligation for online service providers to enable a subscriber to use a portable online content service while the subscriber is temporarily present in another Member State. Furthermore, it provides that any contractual agreements whose effect would be to negate this obligation in the contract between service providers and subscribers shall be unenforceable.

In this context, portability takes the form of a lawful user privilege to enjoy access to and use of copyright and related rights-protected subject matter from anywhere in the EU, despite the territorial restrictions imposed by online service providers and copyright and related rights' holders on the grounds of the well-established principle of copyright territoriality.[37] Ever since the birth of copyright laws, copyright territoriality has acted as an essential safeguard and promoter of national cultural, economic and social idiosyncrasies. On the other hand, within a unified European digital single market, the dogma of the cross-border unhampered flow of copyright-protected content is predominant. In light of the above, the proposed Regulation could take the route either of a final break with the cherished principle of territoriality, by deeming the entire EU to be one copyright territory for online access of EU citizens to copyright-protected works, or alternatively a more conservative approach, whereby copyright territoriality is carefully preserved as the prevailing rule, but some flexibility is introduced through a specific and well-defined exception.

In the following paragraphs, the proposed Regulation's portability will be analysed. Firstly, we shall focus on the impact of portability on the principle of copyright territoriality (Sect. 3.1). Secondly, the specific "mechanisms" of portability will be discussed, with the aim of pinpointing certain grey areas and intricacies in relation to the conception and application of portability (Sect. 3.2).

3.1 Copyright Portability, a Farewell to Copyright Territoriality?

By exporting the cross-border accessibility and use of copyright and related rights-protected works outside the territory of the Member State of habitual residence of a

[37] Peukert (2012).

subscriber to an online service, the idea of online content portability contradicts the exclusive application of national copyright rules solely to the territory of the EU Member State granting it. In this context, it could be considered as a step towards the liberation online content from the fetters of national copyright laws that continue to resist the winds of technological and social changes, and are still abusively partitioning the EU digital market into 28 separate copyright territories.

As we shall show, the proposed Regulation is in general the expression of a restrictive and restrained approach to cross-border access to copyright-protected content, as it does not abrogate or negate the principle of copyright territoriality.[38] Specifically, it appears to be a specific breach of that principle, and thus an exceptional case in which the principle shall not apply. Accordingly, it covers a broad but specific range of online content services and it addresses the needs of a special category of beneficiaries (subscribers-consumers) and not the broader issue of cross-border access to online content within the EU without territorial restrictions. Nonetheless, the path chosen by the EU legislator is not guaranteed to deliver success as the compromise offered by the proposed Regulation is built on nuanced concepts and on fragile balances.

Copyright Territoriality in the EU Digital Single Market: An Oxymoron?

The harmonious co-existence of the principle of copyright territoriality with the free movement of online content services throughout the EU, within a unified digital single market, appears to be an oxymoron. The paradox derives from the deeply divergent roots and priorities of these goals, which could essentially be summed up as the classic dichotomy between diversification and unification. Enabling copyright and related rights-protected content to circulate online without restrictions in the internal digital EU market presupposes the removal of any barriers which could hamper the free flow of works from one Member State to another. Hitherto, the most significant barrier to such a change has historically been the principle of copyright territoriality.

The principle of copyright territoriality is enshrined in the rule of national treatment, which is established in Article 5 (2) of the Berne Convention,[39] and the Court of Justice (ECJ) in its 2005 Lagardère ruling has confirmed it in the EU.[40]

[38]For this view see also: Farrand (2016).

[39]Hugenholtz et al. (2006).

[40]Par. 46: "At the outset, it must be emphasised that it is clear from its wording and scheme that Directive 92/100 provides for minimal harmonisation regarding rights related to copyright. Thus, it does not purport to detract, in particular, from the principle of the territoriality of those rights, which is recognised in international law and also in the EC Treaty. Those rights are therefore of a territorial nature and, moreover, domestic law can only penalise conduct engaged in within national territory." See also: Case C-351/12 – OSA, op.cit. par. 76.

According to this principle, the copyright law applies and is enforceable only to the territory of the Member State that it grants it.

Therefore, despite the EU harmonisation efforts of the last 25 years, there is no uniform EU copyright law, but there are 28 individual national copyright laws that apply respectively in the territory of each Member State. National copyright laws are independent and might present significant differences. Accordingly, the same work can be protected in one Member State, but not to another, while divergent copyright exceptions apply within the territory of the EU.

The principle of copyright territoriality derives from the principle of national sovereignty and is considered as both a safeguard and stimulator for "cultural diversity". Indeed, as it is highlighted by the Institute for Information Law in the Report on the "The Recasting of Copyright & Related Rights for the Knowledge Economy", marketing cultural goods in foreign countries (such as books and films) often necessitates territorial licensing, for instance when the good needs to be customised to cater for local audiences. Furthermore, "*most collective rights management societies currently derive their existence from rights granted or entrusted to them on a national (territorial) basis, while the proceeds from the collective exploitation of these rights flow not only to entitled rightholders, whereby local authors are sometimes favoured over foreign rightholders, but are also channelled to a variety of cultural and social funds, mostly to the benefit of local authors and performers and local cultural development*".[41]

Accordingly, copyright territoriality not only enables copyright rules to reflect the cultural tradition and trends in each individual Member State, but also enables the local cultural economies to sustain and flourish. The existence of multiple economic players in the national cultural markets promotes the pluralism in the distribution and communication channels of cultural goods, as the concentration of the exclusive rights to a few powerful players situated only in a few Member States, might cause the non-accessibility of certain cultural goods to all the EU territories.

Nevertheless, from a purely internal market perspective, which is the major driving force for the harmonisation of EU copyright law, the principle of territoriality appears as an obstacle to the free movement of goods and services in the internal market, as its direct effect is the segmentation of the EU Market in 28 national markets.[42] The disparities caused by copyright territoriality have often been seen as a source of legal uncertainty and of high transaction, licensing and enforcement costs.[43] More significantly, territoriality has majorly been denounced as the main obstacle to the establishment of a unified digital market in Europe.[44] Indeed, the principle of territoriality is ab initio the antithesis of the concept of unification, as

[41]Hugenholtz et al. (2006).

[42]Jougleux (2012).

[43]Madiega (2015).

[44]See for example: Orientation Debate on Content in the Digital Economy (2012)· European Commission: White Paper - A Copyright Policy for Creativity and Innovation in the European Union (2014).

territoriality is by definition linked with the notion of barriers, of "physical lines" having a separating, structuring or an identifying function.

For the distribution of tangible goods the doctrine of the exhaustion of the distribution right, which is a core principle of European copyright law,[45] enables the free circulation within the internal market of a tangible good subject to copyright protection (original work or copy) after its first sale or other transfer of ownership by the rightsholder or with his consent in the territory of a Member State. Thus, the rightholder cannot invoke his exclusive rights to prevent the importation, the export or the resale of tangible goods protected by copyright law that have been put into circulation in another Member State with his consent.[46] Nonetheless, even if it has been highly debated especially after the Used Soft CJEU ruling,[47] no similar principle has been affirmed for intangible goods neither in the EU or internationally.[48] Consequently, the circulation of an intangible good online in the whole territory of the EU presupposes that the service provider has obtained a licence to distribute online the work to all the countries of reception and that, respectively, has cleared the rights in each individual Member State through territorial licensing. If such a license has not been granted, the service provider has to apply geoblocking for disabling the online distribution to territories not covered by the license that was granted to him. Thus, service providers limit territorially the access to the services because they do not have a license to transmit the intellectual property protected content to every country of the reception. It appears that the decision to apply technological restrictions (such as geo- blocking or/and rerouting) is taken either on the own initiative of the service provider to comply with copyright rules or, more often, because of a contractual obligation to geo-block in the contract between the provider and copyright holders. Most often technological restrictions are combined with contractual restrictions on the contracts between the online service providers and their subscribers. In the case where geo-blocking results from an agreement (for example, when it is contractually imposed to the service provider by a licensor), this falls—in principle—within the scope of Article 101(1) TFEU.[49]

On March 18, 2016, the Commission published an initial "Issues paper" on "Geo-blocking practices in e-commerce".[50] As the "Issues paper" confirms, "*With*

[45]Article 4 para. 2 establishes the rule of Community-wide exhaustion of the distribution right. Accordingly, the right is exhausted within the territory of the Community and the European Economic Area if the first sale or other transfer of ownership of an original work or of a copy of it is made by the rightsholder or with his consent.

[46]According to Hilty, even as regards the dissemination of tangible objects, market foreclosures remain still possible because technical protection measures may still hinder the use of tangible copies as long as it is possible to divide the internal market based on differently coded playing devices. See: Hilty (2012).

[47]UsedSoft GmbH v Oracle International Corp., C-128/11, Judgment of the Court of 3 July 2012.

[48]Recital 29 of the Directive 2001/29 appears to exclude such a possibility.

[49]Batchelor (2016).

[50]Commission Staff Working Document (2016).

regard to online digital content, the vast majority of providers participating in the inquiry geo-blocked access to their services to users located in other Member States, mainly through an outright denial of access to the service based on Internet Protocol (IP) address verification. 59 per cent of respondents state that they are contractually required by rightholders to geo-block". However, it is not clear how and under which terms geo-blocking is applied because different practices appear to be applied depending on the category of the online provider or the type of the digital content. Indeed, as the "Issues paper" states *"While licensing agreements on films, TV series and sports events are most likely to include such restrictions, there appear to be large differences in both the extent to which geo-blocking takes place in different Member States, and the extent to which different types of operators implement geo-blocking in relation to different categories of digital content*".

As it is highlighted in the Commission's Staff Working Document "A Digital Single Market Strategy for Europe", "Restrictions to cross-border use often originate from practices aimed at exclusive territorial protection (based on absolute exclusivity in one territory) and are more prevalent for films, TV series and sports programmes. Indeed, producers of audiovisual programmes typically grant an exclusive licence to a single distributor within a given territory. For European films and TV programmes, such an exclusive licence is commonly granted to distributors in order to obtain upfront investments that contribute to the financing of production".[51] Put simply, geoblocking appears as a necessary service restriction to enforce the territorial licensing economic model, which corresponds to the territorial nature of copyright and related rights. This also appears to be in line with Article 20 (2) of the Services Directive. According to this provision, companies may discriminate between service recipients because of nationality or place of residence if it is justified by objective criteria, while Recital 95 of that Directive states that "*Neither does it follow that the non-provision of a service to a consumer for lack of the required intellectual property rights in a particular territory would constitute unlawful discrimination*".[52]

The goal of the achievement of the EU Digital Single Market is undoubtedly found at the antipode of this logic. In this context, the establishment of an EU digital single market has been primarily seen as a call to abolish territoriality. Apart from the possible extension of the exhaustion doctrine to online communications, various approaches, either inside or outside the perimeter of copyright law, have been expressed to mollify the counteractive effects of copyright territoriality for the internal market, such as the application of the "country of origin" principle for the

[51]Commission Staff Working Document (2015).

[52]Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, L 376/36, 27.12.2006. See also: Article 17 (11) of that Directive. See also: Case C-351/12 – OSA, par.64 ("*As regards the question whether Article 16 of Directive 2006/123 applies to such a service, it must be observed, first of all, that under Article 17(11) of that directive, Article 16 does not apply to copyright and to neighbouring rights*.").

online communication of works[53] and the corrective application of EU competition law rules.[54] Certainly, the most maximalist thesis has been the one of replacing national copyright laws by a European Copyright Code or European Unitary Title, on the grounds of Article 118 of the TFEU,[55] which would have given an end to territorial national copyright laws.[56]

While theoretically all of these roads lead to Rome, the materialisation of the most subversive or radical solutions has not thus far appeared to be a realistic option. Indeed, the Commission has finally opted for a notably less holistic approach, with a focus on very specific side-effects of copyright territoriality: geo-blocking and barriers to the portability of legally-acquired content within Europe.[57] In its Communication of 9 December 2015 "*Towards a modern, more European copyright framework*", the Commission's intervention appears more reserved than announced in the Staff Working Paper of 6 May 2015, where concerns were raised both in respect of the portability of content available in the home country and as regards cross-border access to content from another Member State. Indeed, the Commission, following its familiar systematic strategy in the field of copyright law, has separated the issue of portability from the broader question of cross-border access to content from another Member State.[58]

In a similar line of thinking, the European Parliament, in a resolution dated 9 July 2015,[59] supports the Commission's initiatives on the question of portability,

[53]This question is currently under discussion. See on this issue the Full report on the public consultation on the review of the EU Satellite and Cable Directive, 04/05/2016 and the Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes (2016).

[54]Hugenholtz (2013).

[55]According to this provision "*In the context of the establishment and functioning of the internal market, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish measures for the creation of European intellectual property rights to provide uniform protection of intellectual property rights throughout the Union and for the setting up of centralised Union-wide authorisation, coordination and supervision arrangements. The Council, acting in accordance with a special legislative procedure, shall by means of regulations establish language arrangements for the European intellectual property rights. The Council shall act unanimously after consulting the European Parliament.*"

[56]See: DG INFSO and DG MARKT (2009), p. 19: "*By creating a single European copyright title, European Copyright Law would create a tool or streamlining rights management across the Single Market, doing away with the necessity of administering a "bundle" of 27 national copyrights. Such a title, especially if construed as taking precedence over national titles, would remove the inherent territoriality with respect to applicable national copyright rules; a softer approach would be to make such a Community copyright title an option for rightholders which would not replace, but exist in parallel to national copyright titles*".

[57]Commission Staff Working Document (2015).

[58]Commission (2015a).

[59]European Parliament resolution of 9 July 2015 on the implementation of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society P8_TA-PROV(2015)0273.

within the EU, of online services for content legally acquired and made available, whilst affirming at the same time that the existence of copyright and related rights inherently implies territoriality and recalls the importance of territorial licences in the EU. As the Resolution emphasises, there is no contradiction between the principle of copyright territoriality and measures to ensure the portability of content.[60] Similarly, in its draft report on the proposal for the Regulation on Portability,[61] the EU Parliament insists on the solemn declaration of the preservation of copyright territoriality. Specifically, in Amendment 9, it is proposed that an express reference to the significance of copyright territoriality is introduced, as copyright territoriality is considered indispensable for the development and the sustainable funding of the European audio-visual and cinematographic sector. The Report also states that industry geo-blocking practices should not prevent cultural minorities living in EU Member States from accessing existing content or services in their own language, which are either free or paid for. Nonetheless, the proposed Regulation does not deal with this question.

In light of the above, the proposed Regulation's "portability formula" appears to be an exception to the principle of copyright territoriality, which is still the rule. This has a significant effect on how it is to be analysed, because as an exception to the rule of copyright territoriality, it must be interpreted in a way that does not reverse or substantially affect the nucleus of copyright territoriality. Therefore, the Regulation's provisions, as a compromise, carefully avoid to disturb the existing balances and to impose burdensome obligations to service providers and to copyright holders. As in is stated in the Explanatory Memorandum, *"the proposal takes on board a number of concerns signalled by stakeholders, in particular: not imposing a duty to provide portability on those service providers that deliver services free of charge and without authentication of the consumer's Member State of residence; not obliging service providers to deliver the service across-borders with the same quality in the delivery as in the Member State of residence; leaving for the parties to agree on the conditions for ensuring that the service is provided in accordance with the Regulation*".[62]

The proposed Regulation appears to address both technological and contractual territorial restrictions imposed by the service providers. Specifically, it obliges the online services providers to enable the access and use of the online content to subscribers who are being temporarily in another Member State.[63] In parallel,

[60]Report on the implementation of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (2014/2256(INI)), 24 June 2015, Committee on Legal Affairs, Rapporteur: Julia Reda.

[61]Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil visant à assurer la portabilité transfrontière des services de contenu en ligne dans le marché intérieur (2016).

[62]Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market, Brussels (2015).

[63]Article 3.

Article 7 provides that any contractual agreements whose effect would be to negate the obligation of Article 3 in the contract between service providers and subscribers shall be unenforceable.

In the case of technological limitations (mainly geo-blocking), the service provider has the obligation to enable the access and use of the online content service. This, in practice, means that the service providers shall monitor and confirm the temporary location of the subscriber in other Member States and they shall "disable" geo-blocking measures. If the service provider does not apply geo-blocking, but restricts the access and use of the online content service to a particular territory (Member State) only contractually, this contractual obligation shall be unenforceable. Furthermore, in that case the provision shall be understood also in the sense that the service provider is prohibited from applying geo-blocking for the future if the subscriber is being temporarily present in another Member State.

The Legal Nature of Portability: A Right, an Exception or Both?

The proposed Regulation's provisions are vague on the issue of the enforcement of the service providers' portability obligation. In this context, the determination of the legal nature of portability, -a simple copyright exception or a more reinforced legal privilege of the subscriber that could also take the form of a lawful user's consumer right-, is essential for the interpretation and the application of certain key provisions.

Consequently, the introduction of portability in European copyright law brings to the forefront one of the most contentious issues of modern copyright law: the determination of the legal nature of the exceptions to copyright law. Do they grant to copyright users a simple legal possibility to act that is founded on permissive legal rules or do they grant real enforceable rights?[64] The question, although profoundly theoretical, is not a pure doctrinal exercise. The answer presupposes a thorough analysis of the concept of "right" in national legal systems in conjunction with the justifications of the national copyright laws of each Member State. Apart from the Belgian copyright legislation where all copyright exceptions are promoted to *ius cogens,*[65] no other national legislation in Europe declares all copyright exceptions as mandatory.

Traditionally, the research of the position of the user in copyright law could be considered as heretic. Copyright doctrine is characterised by the absence of the user.[66] This controversy stems mainly from the dominant author—centred approach of European continental copyright law (the so called "author's right" approach). According to this approach, the natural person of the author of the intellectual

[64]See on this issue: Synodinou (2010).

[65]Dusollier (2005), Guibault (2002).

[66]Cohen (2005).

creation is the cornerstone of the awarded protection. Public interest is satisfied by the instauration of strictly defined exceptions or limitations to copyright.[67] These exceptions or limitations are not granted in favour of a legally recognised individual entity, but in a general and abstract way in favour of the public. Simply put, the end-user of the works of intellect is not recognised as an individual entity that can claim the application of exceptions or limitations to copyright. Under the light of the above, copyright exceptions or limitations are not traditionally considered as rights of the end-users.[68]

Article 3(1) of the proposed Regulation introduces an obligation of an online service provider to enable a subscriber to access and use the online content service when being temporarily present in other Member States. Furthermore, Article 7 provides that any contractual provisions including those between holders of copyright and related rights, those holding any other rights relevant for the use of content in online content services and service providers, as well as between service providers and subscribers which are contrary to the Regulation, including those which prohibit cross-border portability of online content services or limit such portability to a specific period, shall be unenforceable. The obligation is established as *ius cogens,* which applies irrespective of the law applicable to contracts and, therefore, it is not possible to bypass the Regulation's provisions by defining other Law that is applicable to the contract.[69]

Consequently, portability is established as a mandatory copyright exception that cannot be overridden by contractual terms. The advent of such a "reinforced" exception is not a novelty that is brought in European copyright law by the proposed Regulation. A more robust and active approach to copyright exceptions, which brings closer the "legal prerogatives" safeguarded by the exceptions to the legal nature of "rights", has already been established in the Software[70] and the Database Directive,[71] where the rights of the lawful user of a software or a database were recognised. Recently, in the Ryan air ruling[72] the CJEU affirmed the legal nature of those mandatory exceptions as "rights". According to Recital 39 of the ruling (emphasis added), "*. . .it is clear from the purpose and structure of Directive 96/9 that Articles 6(1), 8 and 15 thereof, which establish mandatory rights for lawful users of databases, are not applicable to a database which is not protected either by copyright or by the sui generis right under that directive, so that it does not prevent the adoption of contractual clauses concerning the conditions of use of such a database*". The Court is more explicit in Recital 40, which states "*That analysis is*

[67]Lucas et al. (2012), Strowel (1993).

[68]Lucas, Lucas, Lucas-Schloetter, op.cit.

[69]Article 7 par. 2.

[70]Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programmes, OJ L 122, 17.5.1991, p. 42–46.

[71]Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28.

[72]Ryanair Ltd v PR Aviation BV, Judgment of the Court of 15 January 2015, Case C-30/14.

supported by the general scheme of Directive 96/9. As Ryanair and the European Commission have stated, that directive sets out to achieve a balance between the rights of the person who created a database and the rights of lawful users of such a database, that is third parties authorised by that person to use the database. . .."

It is undeniable that the attribution of a mandatory character to exceptions or limitations to copyright injects a new perspective into copyright exceptions. It is a point of approach of copyright exceptions with the legal nature of "*rights*". Indeed, the determination of a distinct legal subject, the person of the "*lawful user*", who can claim the application of copyright exceptions and the recognition of the exceptions as "legal prerogatives" of the lawful user that cannot be overridden by the contractual will, marks the advent of a new more active approach of copyright exceptions in EU copyright law. Under the light of this evolution, a new category of "legal prerogatives" also emerges: the "rights of the lawful user". These "rights" could be considered as legal hybrids between exceptions and rights.

Even though not expressly qualified as a "lawful user's right" or a "consumer's or subscriber's right", the obligation of portability which is established by the proposed Regulation, takes the form of a personal right in favour of a consumer. Furthermore, it presents the two essential features of a lawful user's right. First, it is not established generally in favour or the public, but in favour of a specific and distinct legal subject: the subscriber-consumer of an online content service who, based on a contract for the provision of an online content service with a provider, may lawfully access and use such service in the Member State of his residence. Secondly, the portability is fully guaranteed against opposite contractual terms and cannot be overridden by the contractual will.

The qualification of the portability as a legal hybrid between exception and right has concrete consequences. The portability, as a lawful user right, shall be fully guaranteed and enforced both against contrary contractual terms and technological measures of protection (geo-blocking) which prohibit the beneficiary ("the subscriber") to have access to and use the online service, when being temporarily present in another Member State. The establishment of a positive obligation for service providers to enable portability is in line with this approach. Furthermore, the portability, as a mandatory exception, shall be interpreted restrictively[73] and is subject to the three-step test.

The Regulation does not provide how the service provider shall enforce the portability in case of violation of Article 3 (1). This could be a source of legal uncertainty for national copyright laws. Certainly, it could be argued that the margin of appreciation left to the Member States respects the territorial national copyright traditions which have only been harmonised and not unified as far as now. Consequently, each national copyright law will "place" and "qualify" the portability obligation in a way compatible with the national copyright law principles and philosophy.

[73]See: CJEU, Case C-435/12, ACI Adam BV and Others v Stichting de Thuiskopie and Others, Judgment of 10 April 2014, par. 23.

Indeed, introducing portability expressly as a "user" or "consumer" right would appear a priori as a "retreat" of the continental author's rights tradition that denies the recognition or the multiplication of user rights. On the contrary, sanctioning the non-execution of the portability obligation only as a breach of contract by the online service provider leaves the burden of the enforcement of the portability obligation to the consumer. As the proposed Regulation has not expressly opted for a clear mechanism of safeguarding portability against the service provider, it appears to discreetly favour the second option.

3.2 The Specific "Mechanisms" of Portability

The proposed Regulation's portability is constructed as a complex edifice, based on a set of conditions, which aim to safeguard the compatibility of the new exception with the cherished principle of copyright territoriality and the well-established rules of international and European copyright law.

The specific "mechanisms" of the introduction of portability as a new norm in European copyright law embody a modest version of copyright portability. This is also clearly stated in the preamble, where the Regulation's authors aim to reassure everyone that the new exception is a specific case that complies with the copyright *status quo*. Nonetheless, the broad scope of application of the Regulation, its retroactive effect and the flexibilities that it introduces in the interpretation of certain key concepts, together with the hybrid nature of the lawful subscriber's portability privilege, create some grey areas and call for a balancing of the portability mechanisms with the protection of copyright as a fundamental right.

The Muddy Waters of the Scope of Application of Portability

The Teleological Factor: The Main Purpose/Feature of the Service

The proposed Regulation appears to have a broad scope of application. It applies to an "online content service" that are provided lawfully by a service provider on a portable basis and that is an audiovisual media service within the meaning of the Directive 2010/13/EU[74] or a service the main feature of which is the provision of access to and use of works, other protected subject matter or transmissions of broadcasting organisations, whether in linear or nonlinear manner.

In this context, the Regulation's scope is not restricted only to audiovisual services (both linear and on demand), but it covers every service that provides

[74]Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services OJ L 95, 15.4.2010, p. 1.

access to any type of works: e-books, games, images, sport content, news sites. Platforms such as Netflix or iTunes are also covered.

As there is a reference to the concept of "an audiovisual media service within the meaning of the Directive 2010/13/EU" (AVMSD), this shall also be understood in conformity with the interpretation of the concept of "audiovisual media service within the meaning of the Directive 2010/13/EU" by the CJEU. According to Article of the Directive "*Audiovisual media service" means: (i) a service as defined by Articles 56 and 57 TFEU which is under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes, in order to inform, entertain or educate, to the general public by electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC. Such an audiovisual media service is either a television broadcast as defined in point (e) of this paragraph or an on-demand audiovisual media service as defined in point (g) of this paragraph;*". In the CJEU's judgment in the case New Media Online the conditions of application of the Directive to multimedia content offered by a press company was clarified. It was found that videos of short duration which are provided by a newspaper's website constitute content which might classify as a "programme" as defined by the AVMSD on the condition that the form and content of the audiovisual material is independent of written articles.[75]

In both cases (audiovisual media service within the meaning of the Directive 2010/13/EU or a service the main feature of is the provision of access to and use of works, other protected subject matter or transmissions of broadcasting organisations), it appears that the main element that distinguishes the services covered by the Regulation from these which are not covered is the main/principal "purpose" or "feature" of the service (either the provision of a "programme" in case of audiovisual media services within the meaning of the Directive 2010/13/EU" or "the provision of access to and use of works, other protected subject matter or transmissions of broadcasting organisations"). Therefore, services not aiming to offer an audiovisual programme in a way comparable to the form and the content of TV broadcasting (for example, providing a video or a photograph as a complement to a newspaper journalistic article which is published online) are not covered.

[75]CJEU, judgment of 21 October 2015, Case C-347-14 – New Media Online. The concept of 'programme', within the meaning of Article 1(1)(b) of Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), must be interpreted as including, under the subdomain of a website of a newspaper, the provision of videos of short duration consisting of local news bulletins, sports and entertainment clips.

2. On a proper interpretation of Article 1(1)(a)(i) of Directive 2010/13, assessment of the principal purpose of a service making videos available offered in the electronic version of a newspaper must focus on whether that service as such has content and form which is independent of that of the journalistic activity of the operator of the website at issue, and is not merely an indissociable complement to that activity, in particular as a result of the links between the audiovisual offer and the offer in text form. That assessment is a matter for the referring court."

Furthermore, the Regulation does not apply to services which use works or other protected subject matter or transmissions of broadcasting organisations in an ancillary manner (such as graphical elements or music used where the main purpose of the website is not the provision of such works, but other, such as, for example, the sale of goods).[76]

In any case, the concepts of "*principal purpose*" (for an audiovisual media service within the meaning of the Directive 2010/13/EU) and "*main feature*" (other services providing access to works, other protected subject matter or transmissions of broadcasting organisations) must be considered as equivalent.

The proposed Regulation shall also consider the latest developments concerning the review of the Directive 2010/13/EC. Indeed, as regards the definition of an audiovisual media service the Proposal for a Directive amending Directive 2010/13/EU states that "audiovisual media service" means: "*(i) a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or a dissociable section thereof is devoted to providing programmes, under the editorial responsibility of a media service provider, in order to inform, entertain or educate, to the general public by electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC. Such an audiovisual media service is either a television broadcast as defined in point (e) of this paragraph or an on-demand audiovisual media service as defined in point (g) of this paragraph;*". This definition appears to be in line with the findings of the CJEU in the Case C-347-14 - *New Media Online*, which has already been cited. Moreover, additional definitions are introduced, such as the definition of 'video-sharing platform service', 'user-generated video' and 'video-sharing platform provider'.[77]

This might be highly relevant for host providers who also might be deemed to fall within the scope of application of the proposed Regulation. Indeed, while the Regulation's primary aim is to introduce the portability privilege in favour of the lawful subscribers of online service providers, which have an editorial control over the online content they offer, it is less clear under which terms the activities of host providers are also covered. This is also because many online service providers assume both roles either for all their services or for specific online content services.[78]

[76]See Recital 16 of the Proposed Regulation.

[77]Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities (2016).

[78]This is also pinpointed in the recently published Commission's "Issues paper" on "Geo-blocking practices in e-commerce", where it is affirmed that the delineation between the activities of the service providers is not always clear-cut. See: Commission Staff Working Document, Geo-blocking practices in e-commerce, Issues paper presenting initial findings of the e-commerce sector inquiry conducted by the Directorate-General for Competition, op.cit, p. 15.

As it can be assumed that the Regulation also applies to certain categories of "host providers", all the obligations imposed to the service providers by this Regulation must also comply with Article 15 (1) of the E-commerce Directive.[79] According to this provision, "*Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity*."

In the classic case of audiovisual media service within the meaning of the Directive 2010/13/EU, the online content will be communicated to the public by the service provider ("editor") and not by the users. Nonetheless, in the case of services the main feature of which the provision of access to and use of works, other protected subject matter or transmissions of broadcasting organisations, it might occur that the users of the services publish online content. In those cases, the posting of the content by the users on the online platform would normally cover the whole world, if the user has not specifically restricted the access to a specific content to a specific territory. Indeed, par analogy to the line of reasoning in the Svensson case, it could be argued that "*the public targeted by the initial communication consisted of all potential visitors to the site concerned, since, given that access to the works on that site was not subject to any restrictive measures, all Internet users could therefore have free access to them*".[80] Nonetheless, if the user has expressly and specifically put territorial restrictions, the service provider (host provider) shall normally respect the rightholder's will and, consequently, the content shall not be accessible to the territories for which the rightholder (user) did not provide his authorisation. This, for example, could occur when a TV channel is hosting content on an online platform and has put territorial restrictions in respect of all or part of this content. The online content service provider shall block the access to the content posted by the users on those territories, on the grounds of the location of the users who have access to the online content services. To do so, the service provider shall monitor and verify the location of the users of its services.

The Functional Criterion: Services Provided in Return for Payment or Without Payment

Apart from the criterion of the main purpose/feature of the service, the proposed Regulation introduces a significant distinction between online content services,

[79]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000, p 1.

[80]Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd v Retriever Sverige AB,Case C-466/12, Judgment of 13 February 2014, par. 26.

where the main criterion of differentiation is whether the service is provided in return for payment or not.

The Regulation introduces a crucial differentiation of the service providers based on whether the service is provided in return for payment (and, therefore, it falls within the scope of application of the Regulation) or services without payment. In the latter case, the Regulation will apply if the provider has opted for it and if there is verification of the subscriber's Member State of residence by the provider.

Thus, contrary to the initial version of the Proposal,[81] which covered also on line content services, which are provided without payment of money if the provider verifies the subscriber's Member State of residence,[82] the latest version[83] covers only services provided to a subscriber on agreed terms in return for payment. Providers of online content services, which are provided without payment of money, can opt to be included in the scope of this Regulation if they comply with the requirements on the verification of the Member State of residence of their subscribers.[84] In that case, the provider shall inform the subscribers, the relevant holders of copyright and related rights and the relevant holders of any other rights in the content of the online content service of its decision to provide the cross border portability of the online content service, prior to its provision. Furthermore, this information shall be provided by adequate and proportionate means.[85] Consequently, opting in for falling within the Regulation's regime shall be express and straightforward. This is an amelioration compared to the initial Proposal where the fact of the verification of the Member State of residence of the subscriber by the provider of an on line service, without payment, could trigger the application of the Regulation. Accordingly, the scope of application of the Regulation could have been expanded even in cases where the service provider had not expressly chosen for it. This was a source of uncertainty, as on line service providers, without payment, could be caught by the Regulation's ambit by the mere fact of processing the IP address for various purposes of the users of their services, as the IP address check was indicated as one possible means of verification of the Member State of residence of the user.[86]

The distinction acts as a protective shield for the provider of an online service without payment and without a user's registration mechanism, such as Google or Youtube. In this case, the Regulation simply does not apply. For instance, Youtube will not have the obligation to provide access to a Youtube video, which is accessible only in a specific country in another Member State, even if the user

[81]Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market (2015).

[82]Article 2 (e) (2) of the initial version of the Proposal (2015).

[83]European Parliament legislative resolution of 18 May 2017 on the proposal for a regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market (2017).

[84]Article 6 and recital 20 of the proposed Regulation (2017).

[85]Article 6 par. 2.

[86]Synodinou (2016).

proves that he is only temporally present there. The same applies also to Google. Google.com determines the location of the user, and automatically redirects the user to the local portal, often generating different, local search results.[87] A Google user traveling to another Member State cannot claim on the grounds of the Regulation to have access to the same Google results as in the country of his habitual residence when being temporarily in another Member State.

This exemption is justified on the grounds of the principle of proportionality. First, obliging the service providers, when they do not already do it, to verify the Member of residence of their services' users and to monitor their temporary presence in other Member States would significantly interfere with their freedom to conduct business (Articles 16 and 17 of the EU Charter of Fundamental Rights). This is clearly stated in Recital 20 that provides as following: "*Providers of online content services which are provided without payment of money generally do not verify the Member State of residence of their subscribers. The inclusion of such online content services in the scope of this Regulation would involve a major change to the way those services are delivered and involve disproportionate costs*".

Secondly, this exception is compatible with the EU mechanism and principles on personal data protection. It would certainly not have been proportional to oblige every service provider to monitor and record the localisation of the users of its services. On the contrary, in the case of services provided in return for payment, it is can be assumed that the subscriber ("data subject") has already communicated the relevant necessary personal data for the conclusion of the contract of subscription to the service and that the subscriber has agreed contractually to the processing of those personal data for the proper execution of the contract.

The combination of the above two criteria (the provision of works or other protected subject matter as the main feature of the service and provision of the service without payment) will normally exclude the application of the Regulation to on-line applications which produce some content for their users (such as interactive applications providing training programmes, diets, horoscopes etc.) as these will not normally constitute "works" or other protected subject matter. Nonetheless, some intricacies might arise, as there is not a uniform definition of the concepts of "work" and "joint-work" (for content produced with user input and a software application) in European copyright law.

As many of these applications are provided without payment, normally the proposed Regulation will not apply, unless the provider has opted in for providing the cross border portability.

The Regulation does not provide a definition of services provided in return for payment or without payment. Some explanations can be found in Recital 18. As it stated, "*The right to use an online content service should be regarded as acquired against payment of money, whether such payment is made directly to the provider of the online content service, or to another party such as a provider offering a package combining an electronic communications service and an online content service*

[87] Helberger (2007).

operated by another provider. For the purposes of this Regulation, the payment of a mandatory fee for public broadcasting services should not be regarded as a payment of money for an online content service".

While the distinction between services provided in return for payment or without payment appears a priori clear, some grey zones might arise. Indeed, there are some online services (providing mainly videogames) where the user/subscriber does not have to pay for adhering to the service, but payment is requested later if the subscriber chooses to buy additional "features" (music, characters, virtual weapons and abilities, etc.). In that case, even if the classic model of subscription in return for payment is not followed, additional services are provided later on upon payment. For reasons of clarity and to dissipate any doubt, it would have been adequate to include this kind of services in the category of online content services that are provided in return for payment.

Furthermore, it shall also be clarified that the Regulation applies only in case the payment is versed to the online service provider by the subscriber. Indeed, it might occur that an online content service is offered without payment due to the service provider and without an effective mechanism of verification of the user's/subscriber's identity and location by the part of the service provider, where the service provider offers online content (for example an online video game) and the users have the possibility to buy and sell in return for payment virtual abilities or items related to the videogame. In that case, normally the Regulation shall not apply. Nonetheless, if the service provider receives commission fees for acting as an intermediary regarding those sales between its subscribers, a payment is versed to him and the situation might change, as the nature of the service ("without payment") is altered.

Consequently, based on a combination of teleological and functional criteria, and aiming to apply to online content services that provide access to any type of works, the legal amalgam of the Regulation's portability is not strictly restricted to the audiovisual media sector and must be observed by a variety of online service providers. The criterion of whether the service is provided in return for payment or not impedes the application of the Regulation to interactive online platforms. However, in cases where the Regulation's provisions will apply to online host providers, the latter will have to find a proper balance between the portability and the ban on monitoring traffic related to their services imposed under Article 15 of the E-Commerce Directive.

Authentication and Verification: The Cornerstones of the Portability Instrument

The Determination of the Member State of Residence of the Subscriber

Article 5 establishes a detailed mechanism for the verification of the Member State of residence of the subscriber. The lack of such a mechanism was one of the main defaults of the initial text of the Proposal.

Indeed, according to Recital 17 of the initial text, the providers were free to choose the means of verification of the subscriber's Member State of residence, while only a list of possible indicators of means of authentication was provided. The use of those means was not supposed to determine with absolute certainty the Member State of residence of the subscriber, but they could be relied upon if they enabled the provider to have reasonable indicators as to the Member State of residence of the subscriber.

In contrast, Article 5 of the revised text provides for an exhaustive list of verification means of the subscriber's Member State of residence.[88] The service providers can choose the verification means within this list. In this context, the exact means of verification shall be decided by the service providers themselves under the light of the principle of proportionality, as any verification shall not go beyond what is necessary to verify the residence or the presence of a subscriber in a given Member State. While the list is exhaustive, this does not preclude an agreement between providers and rightholders on those means of verification within the limits of the Regulation. Furthermore, a limit on the number of the verification means, which can be used by the provider, is also established. Indeed, the provider shall verify the Member State of residence of the subscriber by using no more than two of the means of verification indicated in the Regulation and shall ensure that the means used are reasonable, proportionate and effective. As Recital 26 states, unless the subscriber's Member State of residence can be verified with sufficient certainty, based on a single means of verification, providers should rely on two means of verification.

The Regulation gives discretion to providers to evaluate whether a single means of verification can verify the subscriber's Member State of residence with sufficient certainty. Right holders are not enabled to require that the service providers use effective means to verify that the service is provided in compliance with the Regulation, as it was the case in the initial text of the Proposal.[89] Consequently,

[88]These are: (a) an identity card, electronic means of identification, in particular those falling under the electronic identification schemes notified in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council, or any other valid identity document confirming the subscriber's Member State of residence; (b) payment details such as the bank account or credit or debit card number of the subscriber; (c) the place of installation of a set top box, a decoder or a similar device used for supply of services to the subscriber; (d) the payment by the subscriber of a licence fee for other services provided in the Member State, such as public service broadcasting; (e) an internet or telephone service supply contract or any similar type of contract linking the subscriber to the Member State; (f) registration on local electoral rolls, if the information concerned is publicly available; (g) payment of local taxes, if the information concerned is publicly available; (h) a utility bill of the subscriber linking the subscriber to the Member State; (i) the billing address or the postal address of the subscriber; (j) a declaration by the subscriber confirming the subscriber's address in the Member State; (k) an internet protocol (IP) address check, to identify the Member State where the subscriber accesses the online content service.

[89]See Article 5(2) of the Proposal (2015).

the control of the application of the Regulation lies solely upon the service providers.

The standard of effectiveness of the verification means is not expressly fixed by the Regulation. The question of "effectiveness" has been raised in European copyright law, both in respect of the prohibition of the circumvention of technological protection measures, in Directive 2001, and in respect of the question of blocking injunctions in IP infringements.[90] In both cases, the standard of "effectiveness" has been interpreted flexibly as being "reasonably" effective, while it has also been affirmed that a standard of absolute or complete effectiveness is not reachable.

Furthermore, the verification shall take place at the time of the conclusion, and upon the renewal, of a contract for the provision of an online content service provided against payment of money. It is noteworthy that the Regulation implicitly classifies the verification means in two categories: means which provide stronger evidence of residence and can be independently relied upon, *(a) to (h)*, and means with more limited verification ability, *(i) to (k)*, which shall only be used in combination with one of the means of verification of the first category.

The IP address check, which identifies the Member State where the subscriber accesses the online content service, falls within the second category and, consequently, it cannot be used as a sole means of verification of the subscriber's Member State of residence. Indeed, the IP address check may not be the appropriate verification means, as it can reveal more data than what is necessary for the Regulation. Specifically, it can lead to the precise location of the subscriber, while for the verification of the subscriber's Member State of residence what matters is not the precise location of the subscriber, but rather the Member State where the subscriber is accessing the service.[91] Furthermore, the IP address based control of the localisation is known for some flaws and making it more effective as a verification means could possibly imply in practice the installation of more sophisticated tools such as proxy or Virtual Private Network (VPN) detection programmes.

Those verification means apply *a priori* to online content services provided against payment of money. Providers of online content services, provided without payment of money, who decide to enable their subscribers, who are temporarily present in a Member State, to access and use the online content service, shall also verify the subscriber's Member State of residence in accordance with the Regulation[92] and, therefore, with the use of those means. Nonetheless, obliging the subscriber to deliver verification documents, such as identity cards or utility documents, might jeopardise the function of certain services without payment which permit their use anonymously, with the use of a pseudonym and without providing a certified address. In those cases, the providers of services without

[90]See: Case C-314/12 - UPC Telekabel Wien, Judgment of the Court of 27 March 2014.

[91]Recital 28.

[92]Article 6.

payment must verify of the subscriber's Member State of residence to be able to provide to their subscribers the right to portability if they decide so. Even though the service providers are free to decide whether they will change their business model to provide to their subscribers the privilege of portability, if they choose so they will have to quit practices that enable anonymity online. Put simply, in those cases the obligation to submit verification documents to be granted the portability right is not in line with the protection of anonymity online.[93]

Interestingly, Article 5 establishes some safeguards that enable the provider to verify with greater certainty the subscriber's Member State of residence. Specifically, Article 5 par. 3 states that if the provider has reasonable doubts about the subscriber's Member State of residence, in the course of the duration of the contract for the provision of an online content service, the provider may repeat the verification of the Member State of residence of the subscriber. In such a case, however, the IP address check may be used as a sole means, while data resulting from the use of IP address check shall be collected in binary format only. Furthermore, the provider shall be entitled to request the subscriber to provide the information necessary to determine the subscriber's Member State of residence. If the subscriber fails to provide that information, and consequently the provider is unable to verify the subscriber's Member State of residence, the provider shall not enable the subscriber to access, or use, the online content service when the subscriber is temporarily present in a Member State. Therefore, when the verification is not possible for reasons related to the subscriber, the cross border portability privilege is neutralised and the provider is not only entitled, but also obliged not to provide the cross border portability.

[93]See on this issue the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (2015). As it is stated (p.19, 20):" 56. *Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. . .60. In addition, States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users. Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms*)." Available at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

The Criterion of "Temporary Presence" in Another Member State Under the Scope of the Three Step Test

The proposed Regulation introduces an obligation for the online service providers to enable subscribers who are temporarily present in a Member State to access and use the online content service.

The portability exception acts in favour of persons who have lawfully acquired access to the services (lawful subscribers of the service) based on a contract. Recital 23 defines what constitutes a lawful provision of services for the purposes of the Regulation by using a dual criterion: the lawfulness of the provision of service and the lawfulness of the provision of the content. Accordingly, an online content service should be considered to be provided lawfully if both the service and the content are provided in a lawful manner in the Member State of residence. This will mainly be the case where a contract is concluded between the provider and the subscriber for the provision of on line services, as long as the content, which is offered, has been authorised by the right holders and/or offered lawfully thanks to the application of certain copyright exceptions. The Regulation gives a broad scope of application to the cross border portability obligation by opting for a broad definition of both the means of provision of services and the term "contract".

According to Recital 15, "*the Regulation should apply to online content services provided on the basis of a contract, by any means including streaming, downloading, through applications or any other technique which allows use of that content. For the purposes of this Regulation, the term contract should be regarded as covering any agreement between a provider and a subscriber, including any arrangement by which the subscriber accepts the provider's terms and conditions for the provision of online content services, whether against payment of money or without such payment*". Nonetheless, the Regulation excludes some acts from this definition. According to Recital 15, a registration to receive content alerts or a mere acceptance of HTML cookies should not be regarded as a contract for the provision of online content service for the purposes of this Regulation. Furthermore, the portability exception does not apply to subscribers who are not consumers (Article 2 (a)).

A key element of the Regulation is the definition of the terms "Member State of residence" and "temporarily present", as the scope of the application of the portability right depends on the interpretation of those terms.

Indeed, because the Regulation introduces a mandatory copyright exception in favour of the lawful users (subscribers) of online services, the exception must be precise to pass the three-step test. This is crucial both in a European and in an international level. As a great number of the online content provided through the services belongs to non-EU rightholders (mainly US), an excessive interpretation of those terms could act against the qualification of the new exception as a certain special case and disturb the international trade. Indeed, according to the test, an exception must be a "certain special case", it "must not conflict with the normal exploitation of the work" and must not unreasonably prejudice the legitimate

interests of the author or other rightholder. In respect of the first condition ("a certain special case"), the WTO panel, in the only case where the compatibility of a copyright exception with the three step test was examined,[94] interpreted this condition as following: "*…, the first condition of Article 13 requires that a limitation or exception in national legislation should be clearly defined and should be narrow in its scope and reach. On the other hand, a limitation or exception may be compatible with the first condition even if it pursues a special purpose whose underlying legitimacy in a normative sense cannot be discerned. The wording of Article 13's first condition does not imply passing a judgment on the legitimacy of the exceptions in dispute. However, public policy purposes stated by law-makers when enacting a limitation or exception may be useful from a factual perspective for making inferences about the scope of a limitation or exception or the clarity of its definition*". However, as the panel decision stressed, "*…there is no need to identify explicitly each and every possible situation to which the exception could apply, provided that the scope of the exception is known and particularised. This guarantees a sufficient degree of legal certainty*."[95]

Thus, the portability exception shall be clearly defined and narrow both "in quantitative as well as a qualitative sense"[96] in its scope and reach. Accordingly, to stay an exceptional special case, the circle of the beneficiaries of the portability exception shall not only be clearly defined, but it shall also be construed narrowly. Thus, the estimated total number of the beneficiaries shall not amount in big numbers reversing the status of the provision as an exception and establishing portability as a rule in all cases. While it is not possible to calculate the exact number of beneficiaries, the proposed provision shall be defined in a way compatible with the three-step test.

The Regulation defines the term "Member State of residence" as "*the Member State where the subscriber has his or her actual and stable residence*". Furthermore, the term "temporarily present" is defined as "*being present in a Member State other than the Member State of residence for a limited period of time*". The combination of the terms "actual" and "stable" means that the residence of the subscriber in a Member State shall be real. Nonetheless, many of the verification means of Article 5, such as the bank account or the credit or debit card number of the subscriber or the registration on local electoral rolls, are purely formal means and are not able to indicate where the subscriber actually resides. In any case, those

[94]Report of the Panel (2000) WTO Document WT/DS 160/R, 15 June 2000, available at www.wto.org.

[95]Par. 6.108, op.cit.

[96]See par. of the panel decision: "The term "special" connotes "having an individual or limited application or purpose", "containing details; precise, specific", "exceptional in quality or degree; unusual; out of the ordinary" or "distinctive in some way". This term means that more is needed than a clear definition in order to meet the standard of the first condition. In addition, an exception or limitation must be limited in its field of application or exceptional in its scope. In other words, an exception or limitation should be narrow in quantitative as well as a qualitative sense. This suggests a narrow scope as well as an exceptional or distinctive objective."

verification means testify a strong link with a Member State, even though not an exclusive one. Indeed, it is possible that persons who have residence in two or more Member States to be able to provide those documents proving residence in a certain Member State, even if they reside in this Member State only for a limited time (for example, during the holidays for expatriates).

There are not quantitative limits on the number of days of presence in a Member State other than the Member State of residence that qualify as "temporary presence". Therefore, the portability exception is applicable to every person in the EU moving/traveling temporarily from his Member State of residence to another Member State for a limited time. Indeed, as it is stated in the Commission's Impact Assessment the main defining feature is that such presence does not change the habitual residence of the subscriber, while the objective of the Regulation would not be served by fixed period of temporary presence, which would imply checks on the exact duration of consumers' presence in another Member State.[97] In a similar line of thinking, the European Parliament, in its draft report on the proposal for the Regulation on Portability[98] suggested that the concept of "temporary presence" should be proportionate to the objective of this Regulation, namely to provide cross-border portability of online content services to subscribers residing transiently in another EU Member State and returning regularly to their Member State of residence. As is also stated in the draft report, the portability privilege could be granted, for example, in cases of temporary presence in other Member States of the European Union, for reasons of leisure, business or education.[99]

The choice of the EU legislator for flexibility is understandable because it would be complicated and burdensome in its application, -even though it could make the exception more "certain"-, to set fixed time lapses (for example, a fixed number of days abroad per stay or per year) which qualify as temporary presence. Indeed, the temporary presences in another Member State might be often and in various periods over the year and a numerical fixed restriction (for example, a maximum of 10 days in a row combined with a maximum of 10 months of presence out of the Member State of residence in a year) would be complicated to apply for service providers.

Moreover, such a restriction is not justified by the purpose of the portability exception, which is ultimately to enable a lawful subscriber to access the online content service they have lawfully purchased wherever he is located in the EU, if his presence is not permanent in this other Member State. This flexible approach is also in line with the line of reasoning of the CJUE in the Football Premier League case.[100]

---

[97]Commission (2015b), p. 24.

[98]Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil visant à assurer la portabilité transfrontière des services de contenu en ligne dans le marché intérieur (COM (2015)0627 – C8-0392/2015 – 2015/0284(COD)), Commission des affaires juridiques, 21.6.2016.

[99]Amendment 2.

[100]C-403/08 - Football Association Premier League and Others, Judgment of the Court (Grand Chamber) of 4 October 2011. According to the CJEU, "*On a proper construction of Article 56 TFEU:– that article precludes legislation of a Member State which makes it unlawful to import*

As the portability is subject to the regime of copyright and related rights exceptions, the rule shall be construed narrowly and shall stay an exceptional case. This means that the exception cannot apply to situations where the criterion of "temporally presence" is abused. A parallelism could be made with the final agreement reached on June 30, 2015 for the end of roaming charges in respect of "permanent roaming", where the rules prevent abusive and unusual uses (for example, if the customer buys a SIM card in another EU country where domestic prices are lower to use it at home; or if the customer permanently stays abroad with a domestic subscription of his home country).[101]

The Content and the Ambit of Portability

Articles 3 and 4 of the proposed Regulation define the scope and the content of the portability, which is constructed both as a copyright exception and as a consumer right. According to those provisions, the provider of an online content service shall enable a subscriber who is temporarily present in a Member State to access and use the online content service without any additional charges. The use of the broad terms "access" and "use" is pertinent, as this will normally cover both situations where the users are prevented from accessing online content that they lawfully purchased in one Member State when being temporarily present in other Member States, but also to "use", such as playing digital content that they lawfully downloaded in a Member State when being temporarily present in other Member States.[102]

It is noteworthy that this obligation does not extend to any quality requirements applicable to the delivery of an online content service that the provider is subject to when providing this service in the Member State of residence, unless otherwise expressly agreed by the provider and the subscriber.

Article 3 par. 3 states that *"The provider shall not take any action to reduce the quality of delivery of the online content service when providing the online content service in accordance with paragraph 1"*.

---

into and sell and use in that State foreign decoding devices which give access to an encrypted satellite broadcasting service from another Member State that includes subject-matter protected by the legislation of that first State;– this conclusion is affected neither by the fact that the foreign decoding device has been procured or enabled by the giving of a false identity and a false address, with the intention of circumventing the territorial restriction in question, nor by the fact that it is used for commercial purposes although it was restricted to private use. 4. The clauses of an exclusive licence agreement concluded between a holder of intellectual property rights and a broadcaster constitute a restriction on competition prohibited by Article 101 TFEU where they oblige the broadcaster not to supply decoding devices enabling access to that rightholder's protected subject-matter with a view to their use outside the territory covered by that licence agreement".

[101] European Commission (2015).

[102] For these kinds of restrictions see: Commission Staff Working Document (2016).

Article 3 par. 4 specifies further the obligation of the provider to provide information about the quality of services. According to this provision, the provider shall, from the information in its possession, provide the subscriber with information concerning the quality of delivery of the online content service. The information shall be provided to the subscriber prior to providing the online content service and by adequate and proportionate means. Recital 22 provides some further explanations and states that "*The provider, on the basis of the information in its possession, should provide its subscribers in advance with information concerning the quality of delivery of an online content service in Member States other than their Member State of residence, in particular the fact that the quality of delivery could differ from that applicable in their Member State of residence. The provider should not be under an obligation to actively seek information on the quality of delivery of a service in Member States other than the subscriber's Member State of residence. The relevant information could be provided on the provider's website*". This is a clear improvement of the initial text of the Proposal, where it was not stated when and how this information shall be provided.

The Legal Fiction of Article 4 Under the Scrutiny of the Protection of Copyright as a Human Right

One of the biggest innovations of the proposed exception lies in the legal fiction, which is introduced by Article 4. According to this provision, "*The provision of an online content service under this Regulation to a subscriber who is temporarily present in a Member State, as well as the access to and the use of that service by the subscriber, shall be deemed to occur solely in the subscriber's Member State of residence*". Simply put, the act of communication to the public and of the reception of the service shall be deemed to occur solely in the Member State of the subscriber's residence and not in the place where physically occurs (the Member State where the consumer is "temporarily" present). This means that from the moment that those acts have been authorised by the rightholders for the Member State or residence of the subscriber, this initial authorisation will cover every subsequent act covered by copyright or related rights or by the database sui generis right (which is made either by the service provider either by the subscriber for having access to the service) which occurs in the Member State of the temporary presence of the subscriber. This provision is necessary for ensuring that neither the service provider or the subscriber will breach copyright law, related rights and the database sui generis right when offering the online content service or when receiving the online content service out of the Member State of the subscriber 's residence.

Such legal fictions are exceptional, but certainly not unknown to European copyright law. Examples of analogous "legal fictions" in European copyright law

are Article 1 (2) (b) of the Satellite and cable Directive[103] or even the Svensson's ruling[104] legal presumption that "*. . . where all the users of another site to whom the works at issue have been communicated by means of a clickable link could access those works directly on the site on which they were initially communicated, without the involvement of the manager of that other site, the users of the site managed by the latter must be deemed to be potential recipients of the initial communication and, therefore, as being part of the public taken into account by the copyright holders when they authorised the initial communication*."

Intellectual property is protected as property by the European Convention of human rights.[105] As this legal fiction interferes with established intellectual property rights, it has to be explored whether this provision could be considered as an unforeseeable and unfavourable for copyright holders interpretation of the scope of copyright and related rights and,[106] as result, whether it fulfills the legality requirement in the fair balancing between intellectual property (Article 17 par. 2 of the Charter) and the general interest.

The Service Providers' Obligation of Enforcement: Evasive or Effective?

On the other hand, one of the most significant weaknesses of the proposed provision can be found in the fact that the Regulation does not define neither the legal nature of the obligation of the service provider to enable a subscriber who is temporarily present in a Member State to access and use the online content service or the legal consequences (type and form of "penalty") for the service provider if the provider does not enable the portability of the online content service. Recital 21 states vaguely that "*It is essential that the obligation to provide cross-border portability of online content services be mandatory and therefore the parties should not be able to exclude it, derogate from it or vary its effect*". In any case, Recital 21 makes it clear that the service provider is obliged to provide the online content service without deliberately technically or/and contractually "downgrading" it or restricting it, when the latter is offered in another Member State. As it is stated,

[103]Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission. According to this provision: "*(b) The act of communication to the public by satellite occurs solely in the Member State where, under the control and responsibility of the broadcasting organisation, the programme-carrying signals are introduced into an uninterrupted chain of communication leading to the satellite and down towards the earth*".

[104]Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd v Retriever Sverige AB, Case C-466/12, Judgment of 13 February 2014.

[105]See: Dima v Romania, App. No, 58472/00 · Melnychuk v Ukraine, App. No. 287343 · Anheuser-Busch Inc. v Portugal, App. No, 73049/01.

[106]As Griffiths and McDonagh note, "*in the case of an unforeseeable unfavourable interpretation of the scope of an intellectual property right or of an exception to that right, a right-holder may be entitled to rely upon Art 17 (2) in objecting to that interpretation*". See: Griffiths and McDonagh (2013).

"Any action by a service provider which would prevent the subscriber from accessing or using the service while temporarily present in a Member State, for example restrictions to the functionalities of the service or to the quality of its delivery, would amount to a circumvention of the obligation to enable cross-border portability of online content services and therefore would be contrary to this Regulation". This provision must be read in conjunction with Article 3 and Recital 22 of the proposed Regulation. The latter sets the acceptable and appropriate quality standard of delivery of the service when the latter is provided in another Member State on the grounds of the Regulation. This is the "*the quality available via the local online access chosen by a subscriber while temporarily present in another Member State*".

It is not clear whether the service provider shall automatically enable the portability of the service when the presence in another Member State is technically noted (via the IP address) or whether the subscriber shall or may inform the service provider accordingly. In any case, the first option appears more logical because it would be burdensome for the consumer to "report" the temporary stay in another Member State to the service provider.

Furthermore, the portability may mean loss of quality of the service and the automatic application of portability could induce some miscomprehension from the consumer. Article 3 par. 4 deals with this question. According to this provision, "*The provider shall, on the basis of the information in its possession, provide the subscriber with information concerning the quality of delivery of the online content service provided in accordance with paragraph 1*". This could be understood as the introduction of a complementary obligation to inform the user of the portability's activation.

As the portability has also the form of a consumer right (a lawful subscriber right that cannot be overridden contractually), it goes without saying that the consumer shall even have the right to self-help, thus to "circumvent" or bypass technical territorial restrictions to access the service in the Member State where he is temporarily present (for example by using a proxy server indicating an IP address in the Member State of residence) if the service provider does not enable the provision of service abroad.

Some additional explanations on the mechanisms of enforcement of the portability right would have been beneficial to the effectiveness of the Regulation. One solution would be to consider the denial of access to the service, in violation of the right to portability, as a breach of contract. As the proposed Regulation does not expressly opt for another solution, an implied reference to this mechanism could be assumed. Nonetheless, sanctioning the non-execution of the portability obligation only as a breach of contract by the online service provider leaves the burden of the enforcement of the portability obligation to the consumer. In this context, the service providers' positive obligation to enable portability shall be read under the light of the Consumer Rights Directive.[107] Article 24 (1) of the Directive states that

[107]Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the

"*Member States shall lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive*". This could be understood as a possibility to vest National Consumer Agencies the responsibility for the enforcement of the portability right.

Another route would be to align the enforcement of the portability right with the solution adopted in Article 6(4) of the Information Society Directive as regards the guarantee of certain exceptions against the application of technological protection measures. According to this provision, "*4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.*"

This parallelism is justified because in both cases (copyright exceptions whose exercise is being hampered by technological protection measures and the portability right whose enjoyment is hampered by geo-blocking) lawful access to copyright and related rights-protected content is de facto restricted because of the application of technical means of restriction. Therefore, useful lessons can be derived from the implementation of Article 6 (4) in Member States. As the Study on the implementation of Directive 2001/29/EC in the Member States provides, "*Procedural solutions for resolving disputes between right holders and certain beneficiaries have been implemented in some Member States that have transposed Article 6(4)…. These include direct access to the judiciary; access to specific administrative proceedings resulting in an administrative order that can be challenged before courts; arbitration procedures resulting in an award that can eventually challenged before courts; mediation and similar dispute resolution mechanisms*;"[108]

The Supremacy of Portability Over Contracts

The Regulation safeguards the effective application of the portability right by invalidating any contractual provisions that prohibit the portability as unenforceable (Article 7) and by giving to the provisions of the Regulation a retroactive effect (Article 9). At first, this would appear a priori compatible with the principle of proportionality, because, by ensuring the application of portability on the grounds

European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304/64, 22.11.2011.

[108] Westkamp (2007).

of the existing contracts which are interpreted mandatorily in a way compatible with the proposed Regulation's provisions, the Regulation appears to mainly respect content of existing licensing contracts and it does not oblige rightholders and service providers to renegotiate those contracts.[109] Nonetheless, a further scrutiny is necessary as the Regulation interferes retroactively with existing contracts. Therefore, it introduces a deviation from the as far as now established EU copyright law principle that EU legislative measures do not affect duly acquired rights, including rights acquired from a contract.[110]

The mechanism of declaring certain copyright exceptions as mandatory in the sense that they cannot be overridden by opposite contractual provisions has been used sporadically in other EU copyright law instruments (the Software Directive and the Database Directive), where specific copyright exceptions were upgraded to lawful users' rights. The same logic lies behind the portability exception, which is transformed to a lawful subscriber's right. The portability right overrides any contractual provision including those between holders of copyright and related rights, those holding any other rights relevant for the use of content in online content services and service providers, as well as between service providers and subscribers. Furthermore, the portability right is given a fully retroactive effect. According to Article 9, "*This Regulation shall apply also to contracts concluded and rights acquired before the date of its application if they are relevant for the provision, the access to and the use of an online content service in accordance with Articles 3 and 6 after that date*".

While those provisions significantly reinforce the portability right and act in favour of the subscriber (lawful user), questions might be raised because the fierce interference of those provisions with the private will of the contractual parties, as this has been expressed in the contract. The Regulation aims to invalidate every contractual clause that grants a territorial exclusivity for service providers or a subscriber's right to use an online content service solely in the territory of a given Member State. Those contractual restrictions correspond to the established practice of territorial licensing of copyright and related rights.

From a consumer point of view, the invalidation of those provisions is necessary for the effective enjoyment of portability. Nonetheless, copyright and intellectual property rights, including contractual rights arising from the exploitation of

[109]See Recital 31 of the proposed Regulation. See also: Gaubiac and Gotzen (2015).

[110]Expressions of that principle are Articles 14(2) and 14 (4) of the Database Directive. According to those provisions "2. Notwithstanding paragraph 1, where a database protected under copyright arrangements in a Member State on the date of publication of this Directive does not fulfil the eligibility criteria for copyright protection laid down in Article 3 (1), this Directive shall not result in any curtailing in that Member State of the remaining term of protection afforded under those arrangements." and "The protection provided for in paragraphs 1 and 3 shall be without prejudice to any acts concluded and rights acquired before the date referred to in those paragraphs.". See also Article 13(6) of the Rental and Lending Directive 93/98/EEC (now Article 11(5) of Directive 2006/115/EC- codified version of 12 December 2006). For the interpretation of those provisions see: von Lewinski (2010).

intellectual property rights, are protected as "possessions" by the First additional protocol of the ECHR and by Article 17 of the EU Charter of Fundamental Rights. Thus, every interference must be prescribed by law, be in the public interest, and shall be necessary in a democratic society. In this balancing exercise, as Griffiths notes, "*in its assessment of proportionality, the European Court of Human Rights has typically accorded national decision-makers a broader margin of appreciation under Art 1, Protocol 1 than has generally been permitted in the case of other qualified rights under the Convention*".[111]

Indeed, the protection of copyright law as a part of property rights stands as a guideline and a constraint that the EU legislator shall consider each time he or she intervenes in that field or makes a law that affects copyright law.[112] In this context, even though legislation which restricts existing rights would not necessarily be inconsistent with Art.1 of the First Protocol to the ECHR or Art.17 of the Charter of Fundamental Rights of the EU, the legislative copyright harmonisation measures taken as far as now have been careful to preserve existing rights, even where the underlying basis of protection has been restricted in scope for the future.[113] The ECHR's standing in Dima v Romania could be a basis for a reserved and careful approach as regards a new law with a retroactive application interfering with an existing possession. Indeed, the ECHR's authority that copyright protection exists from the moment an author creates a work could act in favour of authors and rightholders who challenge a change in applicable law.[114] As Helfer notes, "*this concern extends not only to interactions between the state and rightholders, but also to disputes between private parties*".[115] It has to be explored whether the balance between copyright protection and the public interest will be considered a fair one, as regards the retroactive effect of the proposed Regulation on established property rights. Indeed, as the proposed Regulation interferes with existing possessions, the compatibility of such an interference with the protection of property will be affirmed only if the Regulation's provisions are found to strike a fair and proportional balance between copyright law and the public interest.

Copyright law and related rights are protected as "intellectual property", thus a special kind of "property" according to Article 17 of the Charter of Fundamental Rights. As it has been pinpointed by the CJEU in the Scarlet case, "*The protection of the right to intellectual property is indeed enshrined in Art. 17(2) of the Charter. . .There is, however, nothing whatsoever in the wording of that provision or in the Court's case-law to suggest that that right is inviolable and must for that reason be absolutely protected*".[116]

[111] Griffiths (2013a).

[112] Georgopoulos (2012).

[113] Derclaye and Cook (2011).

[114] Helfer (2008).

[115] Helfer, op,cit., p 71.

[116] Scarlet Extended SA v SABAM (Case C-70/10) [2012] E.C.D.R. 4, par. 43.

So, while in principle it is possible to restrict existing copyright prerogatives, a thorough and detailed analysis of the fair balancing process under the light of the ECHR's case law shall be made to ascertain whether the specific interference is a justified and proportionate restriction. In this context, it has first to be explored whether the interference on copyright and related rights brought by the portability right is a deprivation of "property" or another kind of interference, such as a control of use. The difference is crucial because a total deprivation of property should be normally compensated,[117] while "*the use of property may be regulated by law in so far as is necessary for the general interest*". In this context, "*lesser interferences such as the dispossession of individual rights within the overall bundle have been tended to be viewed as controls of use and therefore not to give rise to a presumed entitlement of compensation*".[118]

The Digital Single Market strategy wants to allow better access for consumers and business to online goods and services across Europe. Thus, in the Commission's Digital Single Market strategy the free movement of goods and services in EU as seen as a pillar for enhancing consumer interests in the EU. Indeed, the internal market freedoms have a twofold relationship with consumer protection. Consumer interests coupled with the principle of human dignity may help to justify an exception to the free movement of goods and services.[119] On the other hand, the economic freedoms and the free completion can also act as a pillar for strengthening consumer protection. Article 169 TFEU provides that "*In order to promote the interests of consumers and to ensure a high level of consumer protection, the Union shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests*".

Article 38 of the Charter recognises consumer protection as a legal principle[120] of EU law. According to this provision, "*Union policies shall ensure a high level of consumer protection*". As Benohr notes, the recognition of the Charter by the Lisbon Treaty can enhance consumer protection. In this context, contractual relations between private parties might be affected and "*A contract can be tested through a fundamental rights review of EU legislation or national laws adopted to implement directives. Such a contractual review may challenge the validity of certain contractual terms and strengthen the position of the consumer as the weaker contractual party*".[121]

---

[117] Article 17 par. 1 of the Charter: ". . .No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest." See also: Griffiths and McDonagh (2013).

[118] Griffiths (2013b), op.cit.

[119] Benohr (2013).

[120] Benohr (2013), op.cit., p 64.

[121] Benohr, op.cit., p 67.

Under the light of the above, there is not a clear and straightforward principle that prohibits the interference of the proposed Regulation's provisions with established copyright and related rights, while, on the other hand, it is also possible that consumer interests will prevail even against the expressed contractual will of the parties in consumer contracts. As the legal fiction of Article 4 does not interfere with the whole bundle of economic and moral prerogatives which constitute the core of the protection awarded by copyright law, but only with a specific economic prerogative (the right to communication to the public, including the making available right), it is much probable that the interference will be considered as a control of use of property and not as a deprivation of property. Therefore, prima facie the imposition of compensation does not seem necessary. On the other hand, as the portability exception must be compatible with the three-step test, which has been interpreted as far as now with economy oriented criteria, such an obligation cannot be absolutely excluded, especially if the scope of application of the privilege of portability is found as not strictly defined.

4 Concluding Remarks

An examination of the impact of the two EU portability formulas on copyright law logically raises the question of the emergence of a common core of the concept of portability in EU Internet law. The concept of portability is a transplant from technology into the law; consequently, any technical meaning does not necessarily correspond to a legal one.

While in technological terms portability is often described as software portability,[122] (the possibility to transfer software and to make it work on multiple platforms, or more generally from one computer environment to another), the two EU portability formulas that have been analysed cannot be fully identified with this definition. Indeed, the new data portability right is related to the flexibility and the ability to use and migrate data, and is intrinsically dependent on the data's format. In this context, portability is in substance essentially a question of interoperability. The proposed Regulation's portability mechanism is generally seen also as a question of transfer (migration) to another "environment". Nonetheless, this "environment" is not geographically or technically defined. Thus, portability focuses on the issue of the accessibility of an online service, regardless of certain territorial restraints on use, the basis of which is legal and not technical. Here, copyright territoriality appears to be the main legal restraint, and consequently, the scrutiny of the proposed mechanism under the established principles of copyright law is direct and more profound.

Despite the significant divergences between the two EU portability mechanisms, both instruments express a definite will to introduce more flexibility in relation to

[122] See: https://www.techopedia.com/definition/8921/portability.

the use of data, services and applications into what could, broadly and somehow arbitrarily, be described as an EU online sphere. This flexibility is essential for the fulfilment of EU law goals, and it is ultimately linked to the internal market ideal of the unhampered smooth flow of services within the EU for the benefit of competitors and consumers. In light of the above, the nascent EU legal portability concept is quite vague, though not devoid of meaning. It could be generally described as the lawful privilege of someone (either a data subject or a consumer-subscriber) to carry, access and enjoy data, a benefit, an interest, or aright from one online environment to another. Even though the EU legislator's purpose has been to add to the free movement of services, persons and goods a new EU "pillar", which might be termed "the free movement of data", the reality of this is far from achieving its objective, with copyright law acting as a protagonist or even a catalyst in this process.

In relation to copyright law, the emergence of portability necessarily results in a delicate calibration of fundamental rights. This difficult task has led to compromises, which raise significant interpretative conundrums and empty or weaken the EU portability formulas. Consequently, and quite disappointingly, the analysis of the specific features of the two mechanisms has shown that both are somewhat incomplete. Even though the nature of the two portability privileges differs *ab initio* (a data subject's right or a hybrid legal creature having the features both of a copyright exception and of a consumer right), the elusiveness and deficiencies in their enforcement mean that the emergent EU portability norm is a work in progress rather than a solid and effective regulatory solution.

References

Batchelor B (2016) Commission Publishes First Issues Paper into EU Geo-blocking. Available: http://kluwercompetitionlawblog.com/2016/03/25/commission-publishes-first-issues-paper-eu-geo-blocking/

Benohr I (2013) EU consumer law and human rights. Oxford Studies in European Law, p 67

Bernault C (2012) Interoperability and European copyright law codification. In: Synodinou T (ed) Codification of European copyright law, challenges and perspectives. Kluwer Law International, p 316

Beutler S (1996) The protection of multimedia products through the European community's directive on the legal protection of databases. Entertain Law Rev 8:324

Bilon JL (1993) L'unité juridique des systèmes de l'information. In : Mélanges offerts à André Colomer. Litec, p 48

Cahen M (2012) Les réseaux sociaux de photos et le droit d'auteur. Available: http://www.murielle-cahen.com/publications/photo-reseau-social.asp

Cohen J (2005) The place of the user in copyright law. Fordham Law Rev 74:347

Commission (2009) Creative Content in a European Digital Single Market: Challenges for the Future, A Reflection Document of DG INFSO and DG MARKT, 22 October 2009 p. 19

Commission (2015a) Impact Assessment Accompanying the Proposal for a Regulation to Ensure the Cross-Border Portability of Online Content Services in the Internal Market, SWD(2015) 270, p. 24

Commission (2015b) Towards a modern, more European copyright framework, Brussels, 9.12.2015, COM(2015) 626 final
Commission Staff Working Document (2015) A Digital Single Market Strategy for Europe - Analysis and Evidence, Brussels, 6.5.2015, SWD (2015) 100 final
Commission Staff Working Document (2016) Geo-blocking practices in e-commerce, Issues paper presenting initial findings of the e-commerce sector inquiry conducted by the Directorate-General for Competition, Brussels, 18.3.2016, SWD(2016) 70 final
De Werra J (2012) An essential brick in the building of European copyright: regulation of copyright transactions. In: Synodinou T (ed) Codification of European copyright law, challenges and perspectives, Kluwer Law International, p 266
Derclaye E, Cook T (2011) An EU Copyright Code: what and how, if ever? Intell Prop Q 3:259–269, at 262. Available: http://eprints.nottingham.ac.uk/1739/1/cook_derclaye_2011.pdf
Dusollier S (2005) Droit d'auteur et protection des œuvres dans l'univers numérique, Droits et exceptions à la lumière des dispositifs de verrouillage des œuvres. Larcier, Bruxelles, p 503
Engels B (2016) Data portability among online platforms. Internet Policy Rev 5(2), doi:10.14763/2016.2.408
European Commission (2014) White Paper - A Copyright Policy for Creativity and Innovation in the European Union, Brussels. Available: http://online.wsj.com/public/resources/documents/EUFRANCES.pdf
European Commission (2015) Fact Sheet, Roaming charges and open Internet: questions and answers, Brussels, 30 June 2015. Available: http://europa.eu/rapid/press-release_MEMO-15-5275_el.htm
European Parliament (2017a) Legislative resolution of 18 May 2017 on the proposal for a regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market (COM(2015)0627 – C80392/2015 – 2015/0284(COD), P8_TA-PROV(2017)0224
European Parliament (2017b) Watching online films and TV while abroad, Press Release, 18 May 2017. Available: http://www.europarl.europa.eu/news/en/press-room/20170509IPR73935/watching-online-films-and-tv-while-abroad
Farrand B (2016) The EU portability regulation: one small step for cross-border access, one giant leap for Commission copyright policy?. Eur Intell Porp Rev 38(6):321–325
Fialova E (2014) Data portability and informational self-determination. Masaryk Univ J Law Technol 8:45
Gaubiac Y, Gotzen F (2015) Première évaluation de la méthode adoptée par la Commission dans ses propositions du 9 décembre 2015 sur la modernisation du droit d'auteur dans un marché unique numérique connecté. Available: http://www.fondation-droitcontinental.org
Georgopoulos Th (2012) The legal foundations of European copyright law. In: Synodinou T (ed) Codification of European copyright law. Kluwer Law International, p 40
Griffiths J, McDonagh L (2013) Fundamental rights and European IP law: the case of Article 17 (2) of the EU Charter. In: Geiger C (ed) Constructing European intellectual property, achievements and new perspectives. Edward Elgar, Cheltenham, Northampton, p 90
Griffiths J (2013a) Constitutionalising or harmonising? – the Court of Justice, the right to property and European copyright law. Eur Law Rev 38:65–78
Griffiths McD (2013b) Fundamental Rights and European IP law: the case of Article 17 (2) of the EU Charter, op.cit., p 81
Grondin A (2013) Réseaux sociaux et photos: Quels sont vos droits?. Available:http://www.20minutes.fr/web/1089701-20130129-reseaux-sociaux-photos-droits (First published on 29.01.2013)
Guibault L (2002) Copyright limitations and contracts, an analysis of the contractual overridability of limitations to copyright. Kluwer Law International, p 219
Helberger N (2007) Refusal to Serve Consumers because of their Nationality or Residence - Distortions in the Internal Market for E-commerce Transactions? Briefing Note (IP/A/IMCO/

IC/2006-207), EU Parliament, DG Internal Policies of the Union, Policy Department Economic and Scientific Policy. Available: http://www.ivir.nl/publicaties/download/244
Helfer L (2008) The new innovation frontier? Intellectual property and the European court of human rights. In: Torremans P (ed) Intellectual property and human rights. Wolters Kluwer, Law & Business, p 43
Hilty R (2012) Reflections on a European copyright codification. In: Synodinou T (ed) op.cit., p 358
Hugenholtz PB (2013) Is harmonizing a good thing? The case of copyright acquis. In: Pila J, Ohly A (eds) The Europeanisation of intellectual property law: towards a European legal methodology. pOUP, pp 69–70
Hugenholtz PB, van Eechoud M, van Gombel S, Guibault L et al (2006) Report on "The Recasting of Copyright & Related Rights for the Knowledge Economy", Institute for Information Law, November 2006, Study commissioned by the European Commission's Internal Market Directorate General, p 23
Jougleux Ph (2012) The plurality of legal systems in copyright law: an obstacle to a European codification?. In Synodinou T (ed) Codification of European copyright law: challenges and perspectives. Kluwer Law International p 62
Kaye D (2015) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015. Available at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx
Klawansky R. Photographers' rights to their photos posted on Twitter and twitpics. Available: http://www.artslaw.com.au/articles/entry/photographers-rights-to-their-photos-posted-on-twitter-and-twitpics/
Koelman KJ (2006) An exceptio standardis: do we need an IP exemption for standards? IIC 37 (7):823–843
Lucas A, Lucas HJ, Lucas-Schloetter A (2012), Traité de la propriété littéraire et artistique, 4th edn. Lexis Nexis, Litec p 331, n°349
Madiega T (2015) EU copyright reform: Revisiting the principle of territoriality, European Parliamentary Research Service, Briefing. Available: http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568348/EPRS_BRI(2015)568348_EN.pdf
Orientation Debate on Content in the Digital Economy, SEC (2012) 680, Brussels, 28 November 2012: p 4
Proposal for a Regulation of the European Parliament and of the Council on ensuring the cross-border portability of online content services in the internal market, Brussels, 9.12.2015COM (2015) 627 final
Peukert A (2012) Territoriality and extra-territoriality in intellectual property law. In: Handl G, Zekoll J, Zumbansen P (eds) Beyond territoriality: transnational legal authority in an age of globalisation. Martinus Nijhoff, Leiden, Boston, pp 190–192
Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil visant à assurer la portabilité transfrontière des services de contenu en ligne dans le marché intérieur (COM(2015)0627 – C8-0392/2015 – 2015/0284(COD)), Commission des affaires juridiques, 21.6.2016
Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes (COM/2016/0594 final - 2016/0284 (COD))
Reda J (2015) Report on the implementation of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (2014/2256(INI)), 24 June 2015, Committee on Legal Affairs
Report of the Panel, WTO Document WT/DS 160/R, 15 June 2000. Available at www.wto.org
Simon HA (1974) La science des systèmes, Science de l'artificiel. EPI, Paris

Sluijs J, Larouche P, Saute W (2012) Cloud Computing in the EU Policy Sphere, Interoperability, Vertical Integration and the Internal Market, JIPITEC (12). Available: https://www.jipitec.eu/issues/jipitec-3-1-2012/3320/sluijs.pdf

Strowel A (1993) Droit d'auteur et copyright, Divergences et convergences, Etude de droit comparé. Bruylant, Bruxelles, L.G.D.J. Paris pp 20–21

Swire P, Lagos Y (2013) Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique. Maryl Law Rev 72(2):338

Synodinou T (2010) The lawful user and a balancing of interests in European copyright law. IIC 7:81

Synodinou T (2014) Image right and copyright law in Europe: divergences and convergences. Laws 3:181–207

Synodinou T (2016) EU Portability Regulation: in-depth analysis of the Proposal. In depth analysis for the JURI Committee of the EU Parliament. Available at: http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/571369/IPOL_IDA(2016)571369_EN.pdf

Von Lewinski S (2010) Commentary of Article 13 of the Rental and Lending Rights Directive and Commentary of Article 14 of the Database Directive. In: Walter M, von Lewinski S (eds) European copyright law, a commentary. OUP, p 344 et seq., p 788 et seq

Weinberger D (2016) How the father of the World Wide Web plans to reclaim it t from Facebook and Google. Available: http://www.digitaltrends.com/web/ways-to-decentralize-the-web/ (published on August 10, 2016)

Westkamp G (2007) The Implementation of Directive 2001/29/EC in the Member States, p 67. Available at: http://ec.europa.eu/internal_market/copyright/docs/studies/infosoc-study-annex_en.pdf

Chapter 11
The Role of Internet Intermediaries in Copyright Law Online Enforcement

Philippe Jougleux

Abstract This chapter discusses the importance of copyright law enforcement as a prerequisite for the emergence of a digital single market. It firstly analyzes the reasons for the current crisis in copyright law enforcement and focuses on the role of Internet intermediaries in this context. The question is examined of whether the Internet intermediary's liability should have been abandoned 15 years ago with the enactment of the E-commerce Directive, whereby the intermediaries' safe harbor was established. However, this chapter shows that the law itself, together with an audacious jurisprudential interpretation, leads in practice to the application of a fault-based approach to Internet intermediaries' liability. As this evolution is obviously not sufficient to resolve the issue of online enforcement of copyright law, this analysis is supplemented by the emerging topic of gag orders. This method, combined with the trends in case law related to pan-European judicial orders, despite being incomplete, nowadays offers the most promising solution towards effective copyright law enforcement.

1 Introduction

With 40% of the world population[1] as their potential clients, e-commerce websites are expanding quite rapidly but with two main obstacles: the costs of physical transportation of goods and various legal obstacles to cross border transactions. In this context, the market for intangible goods does not have any transportation costs and benefits from a high level of harmonization worldwide, and should therefore have been particularly prosperous. Intangible assets undeniably constitute a new source of growth for modern economies.[2] However, the impact of parallel, shadow

[1] 2015's statistics, http://www.internetlivestats.com/Internet-users/.

[2] OECD (2012).

P. Jougleux (✉)
School of Law, European University Cyprus, 6, Diogenis Str., Engomi, P.O. Box 22006, 1516 Nicosia, Cyprus
e-mail: p.jougleux@euc.ac.cy

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_11

economies involving the free sharing of goods should not be underestimated as a substantial factor impeding economic growth. The issue of copyright law online enforcement made its appearance today when the Internet started to become popular, and after 20 years of discussions, no results have yet been found to provide a secure legal framework for e-commerce in intangible goods.

The European Commission has clearly defined the "digital single market" as one of its priorities and based its strategy on three "pillars": better online access to digital goods and services, digital as a driver for growth and an environment where digital networks and services can prosper.[3] The last pillar explicitly mentions the objective of "combatting illegal content on the Internet", with emphasis on the ambiguous role of Internet intermediaries.[4] Indeed, although Internet intermediaries are, as a point of principle, protected against liability by a safe harbor, it is nowadays established that Internet intermediaries have a substantial role to play in copyright law online enforcement.[5]

In this chapter, this specific issue will be examined with emphasis on the idea that, although the safe harbor is justified in theory, a solution has to be found regarding the danger of a denial of justice related to the lack of copyright law enforcement on the Internet. In the first section, the various solutions proposed for the lack of law enforcement online will be analyzed (Sect. 2). The discussion will demonstrate the very audacious way in which the Court of Justice of the European Union (hereinafter the "CJEU") undermined Internet intermediaries' safe harbor and based its logic on a fault-based approach (Sect. 3). Nonetheless, despite this finding, the extent of an Internet Service Provider (hereinafter "ISP")'s liability remains narrow. In this context, the third section of this chapter will be dedicated to pan-European injunctions, as a new form—which is growing, but is also controversial—of law enforcement on the Internet (Sect. 4).

[3]Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the regions (2015).

[4]The communication states that "The principle, enshrined in the e-Commerce Directive, that Internet intermediary service providers should not be liable for the content that they transmit, store or host, as long as they act in a strictly passive manner has underpinned the development of the Internet in Europe. At the same time when illegal content is identified, whether it be information related to illegal activities such as terrorism/child pornography or information that infringes the property rights of others (e.g. copyright), intermediaries should take effective action to remove it. Today the disabling of access to and the removal of illegal content by providers of hosting services can be slow and complicated, while content that is actually legal can be taken down erroneously. 52.7% of stakeholders say that action against illegal content is often ineffective and lacks transparency. Differences in national practices can impede enforcement (with a detrimental effect on the fight against online crime) and undermine confidence in the online world. As the amount of digital content available on the Internet grows, current arrangements are likely to be increasingly tested. It is not always easy to define the limits on what intermediaries can do with the content that they transmit, store or host before losing the possibility to benefit from the exemptions from liability set out in the e-Commerce Directive."

[5]Parti and Marin (2013).

2 Copyright Law Enforcement Online in General

Three different actors are, by definition, involved in copyright law enforcement: the Internet user, the Intermediary and the State. The Internet user would naturally be the first choice of enforcement in the analogue world, based on the general principle of personal liability in civil law. However, in the cyber environment, this idea seems impossible to implement in concrete terms. A European survey in 2015 showed that Internet users "*are most likely to have paid (either by subscription or per item) to access or download e-books (46%), followed by video games (34%), audio-visual content (30%), music (29%), and sports (19%)*".[6] By contrast, it can be reasonably assumed that a substantial proportion of free access online content constituted an infringement of copyright laws. Therefore, both technically and practically, the prosecution of a large proportion of the population is not a realistic strategy. Not only would it have an impossible political cost, as such enforcement measures would be highly unpopular, but also the legal system would not withstand the practical burden of massive prosecutions.

At the same time, substantial legal obstacles block the path of every attempt at enforcement against Internet users, as the main digital trace of illegal access, i.e. the IP address, is protected mainly as personal data but also by the principle of privacy of communications. Indeed, the Directive on Privacy and Electronic Communications[7] explicitly states that traffic data is included in the principle of confidentiality of communication.[8] Similarly, Article 29 (Data Protection Working Party) has on multiple occasions[9] highlighted the potential application of personal data protection to the IP address. In concrete terms, although it is technically possible to collect, for instance, the IP address of all users who download illegal content via peer-to-peer networks, the legality of this practice is subject to all the provisions of Personal Data Regulation.[10] This was explicitly confirmed recently in the landmark Patrick Breyer decision,[11] in which the court found that the IP address collected by the

[6]TNS Political & Social (2015).

[7]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[8]Article 5 (1) states that "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality."

[9]Article 29 Data Protection Working Party (2008).

[10]General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

[11]CJEU, *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, Judgement of 19 October 2016.

website's owner is an item of personal data in its own right, as via legal means (a judicial injunction served on the ISP) the Internet service provider is able to determine the identity of the IP address user.

However, the strict application of the protection of personal data would deprive the rightholder of a concrete means of enforcing his rights and could *de facto* lead to a denial of justice, which means a violation of Article 6 of the European Convention on Human Rights (hereinafter "the ECHR"). At this stage, it could be interesting to focus on a State's involvement in copyright law online enforcement. For instance, in the ECHR's case *K.U v Finland*,[12] a picture of a 12 year-old child was uploaded by an anonymous user on a pedophile website. The national legal framework prohibited the police from requesting the real identity of the user. For the European Court of Human Rights however, the protection of the child had to be expressed in terms of concrete actions and the authorities' inaction was deemed to constitute a violation of Article 6 on free access to justice. Nonetheless, although States have a responsibility to ensure a safer Internet, this would not apply to every violation of rights on the Internet on a daily basis for practical reasons. The CJEU also had an opportunity to discuss this question in the cases of *Promusicae,*[13] *Scarlet v. Sabam*[14] and *Netlog*.[15] The European Court has left the task of a concrete calibration of the interests at stake to the discretion of the Member States, making it clear that the protection of the fundamental right to property, which includes rights linked to intellectual property, must be balanced against the protection of other fundamental rights.[16] These other legitimate interests include the user's right to privacy[17] and the intermediary's freedom to conduct business.[18]

Consequently, Parliament is focusing, logically, on Internet intermediaries as its last possible solution. Internet Intermediaries procure the technical means for infringement, extract a profit from it, through increased traffic, and have, at last, the technical means to control content. On the other hand, the involvement of Internet intermediaries in copyright law enforcement entails the risk of creating a disproportionate economic burden, and therefore of endangering the dynamism of e-commerce. From a first wave of uncertainty based on the false assumption that the Internet is a "no man's land", a general rule of non-liability of intermediaries came into being, applicable to both ISPs and OSPs (online service providers). The intermediaries' safe harbor is justified by the idea that the burden of control should not be borne by the private sector, which should remain dynamic and as unregulated

[12]ECHR, K. U. v. Finland (Requête n° 2872/02), 2/12/2008.

[13]ECJ, *Promusicae* Case C-275/06, Judgment of the Court (Grand Chamber) of 29 January 2008 ECR I-271.

[14]CJEU, *Scarlet v. Sabam*, case C-70/10, Judgement of 24 November 2011.

[15]CJEU, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, case C-360/10, Judgement of 16 February 2012.

[16]Paragraphs 62 to 68 of the judgment in Case C-275/06 Promusicae.

[17]See par. 50 of the judgment in Case Scarlet v. Sabam.

[18]See par. 46 of the judgment in Case Scarlet v. Sabam.

as possible. This type of legal protection was first created in the USA,[19] but it was also adopted at European Union level with the famous E-commerce Directive in 2001.[20] However, while the Americans preferred a sectorial approach, with a limited safe harbor only for copyright issues, the European Parliament extended the safe harbor to every issue of civil law, such as defamation or privacy.

3 Internet Intermediaries' Liability: A Dead End or an Optical Illusion?

It seems clear at first sight that the E-commerce Directive aims to protect Internet intermediaries from liability and offers, in this context, a "safe harbor". However, the content of the relevant provisions itself (A) as its jurisprudential application (B) shows that the practical extent of this safe harbor is much more limited than expected.

3.1 The E-commerce Directive: Fifteen Years of Application

Three different kinds of activities are defined by the European Parliament in the E-Commerce Directive: mere conduit, caching and hosting. If the intermediaries only facilitate the communication (mere conduit) without intervention or just store the information temporarily for the sole purpose of facilitating the information's onward transmission to other recipients of the service upon their request (caching), the safe harbor acts essentially as an absolute asylum with very limited exceptions.

The third category of intermediary services, defined as "hosting", constitutes in practice the heart of the safe harbor mechanism. Indeed, in the era of social networks, which is sometimes called the Web 2.0 era, content hosted on a digital platform that is independent from the user cannot be compared, in terms of both quantity and quality, with information traditionally provided by a user on a personal platform, such as a personal website. Therefore, hosting services encompass a significant proportion of current activities on the Web, such as sharing videos, pictures, small texts (tweets), ideas and souvenirs, commenting on journalistic articles, personal blogs, rating hotels and restaurant services, contributing to encyclopedias and other collective works, trading in goods and services, or even developing new romances.

[19]See section 230 of the Communications Decency Act and section 512 of the Digital Millennium Copyright Act.

[20]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

The principle of non-liability of the host provider for hosted content recognizes more exceptions than in the case of mere conduit and caching. The host provider can seek the protection of the safe harbor only provided that: (a) he does not have any actual knowledge of the illegal activity or information and, regarding claims for damages, he is not aware of the facts or circumstances from which the illegal activity or information is apparent; or (b) upon obtaining such knowledge or awareness, he acts expeditiously to remove or to disable access to the information.

Simply put, the E-Commerce Directive imposes a "notice and take down" procedure as a mandatory component of the safe harbor mechanism, with emphasis on the development of self-regulation measures.[21] Upon notification of the existence of illegal content on its server, the intermediary's failure to fully block access to the content renders it liable, as has been ruled for instance in Germany.[22] The 'notice and take down' procedure has sometimes been inserted in national legislation, in combination with a counter-notice and put-back option, which means that the plaintiff must provide a legal basis for his claim in due time, otherwise, in the event of a counter-notice from the user, the content could automatically be posted back online.[23]

The lack of precision regarding the practical aspects of the procedure is often subject to criticism[24] and the European Commission, which is well aware of this flaw, has been working on the preparation of a more detailed procedure, to regulate the position and type of a complaint button and the maximum period allowed for an answer. A public consultation held in 2012[25] showed that society regards the procedure mainly as ineffective. However, the consultation has not thus far led to any concrete measures. One of the reasons for this lack of effectiveness could be the rejection of the "take down, stay down" theory by the courts. This theory aimed to demonstrate that the 'take down' notice logically creates a duty for the intermediary to act appropriately to prevent further illegal uploads from the same user. However, ordering ISPs to block all future attempts to upload illegal content without further notice would in concrete terms mean that the rightholder is in effect forcing ISPs to filter all content as a matter of routine, which is clearly at odds with the E-Commerce Directive's provision concerning the interdiction on imposing a general surveillance duty.[26] Consequently, in France in 2012,[27] the Supreme Court definitively rejected the "take down, stay down rule" as a legal obligation incumbent on the intermediary.

[21] See article 16 and recital 40 of the Directive.

[22] Urteil des I. Zivilsenats vom 12 July 2012 - I ZR 18/11.

[23] Verbiest et al. (2007).

[24] Synodinou (2014).

[25] European Commission (2012).

[26] Article 15.

[27] France, Court of Cassation, *Google France v. Bac Films*, First civil chamber, decision of 12 July 2012. http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3461.

Other critics point out the dangers inherent in the 'notice and take down' procedure.[28] Media law is founded on the principle of analogy, because by definition, classifying a particular piece of content as illegal constitutes a violation of the freedom of expression. However, a judicial analysis is replaced here with a private form of justice, as the ISP has a responsibility to decide upon the legitimacy of the notice. The mechanism therefore produces some perverse results, as it is in the ISP's basic interest to comply with the notifications, even if they are exaggerated, to avoid losing its safe harbor. A famous example is the "dancing baby" case in USA, when Youtube deleted the video of a baby dancing for a half a minute to a song by Prince playing in the background, for reasons of copyright law infringement. The mother finally won her case against Google's Youtube service, as it was clearly a case of fair use. Interestingly, on appeal the Court noted that "*Copyright holders cannot shirk their duty to consider … whether allegedly infringing material constitutes fair use*".[29] Put simply, the burden of applying the appropriate safe harbor mechanism is placed not on the intermediary, but on the rightholder.

3.2 The Rise and Fall of the "Passive Role" Doctrine

The CJEU has gradually undermined the foundations of the safe harbor, adopting an audacious approach to the accountability of intermediaries. Primarily, it should be noted that the famous Google Spain[30] case concerning the right to be forgotten could be interpreted as a neutralization of the safe harbor mechanism as regards personal data protection. From one point of view, Google's search engine was acting as an intermediary in this case, by automatically listing the web's content. From another point of view, which is the one adopted by the European Court, the search engine directly processes personal data, and is therefore responsible for the correct application of the principles of protection of personal data.

The E-Commerce Directive's safe harbor principle has also been analyzed by the CJEU. Two landmark cases—Google France and Google v. Louis Vuitton[31] and L'Oréal SA and others v. eBay International AG and others[32]—have established the basic principles of interpretation of the safe harbor mechanism and have highlighted the need for the Internet intermediary to play a "passive role" Internet, as a fundamental prerequisite of the safe harbor's application. The passive role

[28] Akdeniz (2010).

[29] United States Court of Appeals for the Ninth Circuit, *Lenz v. Universal Music Corp*., 801 F.3d 1126 14 September 2015.

[30] CJEU, *Google Spain v AEPD and Mario Costeja Gonzalez*, case C-131/12, Judgment of the Court (Grand Chamber) of 13 May 2014.

[31] CJEU, *Google France and Google v. Louis Vuitton* case C-238/08, Judgment of the Court (Grand Chamber) of 23 March 2010.

[32] CJEU, *L'Oréal SA and others v. eBay International AG, and others*, case C-324/09, Judgment of the Court (Grand Chamber) of 12 July 2011.

could be summarized as the absence of a special relationship between the hosted content and the online service provider. Simply put, the court interprets the safe harbor in the sense that the intermediary avoids liability only if he can prove that he is not *actively* involved in the illegal activity, but is merely providing technical support (a passive contribution).

The "passive role" doctrine has the wherewithal to provide the national courts with a precise tool to analyze the behavior of the online service provider. However, this doctrine also leads to some strange consequences, described commonly as the "Good Samaritan syndrome".[33] Indeed, if the ISP maintains a neutral attitude towards its content, it will not have to fear prosecution. On the other hand, if it wants to act and takes some measures to control this, its action could be seen by the court as an intervention and it could lose the benefit of the safe harbor. For instance, in a Dutch case,[34] a file-sharing site (Mininova) was found guilty of copyright law infringement and the safe harbor protection mechanism did not apply. However, as the site did filter out pornography and viruses, it demonstrated that it exercised a degree of control over the content of the website, and therefore did not maintain a completely passive role. Therefore, it was not considered an intermediary within the meaning of the E-commerce Directive and it was held liable because of its lack of control over content that was illegal in terms of copyright law.

It seems that, in concrete terms, the passive role doctrine neutralizes the safe harbor as a philosophy, because ultimately, via evaluation of the awareness of the online service provider in practice, a fault-based approach is adopted. Put simply, as the company knew about the copyright law infringement and did not act promptly, it was liable for providing assistance with this illegal communication. A contributory liability for the infringement of copyright will depend more on the interpretation of the European "actual or presumed knowledge" criterion, than on national legal traditions. In Germany for instance, the concept of Störerhaftung (interferer liability) applied,[35] and the provider of an insecure WIFI network was not held liable. Although it was at fault, in the sense that it failed in its duty to secure its network, it did not have any actual knowledge of the misuse of its network by a third party in infringing copyright.[36]

Furthermore, it should be noted that the landmark decision in the *Svensson* case[37] concerning the legal nature of hyperlinks in the context of copyright law could be interpreted as a manifestation of the 'passive role' doctrine. Although this issue does not concern online service providers only, the issue is also strictly related to them as most intermediaries authorize hyperlinks. In the *Svensson* case, it has

[33]Bart Van der Sloot (2015).

[34]ECLI:NL:RBUTR:2009:BJ6008.

[35]BGH GRUR 2004, 860 – Internetauktion I; GRUR 2007, 708 – Internetauktion II; GRUR 2008, 702.

[36]BGH GRUR 2010, 633, 634 – Sommer unseres Lebens. See the analysis of Leistner (2014).

[37]CJUE, *Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd v Retriever Sverige AB*, case C-466/12, Judgment of the Court (Fourth Chamber) of 13 February 2014.

been held that linking to free accessible content is by definition not covered by the right of communication to the public, as the first act of uploading this content means that all Internet users already have full access to it. This creates a kind of *a priori* safe harbor: no liability can be established for copyright infringement via a hyperlink because there is no violation of copyright law in the first location. Simply put, the secondary liability of intermediaries cannot be established, as the primary liability of users is avoided in the first instance. However, the Svensson case left the issue of the legality of accessible content in the shadows. In the CJEU's case law on that matter (the *Bestwater* case[38] concerning a streaming activity), the court explains that only hyperlinks avoid being classed as an act of communication to the public only when the related content has been uploaded with the rightholders' authorization,[39] but at the same time avoided giving a clear answer regarding the main issue of the link to illegal content. The recent *GS Media* landmark case[40] clarifies the CJEU's position on this point and States that linking to unauthorized content does not constitute communication to the public, but only on the dual condition that the person who posts that link does not seek financial gain and acts without the knowledge that these works have been published illegally. We can therefore see that the notion of actual knowledge of illegality, which is a notion closest to the concept of fault in the conceptual framework of civil liability, is imposed both in the case of primary and secondary liability.

3.3 A Worldwide Shift Towards an Active-Preventative Approach, or a Return to a Fault-Based Approach?

As we have seen above, the 'passive role' approach already possessed in its core the potential to neutralize the safe harbor's provision. The current trend, sometimes described as a "shift towards an active-preventative approach",[41] should therefore be seen as a development of the passive role approach more than a radical shift in perspective. In both cases, the discussion contains the same implicit appeal to the

[38]CJUE, *BestWater International GmbH v Michael Mebes, Stefan Potsch*, case C-348/13, Order of the Court (Ninth Chamber) of 21 October 2014.

[39]At the par.18 of the decision it is possible to read that "En effet, dès lors que et tant que cette œuvre est librement disponible sur le site vers lequel pointe le lien Internet, il doit être considéré que, lorsque les titulaires du droit d'auteur ont autorisé cette communication, ceux-ci ont pris en compte l'ensemble des internautes comme public", which we can translate by "Indeed , as soon as this work is freely available on the site pointed by the hyperlink, it must be considered that , when the holders of the copyright authorized the communication, these have included the entire Internet as public".

[40]CJUE, *GS Media BV v Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker*, case C-160/15, Judgment of the Court (Second Chamber) of 8 September 2016.

[41]De Beer and Clemmer (2009).

classic rules of secondary liability. The purpose is to critically assert the involvement of the third party with the idea that a fault would mean liability. This evolution is caused mainly—but not only—by judicial activities, as we shall see.

First, it is worth referring to a recent development in the human rights field. To the general surprise of scholars, the European Court of Human Rights (hereinafter "ECrtHR") *Delfi v Estonia*[42] decision, whereby holding a journal liable for the existence of defamatory content on the comments of the articles was ruled not to be a violation of Article 10 of the Convention (freedom of expression), was recently confirmed by the Grand Chamber of the Court.[43] The line of thinking adopted by the courts in that case was that the online journal could not be unaware of the obvious potentiality of illegal content generated by the comments.[44] However, as explained in detail in a subsequent case with very similar facts,[45] the ECrtHR does not believe in general that the entire safe harbor concept is incompatible with human rights. On the other hand, it limits its jurisprudence to cases of online comments that clearly involve a violation of the law.

Furthermore, as has been emphasized in the past, the safe harbor works only in the event of ignorance of the illegal content, with two distinct possibilities: cases in which the existence of illegal content is obvious to the host provider, such as the example of Pirate Bay,[46] and cases in which the existence of illegal content is notified by the users themselves, via the 'notice and take down' procedure. Based on the above, it is worth examining whether this mechanism ultimately greatly differs from the general principle governing secondary liability in civil law. The

[42]ECHR, *Delfi v Estonia*, app no 64569/09, 10 October 2013.

[43]ECHR, *Delfi v Estonia*, app no 64569/09, 16 June 2015.

[44]"The Court notes that in the interested person's opinion, shared by the domestic courts, the prior automatic filtering and notice-and-take-down system used by the applicant company did not ensure sufficient protection for the rights of third persons. The domestic courts attached importance in this context to the fact that the publication of the news articles and making public the readers' comments on these articles was part of the applicant company's professional activity. It was interested in the number of readers as well as comments, on which its advertising revenue depended. The Court considers this argument pertinent in determining the proportionality of the interference with the applicant company's freedom of expression. It also finds that publishing defamatory comments on a large Internet news portal, as in the present case, implies a wide audience for the comments. The Court further notes that the applicant company—and not a person whose reputation could be at stake—was in a position to know about an article to be published, to predict the nature of the possible comments prompted by it and, above all, to take technical or manual measures to prevent defamatory statements from being made public. Indeed, the actual writers of comments could not modify or delete their comments once posted on the Delfi news portal—only the applicant company had the technical means to do this. Thus, the Court considers that the applicant company exercised a substantial degree of control over the comments published on its portal even though it did not make as much use as it could have done of the full extent of the control at its disposal".

[45]ECHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, app no. 22947/13, 2 February 2016.

[46]ECHR, *Fredrik Neij and Peter Sunde Kolmisoppi (Pirate Bay) v. Sweden*, app no 40397/12, 19 February 2013.

safe harbor normally applies only to civil cases but its general principle can be extended to encompass criminal cases too. In all cases, the obvious illegality of content neutralizes the safe harbor in practice. In this context, it has been asserted that the passive role doctrine has evolved from a purely reactive role to an "active-preventative" role.[47] For instance, both in the *TV Catchup* case[48] in the UK and the *Pirate Bay* case[49] in Sweden, the defendant merely offered links to illegal content. Although it could be seen as an intermediary, the courts ruled that the obvious illegality of the vast majority of the website's content could not be ignored.

This general trend towards a progressive neutralization of the safe harbor's original philosophy is also perceptible on the other side of the Atlantic. In a landmark ruling[50] in 2015, confirmed in 2016 by the Court of Appeal, the Federal Judge upheld a $25 million infringement penalty against Cox Communications. The Internet provider did not receive the safe harbor's protection as it was proven that it did not take sufficient measures to create and enforce an appropriate termination policy for repeat infringer customers. Put simply, the 'take down' mechanism in the event of a complaint no longer constitutes sufficient grounds for claiming immunity. By not taking active steps to tackle repeated violations of copyright law, Cox contributed to the infringement.

Likewise, it is worth mentioning that recently, a German court held a file-sharing host liable because not only it had failed to remove large numbers of illegal files, but also primarily, because of its design and application, it increased the likelihood of copyright infringement. In the court's view, pirate sites whose business models are based on copyright infringement should be made to pay damages if they do not prevent the uploading and distribution of copyright-protected material.[51]

The safe harbor's *coup de grace* seems to be on the way, as it was recently revealed on President Juncker's 2016 State of the Union address, that the Commission is actively preparing a new package of reforms of EU Copyright law.[52] Among other new modernization measures for Copyright law, the commission intends to introduce a new obligation for online service providers to seek, in good faith, to conclude agreements with rightholders regarding the use of their content, and to put in place appropriate and proportionate measures, in cooperation with rightholders, to avoid unauthorized content on their services. Specifically, Article 13 of the Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market[53] "creates an obligation on information society

[47]Mlynar (2014–2015).

[48]*ITV Broadcasting Limited and others v TV Catchup Limited and others* [2015] EWCA Civ 204.

[49]*Pirate Bay* (B 13301-06, 2009-04-17, STOCKHOLMS TINGSRÄTT).

[50]*BMG RIGHTS MANAGEMENT (US) LLC, and ROUND HILL MUSIC LP v.COX COMMUNICATIONS, INC., and COXCOM, LLC*, Civil No. 1:14-cv-1611,12 January 2015.

[51]LG München (21 O 6197/14), 10 August 2016.

[52]Commission's press release (2016).

[53]Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016)593.

service providers storing and giving access to large amounts of works and other subject-matter uploaded by their users to take appropriate and proportionate measures to ensure the functioning of agreements concluded with rightholders and to prevent the availability on their services of content identified by rightholders in cooperation with the service providers".[54]

Recital 39 of the Proposal provides a further explanation of this new mechanism as it refers to "content recognition technologies".[55] The Google solution of ID tagging for Youtube services is advanced as a model for the new policy of online enforcement. This system, known as "content ID", allows rightholders to identify and manage their content on YouTube. In concrete terms, it automatically analyzes the video's content and determines whether it is similar to another video, in which case the rightholder may choose to mute the music, block the video or monetize it by placing ads (the revenue will be shared with the video's uploader).[56] It is easy to understand why this approach has seduced the European Commission: as the rightholder obtains revenue from the online exploitation of the work, litigation is avoided and the content remains online. At the same time, if this idea comes to fruition (if it passes into law), it would clearly mean that the new active-preventative approach is sanctioned by the EU Parliament, with the consequence that the safe harbor mechanism would have lost much of its significance. Indeed, the general reporting mechanism is replaced by an automatic tagging system and liability would not be an issue of whether the reporting mechanism is in place or not but of whether the tagging system is sufficiently effective. While the Free Frontier foundation is alarmed by the impact of this measure on Internet freedom,[57] rightholders would have sound reasons to celebrate as it could greatly reduce some online copyright law infringement. However, the tagging system used by Google for its YouTube service was very expensive to produce and it remains to be determined whether this new obligation is proportionate in terms of the right to entrepreneurship. One solution would be to assert the online service provider's duty of content tagging in light of a concrete estimation of its available resources.

In conclusion, the online intermediaries' "willful blindness"[58] was justified at the time when the web 2.0 was still emerging and fragile, whereas nowadays, online

[54]Explanatory Memorandum of the proposal (2016), p. 10.

[55]The recital 39 states that "*Collaboration between information society service providers storing and providing access to the public to large amounts of copyright protected works or other subject-matter uploaded by their users and rightholders is essential for the functioning of technologies, such as content recognition technologies. In such cases, rightholders should provide the necessary data to allow the services to identify their content and the services should be transparent towards rightholders with regard to the deployed technologies, to allow the assessment of their appropriateness. The services should in particular provide rightholders with information on the type of technologies used, the way they are operated and their success rate for the recognition of rightholders' content. Those technologies should also allow rightholders to get information from the information society service providers on the use of their content covered by an agreement.*"

[56]Source: https://support.google.com/youtube/answer/2797370?hl=en.

[57]Malcom (2016).

[58]Friedmann (2014).

service providers have become the new backbone of the Internet. It would be naïve not to realize that this trend is linked to constant pressure from rightholders to establish a higher level of liability but at the same time, it does not mean they are wrong to defend their rights. However, this return to a fault-based approach only concerns online intermediaries as contributors to the act of infringement, which normally affects online service providers (OSP), while Internet service providers' (ISP) liability, at least in the EU, should remain minimal. On the other hand, the injunctions mechanism mainly applies to ISP and offers innovative solutions for combatting online infringement.

4 The Growing Role of Injunctions Against Internet Intermediaries in the Internet Regulation Ecosystem

We are now witnessing a vast shift in the nature of liability, away from liability to cover the damages caused and towards liability for stopping an activity. The main idea is that while illegal downloading, sharing and streaming cannot be stopped after the event, it could probably be prevented. As the intermediary is the legitimate destination of such an injunction (A), this new opportunity for copyright law online enforcement should be read in conjunction with the growing question of pan-European injunctions (B).

4.1 The Legitimacy of the Blocking Measures in Question

Certainly, injunctions are not a new kind of remedy in copyright law, even against intermediaries. According to Article 8 (3) of the InfoSoc Directive,[59] "*Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right*". What does the injunction mechanism have to offer in terms of the issue of Internet intermediaries' liability? The quite remarkable point is that the injunction works independently of the question of liability, and therefore the safe harbor is completely neutralized. Article 13 (2) of the E-Commerce Directive[60] clearly explains that injunctions can be granted independently of the safe harbor's protection, and this means that new kinds of solutions for online law

[59]Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

[60]The article 13 (2) states that the safe harbor "shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement."

enforcement are slowly emerging, focusing specifically on the ISP's contribution to the prevention of copyright law infringement.

In theory, rightholders could seek a wide range of injunctions against ISPs: temporarily or permanently disconnecting a user,[61] blocking access to a website, blocking a specific type of Internet use (p2p networks), preventing an illegal work of mind from circulating online or adopting a Graduated Response Scheme (like recently in Ireland[62]). However, the graduated response or "three strikes" system issue goes beyond the mere discussion of the issue of an injunction as it generally presupposes a new legislative framework. This solution is usually seen as rather complex and costly because it imposes a cost burden on the State and on ISPs.[63] At the same time, the Enforcement Directive[64] explicitly confirms that rightholders have the right to seek an injunction intended to prevent an imminent act of infringement, or to forbid the continuation of the alleged infringement.[65]

However, these injunctions might violate several principles of EU law, such as the freedom to conduct business, the general rule of Article 15 of the E-Commerce Directive, which forbids the Member States to impose a general duty of surveillance on ISPs, and obviously the freedom of expression. In the *Promusicae* case,[66] the CJEU ruled that, in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and protection of the fundamental rights of individuals who are affected by such measures. It is reasonable to assume that this, by definition, excludes measures such as the disconnection injunction or the network-blocking injunction that would disproportionately affect the right to information.

The CJEU highlighted the issue in the *Sabam v Scarlet*[67] decision, and decided that it would be incompatible with European law for a national court to order an injunction against an ISP forcing it to filter all communications passing through its servers for content that infringes copyright. General filtering systems, intended to protect copyright, challenge several fundamental rights protected under the Charter of Fundamental Rights of the European Union. The Court acknowledged that, firstly, it would affect Netlog's freedom to conduct its business, as it would require it to install a complicated, costly, permanent computer system at its own expense. Secondly, it would affect users' rights to the protection of their personal data as it would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network. Finally, such a system

[61]Husovec and Peguera (2014).

[62]Irish High Court, *Sony v UPC Communications Ireland Limited,* 27 March 2015.

[63]Iglezakis (2012).

[64]Directive 2004/48/EC on the Enforcement of Intellectual Property Rights.

[65]Article 9 and 11 of the Directive.

[66]CJUE, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, case C-275/06, Judgement of 29 January 2008.

[67]CJUE, *Sabam v Scarlet*, case C-70/10, Judgement of 24 November 2011.

would put at risk the freedom of information, i.e. the freedom to receive or impart information, as the system might not always be able to distinguish between unlawful content and lawful content, and might block lawful communications. By extension, injunctions against search engines aiming to block the association between a copyrighted content and a specific technology (for instance, a movie name associated with the word "torrent") do not strike a fair balance in the light of this jurisprudence. It has been for instance ruled in France that Google and Microsoft (Bing) could not be forced to instruct their search engines to remove all results involving the word "torrent" used in conjunction with the names of three French musicians.[68]

However, the general discussion of the issue of the injunction's legality against ISPs has not been entirely closed and here again the Court nuances its position on a landmark case and a turning point on this issue, the *Telekabel* case.[69] Whereas the Advocate General agreed on his conclusions that blocking orders could be valid, he ruled out the possibility of a general blocking order, explaining that such a court order must refer to specific blocking measures to be valid. However, the Court decided to follow the Advocate General only on the first point, and to the general surprise of all interested scholars, it was held that a general blocking order is compatible with EU law.

However, two conditions are explicitly provided by the Court for the injunction to be valid. The access provider can avoid sanctions for breach of injunction "*provided that (i) the measures taken do not unnecessarily deprive Internet users of the possibility of lawfully accessing the information available and (ii) that those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging Internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right*".[70]

These two conditions are vital.[71] The first one protects the ISP against general measures, which would have a disproportionate effect on the right to be informed, such as injunctions to block Google blogs or Youtube. The second condition relates to the effectiveness of the injunction. It indicates an in-depth understanding of the Internet's mechanisms, as it must be understood that communication of illegal content cannot in practice be absolutely controlled. Proxy servers, VPN (hereinafter "Virtual Private Network"), traffic data encryption and other manipulations can easily circumvent any effort to control the flow. However, the proposed definition of the effectiveness of the blocking measure is more realistic, although somehow

[68]TGI Paris, Ref, N° RG : 16/51682, Judgement of 8 July 2016.

[69]CJUE, *UPC Telekabel Wien v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, case C-314/12, Judgement of 27 March 2014.

[70]Par.63 of the Decision.

[71]Synodinou (2014) Intermediaries' liability for online copyright infringement in the EU: Evolutions and confusions, op.cit.

more cynical. More specifically, the Court requests the measure in practice not to block access to content, but only to make access to illegal content harder to discourage the average user. For instance, intensive use of proxy servers in illegally downloading protected works poses certain problems, such as risks to privacy (who controls the proxy and what data is collected?), Internet speed limitations and technical burdens (finding an available proxy). Assuming that the alternative legal market is simple, fast, practical (without geo-blocking limitations[72]) and cheap enough, a blocking injunction would add the necessary space for it to flourish.

The practical consequences of the *Telekabel* decision have already been analyzed in several national courts, with various results. In some cases, it seems that the logic followed by the European Court has not been convincing enough, as national courts strictly apply the two criteria proposed in this case and refuse, as a rule, to grant injunction orders against ISPs.[73] In some other instances, such as in Greece, the situation is even more confusing. Although in 2012 the First Instance Court of Athens accepted the legality of blocking injunctions,[74] in 2014[75] it overturned its previous decision. More interestingly, at present the 2014 decision appears to be binding because of the application of the *non bis in idem* rule.[76] However, in other cases, the courts have apprehended all the consequences of this new case law and have followed it, by granting, under certain conditions, blocking injunction orders against intermediaries, like in Germany.[77]

4.2 The Rise of Pan-European Injunctions

In isolation, the effectiveness of injunctions against ISPs could indeed be judged as insignificant. One of the limitations of this system lies in the territorial application of the injunction. In concrete terms, as has already been mentioned, a proxy from a neighboring country (to maintain an adequate Internet speed) would neutralize the injunction's effect. This situation would be radically different if the new possibilities offered by the Telekabel case were combined with the emerging legal mechanism of pan-European injunctions.

[72]The European Commission has made the geo-blocking ban a priority in the frame of its Single Digital Market strategy. See, 'A Digital Single Market Strategy for Europe', op.cit.

[73]District Court of Stockholm, *Universal Music, Sony Music, Warner Music, Nordisk Film and the Swedish Film Industry vs Bredbandsbolaget*, Judgement of 27 November 2015.

[74]District Court of Athens, 4658/2012.

[75]District Court of Athens, 13478/2014.

[76]District Court of Athens, 10452/2015.

[77]Bundesgerichtshof- I ZR 3/14 und I ZR 174/14, Nr. 194/2015, Judgement of 26 November 2015.

Pan-European injunctions are governed by Brussels Regulation No. 44/2001[78] (hereinafter "the Brussels Regulation", which gives measly margin of discretion to the national court on the matter of IP rights. The Regulation provides that the courts of the Member State where registration has taken place shall have exclusive jurisdiction for "*proceedings concerned with the registration or validity*" of such intellectual property rights.[79] However, this limitation does not affect the issue of preliminary injunctions. According to Article 31 of the Brussels Regulation, "*application may be made to the courts of a Member State for such provisional, including protective, measures as may be available under the law of that State, even if, under this Regulation, the courts of another Member State have [exclusive] jurisdiction as to the substance of the matter*".

In the past, one ECJ decision eliminated the possibility of pan-European injunctions as a means of IP enforcement. The CJEU decided first that "*The rule of exclusive jurisdiction laid down [by Article 22.4 of the Brussels Regulation] concerns all proceedings relating to the registration or validity of a patent, irrespective of whether the issue is raised by way of an action or a plea in objection*",[80] which means that no crossborder injunction is in fact possible. However, at the same time, the Roche v. Primus case[81] offered some grounds for a shift in interpretation, since the Court decided that "*Article 6(1) of the [Brussels Regulation] must be interpreted as meaning that it does not apply in European patent infringement proceedings involving a number of companies established in various Contracting States in respect of acts committed in one or more of those States even where those companies, which belong to the same group, may have acted in an identical or similar manner in accordance with a common policy elaborated by one of them*". Put simply, judgments may only be regarded as being at risk of being irreconcilable within the meaning of Article 6(1) if a divergence in the outcome of the dispute arises in the same situation of fact and law. The high level of interconnectivity among national legal frameworks in the fields of industrial property law has certainly played a substantial role in the spread of pan-European injunctions.[82]

However, the turning point in terms of case law came in the landmark *Solvay v. Honeywell Companies* decision,[83] where the European Court confirmed that national courts in Europe are not prevented by European legislation from granting pan-European preliminary injunctions. Therefore, crossborder injunctions may be granted in preliminary proceedings where the court does not make a final decision

[78]Brussels Regulation No44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[79]Article 22(4) of the Regulation.

[80]ECJ, *GAT v. LuK*, case C-4/03, Judgment of 13 July 2006.

[81]ECJ, *Roche v. Primus*, case, C-539/03, Judgment of 13 July 2006.

[82]Trimble (2009).

[83]CJEU, *Solvay v. Honeywell Companies*, case C-616/10, Judgement of 12 July 2012.

on the validity of the patent, insofar as the validity of the patent is not seriously challenged.

Even if a new era of crossborder injunctions has now commenced, strict control still applies. The CJEU made it very clear in its 2011 ruling in the *DHL v Chronopost* case[84] that a Europe-wide injunction should only be granted to ensure that the proprietor could protect his trademark, prohibiting only uses that affect or are liable to affect the functions of the trademark. Further, it should be noted that within the scope of the new European patent, which has a unitary effect, the Patent Court possesses the power to grant provisional and permanent injunctions enforceable in all the participating Member States where the European patent has a unitary effect.[85] The same applies to Community trademarks.

These developments have emerged in the domain of industrial property rights, but at the same time, nothing in this approach excludes by definition copyright law from the mechanism of crossborder injunctions. The steep level of harmonization of copyright law within the Union fosters the application of this method. For instance, the Software Protection Directive[86] provides the same level of protection for software within the EU. In this context, in Holland, in 2010 a court had the opportunity to grant a pan-European injunction[87] based on copyright law infringement of a software program. The same court confirmed its jurisprudence in 2013 with another injunction.[88] In the landmark *Painer* decision,[89] the CJEU had no difficulty in applying the rules of pan-European injunction in a Copyright case, ruling that the defendant was in the same situation in terms of law. More precisely, the Court stated that "*Article 6(1) of Regulation No 44/2001 must be interpreted as not precluding its application solely because actions against several defendants for substantially identical copyright infringements are brought on national legal grounds which vary according to the Member States concerned. It is for the referring court to assess, in the light of all the elements of the case, whether there is a risk of irreconcilable judgments if those actions were determined separately*".[90]

In practice, the various European Internet service providers should be seen as sharing the same situation in fact, as by definition, the injunction is related to an online infringement, resulting in an infringement of a global nature. In this context,

[84]CJEU, *DHL v Chronopost*, case , C-235/09, Judgement of 12 April 2011.

[85]The article 5 (1) of the Regulation 1257/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection states that "The European patent with unitary effect shall confer on its proprietor the right to prevent any third party from committing acts against which that patent provides protection throughout the territories of the participating Member States in which it has unitary effect, subject to applicable limitations."

[86]Directive 91/250/EEC, 2009/24/EC.

[87]Court of Appeal of The Hague, *Technip*, 20 September 2010, cited by De Brauw Blackstone Westbroek (2013).

[88]Court of Appeal of The Hague, *Bang & Olufsen v Loewe*, 21 January 2013.

[89]CJUE, *Eva-Maria Painer v Standard VerlagsGmbH and others*, case C-145/10, Order of the Court (Third Chamber) of 7 March 2013.

[90]Par.84 of the Judgment.

the planned abolition of roaming charges within the EU,[91] which is a precursor of a real single market for telecommunications, has the *de facto* effect of placing all European ISPs in a situation of competiveness.

5 Conclusions

A shift in approach regarding the role of Internet intermediaries in IP law enforcement is clearly apparent. The safe harbor has in part been neutralized, as its practical application implies providing proof of the intermediary's tortious participation in terms of awareness of the illegal content. At the same time, the 'notice and take down' procedure has evolved to the point where it plays the role of a private means of copyright law enforcement.

However, the multiple flaws of the take-down procedure show that the classic 'liability for damages' system, as a form of deterrence and control of societal behavior, is still paralyzed by the safe harbor mechanism. Therefore, a combination of two parallel evolutions might offer a (excessively?) powerful tool in the hands of rightholders. Blocking orders against intermediaries are nowadays accepted in the Union under certain conditions. Injunctions do not have to be limited to a specific geographical area, because in the event of similarity of law and of facts, the injunction can extend to other European countries. In practice, it seems that nobody has yet applied to combine these in a pan-European blocking injunction against an access provider.

However, it is our view that this is in theory possible, if the safeguards established by the *Telekabel* case are complied with. It is surely not alien to copyright law in general to rely on provisional measures as a primary enforcement remedy,[92] but the opportunity of pan-European injunctions against intermediaries poses new challenges. Nonetheless, it is accompanied by potential threats to fundamental rights, such as the right to defense and the right to be informed, which are clearly apparent in the CJEU's thinking. It is ultimately a matter of judgement to determine whether the creation and protection of a digital single market justify those risks.

More than 15 years ago, the concept of an intermediary was imposed to justify a general immunity for online professional services. We are now seeing that the situation of ISPs and OSPs varies widely and that they do not ontologically belong

[91]Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open Internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

[92]European observatory on counterfeiting and piracy (undated) Injunctions in Intellectual Property Rights. p. 4, available at http://ec.europa.eu/internal_market/iprenforcement/docs/injunctions_en.pdf.

in the same category. OSPs are gradually losing the safe harbor battle, through the enforcement of the new active-preventative approach and with the expected action of the EU Parliament, while ISPs need to be protected against this change. On the other hand, the highly effective but most dangerous method—which is the injunction—mainly concerns ISPs.

References

Akdeniz Y (2010) To block or not to block: European approaches to content regulation, and implications for freedom of expression. Comput Law Secur Rev 26(3):260–272

Article 29 Data Protection Working Party (2008) Opinion 1/2008 on data protection issues related to search engines, WP 148, p.6; (2002) Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, WP58, p 3

Commission's press release (2016) State of the Union 2016: Commission proposes modern EU copyright rules for European culture to flourish and circulate, IP/16/3010

Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the regions (2015) A Digital Single Market Strategy for Europe. SWD 100 final

De Beer J, Clemmer C (2009) Global trends in online copyright enforcement: a non-neutral role for network intermediaries? Jurimetrics 49(4):375–409. Retrieved from http://www.jstor.org/stable/29763019

De Brauw, Blackstone, Westbroek (2013) The Netherlands: the country of crossborder injunctions in IP. Intellectual Property newsletter, 11/02/2013

European Commission (2012) Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries. Available athttp://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internetInternet/summary-of-responses_en.pdf

Friedmann D (2014) Sinking the safe harbour with the legal certainty of strict liability in sight. J Intellect Prop Law Pract 9(2):148–155

Husovec M, Peguera M (2014) Much Ado about little – privately litigated internet disconnection injunctions. IIC Int Rev Intellect Prop Compet Law 46(1):10–37

Iglezakis I (2012) The legal struggle in the EU against Online Piracy. In: Synodinou T-E (ed) Codification of European copyright Law, challenges and perspectives. Wolters Kluwer, p 283

Leistner M (2014) Structural aspects of secondary (provider) liability in Europe. J Intellect Prop Law Pract 9(1):75–90

Liability of Internet Intermediaries for Privacy Violations in Europe. JIPITEC – Journal of Intellectual Property, 6 (3)

Malcom J (2016) European Copyright Leak Exposes Plans to Force the Internet to Subsidize Publishers, EFF. Available at https://www.eff.org/deeplinks/2016/08/european-copyright-leak-exposes-plans-force-internetInternet-subsidize-publishers

Mlynar V (2014–2015) A storm in ISP safe harbor provisions: a shift from requiring passive-reactive to active-preventative behavior and back. Intellect Prop Law Bull 19:1

OECD (2012) New sources of growth knowledge-based capital driving investment and productivity in the 21st century. Interim Project findings, May 2012. Available at http://www.oecd.org/sti/50498841.pdf

Parti K, Marin L (2013) Ensuring freedoms and protecting rights in the governance of the Internet: a comparative analysis of blocking measures of illegal Internet content and the liability of ISPs. J Contemp Eur Res 9(1):138–159

Synodinou TE (2014) Intermediaries' liability for online copyright infringement in the EU: evolutions and confusions. Comput Law Secur Rev 31(1):57–67

TNS Political & Social (2015) Flash Eurobarometer 211 - Cross Border Access to Online Content, EuropeanCommission

Trimble M(2009) Crossborder Injunctions in U.S. Patent cases and their enforcement abroad. Marq Intell Prop Law Rev 13:331

Van der Sloot B (2015) Welcome to the jungle: the liability of internet intermediaries for privacy violations in Europe. JIPITEC 6:211, para 1

Verbiest Th,Spindler G, Riccio GM (2007) Study on the liability of Internet intermediaries, p 17, Available at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf

Chapter 12
Responsibility and Liability of Internet Intermediaries: Status Quo in the EU and Potential Reforms

Gerald Spindler

Abstract The article provides a short overview of the recent developments and open issues in European intermediary liability with reference to the E-Commerce-Directive privileges. Moreover, hyperlinks and search engine issues are addressed, as well as the fundamental problem of blocking injunctions against access providers.

1 Introduction

Since the Internet increasingly became a global medium, issues of liability have also progressively come to the fore. Consequently, legislators across the globe realised that legal certainty was required for providers who were facing actions filed by right holders, as well as actions by criminal prosecutors.[1] Thus, different safe harbours concerning responsibility and liability were enacted, first in the U.S. with the Digital Millennium Copyright Act introducing the well-known notice-and-take-down action[2] and Germany with the Teledienstegesetz,[3] exempting all host providers from any kind of liability (and criminal responsibility)

[1]For example, Local Court of Munich, Case DS 465 Js 173158-95, 28 May 1998—CompuServe, published in Neue Juristische Wochenschrift (1998), pp. 2836–2840; District Court of Munich, Case 7 O 3625/98, 30 March 2000—AOL MIDI Files, published in Neue Juristische Wochenschrift (2000), pp. 2214–2217; see further, Spindler (1996), pp. 533–563; Sieber (1996), pp. 429–442.

[2]For notice and take down actions under the DMCA, see Clark (2002), pp. 206–210. In general, for DMCA regulations see Ginsburg (1999), pp. 137–179; Saltarelli (2002), pp. 1647–1689.

[3]This is now substituted by the Telemediengesetz.

G. Spindler (✉)
University of Goettingen, Platz der Göttinger Sieben 6, 37073 Göttingen, Germany
e-mail: lehrstuhl.spindler@jura.uni-goettingen.de

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_12

if they did not have actual knowledge of what was occurring on their servers.[4] The EU used both acts as a blue print for the safe harbour privileges in the E-Commerce Directive.[5]

However, the safe harbour privileges have come under attack from different sides. In particular, right holders have attempted several techniques aimed at restricting Internet piracy in most countries by filing actions for injunctions, or by putting pressure on legislators to introduce new agencies or actions to block websites or warn Internet users from continuing to infringe upon copyright, like the French HADOPI law.[6] These tendencies are currently culminating in the review of enforcement actions concerning copyright infringement, which also involves a review of safe harbour privileges accorded to service providers.

Hence, we will shortly describe the general setting of the safe harbour privileges contained in Art. 12–15 of the E-Commerce Directive (ECD) and then turn to some important cases of the European Court of Justice (ECJ) concerning injunctions, as well as interpretations of Art. 12–15. The second part examines the ongoing discussion concerning the potential reform of Art. 12–15, including the strategy of the EU for the Digital Single Market ("follow-the-money" approach, 4.3.); with a particular focus on one of the first proposed provisions regarding online platforms with copyright content in the leaked proposal of the EU-Commission relating to copyright in the Digital Single Market (6.1.).

2 The Setting

As a general principle and likely serving as a source of guidance for all safe harbour privileges, Art. 15 of the ECD states that providers do not have any obligation "to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity." The ECD distinguishes between different types of providers such as access providers dealt with in Art. 12 or host providers regulated in Art. 14 of the Directive. The underlying rationale is that mere conduit and simply offering technical assistance cannot be qualified in the sense of secondary liability as assisting an infringer in their illegal activities.[7] Access providers (mere conduit) are exempted from any kind of civil liability, as well as criminal responsibility for content that is routed by

[4] An overview of the main liability problems regarding TDG is described by Spindler (1997), pp. 3193–3199.

[5] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17 July 2000, pp. 1–16. See further, Peguera (2009), pp. 481–512, who compares DMCA Safe Harbours and the European Counterparts.

[6] Lucchi (2011), gives an overview of the French HADOPI Law; for an analysis of the three strikes policy see further, Haber (2010), pp. 297–339.

[7] See recitals 42, 43, 44 of Directive 2000/31/EC.

their networks, even if they have actual knowledge of illegal activities—given that they do not intentionally collaborate with infringers, Art. 12 ECD. Host providers are freed from criminal responsibility if they do not have actual knowledge of illegal content or activities and from civil liability if they are not aware of evident circumstances of illegal content and activities. Once they receive a notification that illegal content is stored on their servers or illegal activities are carried out, they have to take the content down or disrupt access to illegal activities.

However, Art. 12(3) and Art. 14(3) of the ECD provide for an exemption to the safe harbour privileges regarding court or administrative orders to stop illegal activities or access to it in the future. Thus, Art. 12(3) states that the exemption shall not affect the "possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement", similar Art. 14(3) "shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information."

Whereas some of the notions are open to interpretation, such as the "knowledge" of a provider (e.g. does this concern specific content? Is knowledge of incidents sufficient?), the backdoor of the safe harbour privileges has been the injunctions. They still play a decisive role in allowing rightholders (and other victims) to file claims—and most ECJ decisions concern these types of injunctions:

3 Injunctions

3.1 Access Providers

Decisions and Pending Cases at the ECJ

As access providers supply gateways for all kinds of websites, it is evident that as one of the strongest means to intercept piracy activities, rightholders attempted to get blocking injunctions from courts. The first decision of the ECJ is characteristic of the charges that rightholders fired against access providers:

Scarlet v. SABAM

In the ECJ case of *Scarlet v SABAM* the Belgian Society of Authors, Composers, and Publishers (SABAM) initiated a claim against service provider Tiscali (later Scarlet). SABAM claimed that users of Tiscali's network were illegally downloading works via P2P networks, and therefore suggested that Tiscali should use filtering software that would prevent further infringement. The District Court of Brussels relied upon an expert who claimed that there were at least 13 systems

capable of effectively filtering P2P transmissions.[8] In contrast, the Brussels Court of Appeals[9] realised that different directives were conflicting, such as the Copyright Directive 2001/29,[10] the IP Enforcement Directive 2004/48,[11] the Data Protection Directive 95/46,[12] the ePrivacy Directive 2002/58,[13] and finally Articles 8 and 10 of the European Convention on Human Rights (ECHR). The Court of Appeals referred the case to the ECJ asking if and how the different requirements could be balanced.

The ECJ[14] clarified that Art. 15 of the ECD with its prohibition of general monitoring obligations for intermediaries does not permit a general filtering and blocking system without any incidence. Hence, the ECJ classified the following injunction as incompatible with European law:

> – first, that the ISP identify, within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic;
> – secondly, that it identify, within that traffic, the files containing works in respect of which holders of intellectual-property rights claim to hold rights;
> – thirdly, that it determine which of those files are being shared unlawfully; and
> – fourthly, that it block file sharing that it considers to be unlawful.[15]

The ECJ explicitly stated that rights protected under intellectual property legislation have to be balanced with other rights, specifically citing the *Promusicae* case[16] that "in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures."[17] Moreover, the ECJ also laid emphasis on the rights of users, in particular that the filtering system would affect their "right to protection of

[8]District Court of Brussels, Case No. 04/8975/A, 29 June 2007—SABAM v. S.A. Tiscali (Scarlet), a translated version is published in CAELJ Translation Series #001 (Mady, Bourrouilhou, & Hughes, trans), 25 Cardozo Arts & Ent. J. 2008.

[9]La cour d'appel de Bruxelles, Case No. 2007/AR/242, 28 January 2010 – Scarlet Extended v. SABAM.

[10]Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22 May 2001, pp. 10–19.

[11]Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights OJ L 157, 29 April 2004, pp. 16–25.

[12]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23 November 1995, pp. 31–50.

[13]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 12 July 2002, pp. 37–47.

[14]ECJ, Case C-70/10, 24 November 2011 – Scarlet Extended SA v. SABAM.

[15]ECJ, Case C-70/10, 24 November 2011 – Scarlet Extended SA v. SABAM, rc. 38–40.

[16]ECJ, Case C-275/06, 29 January 2008 – Promusicae v. Telefónica de España SAU.

[17]ECJ, Case C-70/10, 24 November 2011 – Scarlet Extended SA v. SABAM, rc. 45.

their personal data and their freedom to receive or impart information", protected by Arts. 8 and 11 of the ECHR.

The ECJ ruled against such a blanket filtering system suggested by SABAM:

> [The cited Directives] read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an internet service provider which requires it to install a system for filtering all electronic communications passing via its services, in particular those involving the use of peer-to-peer software; which applies indiscriminately to all its customers; as a preventive measure; exclusively at its expense; and for an unlimited period, which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual-property rights, with a view to blocking the transfer of files the sharing of which infringes copyright.[18]

Telekabel

Whilst at first glance, it appears that the SABAM case put an end to all intentions to introduce blocking and filtering mechanisms, in the Telekabel case the ECJ allowed a very specified and balanced injunction against access providers. This case refers to a claim brought against the Austrian access provider, UPC Telekabel, with the aim to block the website kino.to, which allowed users to illegally stream movies. The Austrian Supreme Court referred the case to the ECJ,[19] which established a set of criteria to be met to hand down court orders/injunctions against access providers.

First, the ECJ confirmed the view that an access provider has to be qualified as an intermediary according to Art. 8 (3) of Directive 2001/29 (InfoSoc), citing Recital 59 of Directive 2001/29 and formulas used in the decision LSG v. Tele2.[20] This is because of the fact that:

> the internet service provider is an inevitable actor in any transmission of an infringement over the internet between one of its customers and a third party, since, in granting access to the network, it makes that transmission possible [...] and allows customers to access protected subject-matter made available to the public on the internet by a third party.[21]

It is thus sufficient that by qualifying as an intermediary, there is a chance that users have access to the infringing website. So, the holders of a copyright or of a related right may act without having to prove that the customers of an internet

[18] ECJ, Case C-70/10, 24 November 2011 – Scarlet Extended SA v. SABAM, rc. 55.

[19] Austrian Supreme Court, Case 4 Ob 6/12d, 11 May 2012, published in Gewerblicher Rechtsschutz und Urheberrecht International (2012), pp. 934–939; see further Heidinger (2011), p. 37.

[20] ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 30; ECJ, Case C-557/07, 19 February 2009 – LSG v. Tele2 rc. 43 - 45; this judgement is commented by Nordemann and Schaefer (2009), pp. 583–584.

[21] ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 32.

service provider actually access the protected subject-matter made available to the public without their agreement.[22]

One of the core elements of the UPC Telekabel decision is once again the balancing of rights between rightholders, providers, and users.[23] Surprisingly however, the court does not mention the danger of overblocking and its impact upon users and their rights—in particular freedom of speech.

The ECJ realises that blocking and filtering entails huge expenses. However, from the perspective of the court these costs are outweighed by the possibility for the provider to determine the specific measures:

> an injunction such as that at issue in the main proceedings leaves its addressee to determine the specific measures to be taken in order to achieve the result sought, with the result that he can choose to put in place measures which are best adapted to the resources and abilities available to him and which are compatible with the other obligations and challenges which he will encounter in the exercise of his activity.[24]

Moreover, the ECJ points out that:

> such an injunction allows its addressee to avoid liability by proving that he has taken all reasonable measures. That possibility of exoneration clearly has the effect that the addressee of the injunction will not be required to make unbearable sacrifices, which seems justified in particular in the light of the fact that he is not the author of the infringement of the fundamental right of intellectual property which has led to the adoption of the injunction.[25]

However, what is specifically required of the provider remains unclear and is left to the discretion of the (national) court. On the other hand, the ECJ does not require that blocking and filtering systems really put an end to the infringement of intellectual property rights:

> Secondly, it is possible that a means of putting a complete end to the infringements of the intellectual property right does not exist or is not in practice achievable, as a result of which some measures taken might be capable of being circumvented in one way or another.[26]

Blocking and filtering should thus only be used to curb illegal access:

> None the less, the measures which are taken by the addressee of an injunction, such as that at issue in the main proceedings, when implementing that injunction must be sufficiently effective to ensure genuine protection of the fundamental right at issue, that is to say that they must have the effect of preventing unauthorised access to the protected subject-matter

[22]ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 38.

[23]ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 47.

[24]ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 52.

[25]ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 53.

[26]ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 60.

> or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter made available to them in breach of that fundamental right.[27]

In sum, only specific blocking injunctions are allowed. This is contrary contrast to general monitoring systems—i.e. what the court already indicated in the SABAM case.[28] It is up to the provider to strike the right balance (and for the court to control that balance). Moreover, third parties such as users should be allowed to claim their fundamental rights in the procedure leading to an injunction:

> It must be possible for national courts to check that that is the case. In the case of an injunction such as that at issue in the main proceedings, the Court notes that, if the internet service provider adopts measures which enable it to achieve the required prohibition, the national courts will not be able to carry out such a review at the stage of the enforcement proceedings if there is no challenge in that regard. Accordingly, in order to prevent the fundamental rights recognised by EU law from precluding the adoption of an injunction such as that at issue in the main proceedings, the national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known.[29]

Hence, the ECJ leaves most of the assessment regarding suitability of blocking and filtering mechanisms and their balancing of fundamental rights to national courts—which has had a considerable impact on national proceedings.[30]

McFadden Case

A third case concerns injunctions against providers of WiFi hotspots, which was referred to the ECJ by the lower regional court in Germany. In March 2016, the Advocate General Szpunar delivered his opinion, which accentuates the restrictive line with regard to injunctions. Sony Music applied for injunctions against an operator of a business who sold lighting and sound systems whilst operating a WiFi network, which was unprotected and open to anyone. In 2010, the hotspot was used to offer an illegal download of musical work. Sony Music demanded that the operator cease his activities, but the operator denied liability. The regional court considered applying the so-called Störerhaftung—the German secondary liability for future infringements. Prior to this, the German High Federal Court stated that a WiFi network which is operated by a private person should be secured against access by third parties (12 May 2010, I ZR 121/08).

---

[27] ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 62.

[28] ECJ, Case C-70/10, 24 November 2011 – Scarlet Extended SA v. SABAM, rc. 48, 50 ff.

[29] ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 57.

[30] Cf. 3.3.

Opinion of AG Szpunar

The opinion of the Advocate General (AG) highlights two important points for injunctions: first, payment of enforcement (pre-litigation) costs as well of court costs and second, specification of requirements for blocking and filtering systems of WiFi networks.

First, concerning pre-litigation costs and court costs, the AG upheld that Art. 12 of the ECD shields an access provider not only from liability, but also from any costs connected with an alleged infringement as such costs would result in a punitive effect on these intermediary services.[31] Although the AG realises that Art. 12(3) of the ECD "provides for the possibility of a court or administrative authority imposing certain obligations upon an intermediary service provider following the commission of an infringement, in particular by means of an injunction", the AG argues that Art. 12(3) can only be based upon a "specific obligation contemplated by Art. 12(3)",[32] not upon a general liability. However, the AG does not provide any hints regarding what could be interpreted as "specific obligation". In fact, it is hardly conceivable how a court could order an injunction that is not based upon any kind of obligation as the AG acknowledges the possibility to claim injunctions in general.[33] Finally, court costs depend upon national procedure law, which is not being modified by the ECD, as these costs are not part of damages but rather the distribution of costs in a civil procedure.[34]

The second issue concerns the widely discussed range of blocking and filtering mechanisms, i.e. if and how they could be required. Regarding the decision in the Telekabel case, one would be tempted to view the matter as settled, leaving it to the provider and national courts to strike the balance. However, whilst the AG admits that infringements against court orders can be sanctioned under Art. 12(3) ECD,[35] the Advocate limits the range of blocking orders widely.

In contrast to the ECJ in the Telekabel case, which left the selection of measures to the discretion of the provider, the AG rather objects to such a transposition in the case of WiFi networks:

> 123. The possibility of choosing which measures are most appropriate can, in certain situations, be compatible with the interests of the addressee of an injunction, but it is not so where that choice is the source of legal uncertainty. In such circumstances, leaving it

[31] Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 76.

[32] Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 79.

[33] Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 83.

[34] Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 85.

[35] Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 90.

> entirely to the addressee to choose the most appropriate measures would upset the balance between the rights and interests involved.

Thus, the AG requires the national court:

> hearing an application for an injunction to ensure that appropriate measures do indeed exist that are consistent with the restrictions imposed by EU law.[36]

However, it remains wholly unclear why there is less legal uncertainty in the case of telecommunication providers than for WiFi networks; the AG does not offer any insight into how he reached such a conclusion.

Instead, the AG declared some measures as totally incompatible with the aims of Art. 12 ECD. One such measure involves shutting down the entire Internet connection.

> 131 Indeed, a measure which requires an Internet connection to be terminated is manifestly incompatible with the need for a fair balance to be struck between the fundamental rights involved, since it compromises the essence of the freedom to conduct business of persons who, if only in ancillary fashion, pursue the economic activity of providing Internet access. Moreover, such a measure would be contrary to Article 3 of Directive 2004/48, pursuant to which a court issuing an injunction must ensure that the measures imposed do not create a barrier to legitimate trade.[37]

It is evident that these actions would be in contradiction to the socially desired infrastructure of the Internet and its access points. The same is true for orders that would result in a monitoring of all communication on a WiFiNetwork without any incident[38]—in line with the SABAM decision of the ECJ.[39]

However, in contrast to the German High Federal Court, the AG also rejects obligations to safeguard the WiFiNetwork–.[40] The AG puts forth several arguments: First, that "the introduction of a security obligation could potentially undermine the business model of undertakings that offer Internet access as an adjunct to their other services."[41]

In particular and in contrast to telecommunication providers, the AG discards any obligation for WiFi networks to identify their customers.

> 139. Indeed, some such undertakings would no longer be inclined to offer that additional service if it necessitated investment and attracted regulatory constraints relating to the

[36]Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 124.

[37]Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 131.

[38]Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 132.

[39]ECJ, Case C-70/10, 24 November 2011 – Scarlet Extended SA v. SABAM, rc. 35, see further Spindler (2012), pp. 311–313.

[40]Fundamental German Federal Court of Justice, Case I ZR 121/08, 12 May 2010 - Sommer unseres Lebens, published in Neue Juristische Wochenschrift (2010), pp. 2061–2065.

[41]Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 138 f.

> securing of the network and the management of users. Furthermore, some users of the service, such as customers of fast-food restaurants or other businesses, would give up using the service if it involved a systematic obligation to identify themselves and enter a password.[42]
>
> 142. I would observe that obligations to register users and to retain their private data fall within the scope of the regulations governing the activities of telecoms operators and other Internet service providers. The imposition of such administrative constraints seems to me to be clearly disproportionate, however, in the case of persons who offer their customers and potential customers access to the Internet via a Wi-Fi network as an adjunct to their principal activity.

In addition, the AG deems any control of the identity of customers as (in some way) contradicting the prohibition of general monitoring obligations:

> 143. Thirdly, although an obligation to make a Wi-Fi network secure that is imposed in a particular injunction is not the same as a general obligation to monitor information or actively to seek facts or circumstances indicating illegal activities, such as is prohibited by Article 15 of Directive 2000/31, any general obligation to identify and register users could nevertheless lead to a system of liability applicable to intermediary service providers that would no longer be consistent with that provision.
>
> 144. Indeed, in the context of prosecuting copyright infringements, network security is not an end in itself, but merely a preliminary measure that enables an operator to have a certain degree of control over network activity. However, conferring an active, preventative role on intermediary service providers would be inconsistent with their particular status, which is protected under Directive 2000/31.

Perhaps the strongest (and most disputed) argument of the AG refers to that:

> 145 (. . .) the measure at issue would not in itself be effective, and thus its appropriateness and proportionality remain open to question.
>
> 146. It must also be observed that, given the ease with which they may be circumvented, security measures are not effective in preventing specific infringements of protected works. As the Commission states, the use of passwords can potentially limit the circle of users, but does not necessarily prevent infringements of protected works. Moreover, as the Polish Government observes, providers of mere conduit services have limited means with which to follow exchanges of peer-to-peer traffic, the monitoring of which calls for the implementation of technically advanced and costly solutions about which there could be serious reservations concerning the protection of the right to privacy and the confidentiality of communications.

Finally, the AG observes:

> 148. (. . .) that any general obligation to make access to a Wi-Fi network secure, as a means of protecting copyright on the Internet, could be a disadvantage for society as a whole and one that could outweigh the potential benefits for rightholders.

Here the AG refers to the lower risk of infringement due to the large number of users given a limited bandwidth, and in general that WiFi access points "indisputably offer great potential for innovation."[43]

---

[42]Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 139.

[43]Opinion of the Advocate General Szpunar, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 149.

However, many issues could be raised against the opinion of the AG. Concerning the differences in bureaucracy costs due to safeguards of a WiFi network, there is little evidence given by the AG regarding why it should be easier for a "normal" access provider to comply with these obligations. Moreover, the AG seems to be driven by the specific circumstances of the case: the WiFi network does not constitute the core of the business, but it is offered as something "nice to have" for customers. Given that WiFi hotspots are offered by a wide range of businesses, it is doubtful whether the underlying assumptions of the AG are true. For example, in the case of a hotel that offers an open WiFi hotspot that does not require any identification, an individual would have enough time (and potentially bandwidth) to download a large amount of copyrighted works. Moreover, many telecommunication providers offer their own "hotspots" to their customers, sometimes in the form of a WiFi sharing device that uses the routers of other customers. How should such hotspots be treated? It is apparent that in these cases the provider does have information about the identity of the customer.[44] The argument that a simple log file that identifies the user (by a Mac address or a mobile phone number) is too burdensome, is not really convincing.

Finally, the AG simply declared which borderlines apply for injunctions concerning WiFi networks; however, what is conceivable to protect rightholders remains totally unclear. In sum, none of the existing mechanisms or technologies appears to satisfy the tests of the AG. If so, it would be an overstatement to continue to speak of balance of rights as rightholders are deprived of any means to prevent infringements of their rights. Moreover, neither the operator of the WiFi network is obliged to identify the users so that they remain anonymous and cannot be held liable, nor can the rightholder claim any action against the operator of the WiFi network. The same would apply not only in cases of rightholders, but also of personality rights like defamation or hate speech. In contrast to the Telekabel decision of the ECJ, it is somewhat surprising that AG Szpunar does not clarify sufficiently the differences between WiFi networks and "traditional" access providers that justify the complete disregard of any blocking injunctions.

The ECJ Decision

Just recently, the ECJ handed down the final decision and rejected some of the proposals of AG Szpunar—roughly following the criticism outlined above. Besides the clarification that Art. 12(1) ECD applies without any further conditions[45] (in particular not applying by analogy Art. 14(1) ECD),[46] the court follows the

[44]Ohly (2015), pp. 308–318, especially pp. 316 f.; apparently assessed different by Mantz and Sassenberg (2015), pp. 298–306, especially pp. 304 f.; likewise before Mantz and Sassenberg (2014), pp. 3537–3543, especially pp. 3541 f.

[45]ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 67 et seq.

[46]ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 64 et seq.

reasoning of the AG regarding pre-litigation cost and expenses; however, with an important specification that this exemption for costs refers only to actions for damages, and not for injunctions.[47] As the court states:

> 75 As a result, a copyright holder is also, in any event, precluded from claiming the reimbursement of the costs of giving formal notice or court costs incurred in relation to its claim for compensation. In order to be well founded, such an ancillary claim requires that the principal claim is also well founded, which is precluded by Article 12(1) of Directive 2000/31.

This reasoning follows the line already pointed out concerning the critique of the AG's opinion: If a claim for damage cannot be filed, a provider must not incur any costs that are related to this kind of claim. Hence, the first notice to a provider that an infringement has taken place on his networks is "free of charge".[48]

On the other hand, the court also upheld that Art. 12(3) ECD allows for actions of a rightholder against network operators to prevent future infringements, including the claim for the reimbursement of the costs for such an order:

> 76 Nevertheless, Article 12(3) of Directive 2000/31 states that that article is not to affect the possibility, for a national court or administrative authority, of requiring a service provider to terminate or prevent an infringement of copyright.
>
> 77 Thus, where an infringement is perpetrated by a third party by means of an internet connection which was made available to him by a communication network access provider, Article 12(1) of the directive does not preclude the person harmed by that infringement from seeking before a national authority or court to have the service provider prevented from allowing that infringement to continue.
>
> 78 Consequently, the Court considers that, taken in isolation, Article 12(1) of Directive 2000/31 does not prevent that same person from claiming the reimbursement of the costs of giving formal notice and court costs incurred in a claim such as that outlined in the preceding paragraphs.

Concerning the actions that a WiFi provider has to take, the court follows the reasoning of the AG with regard to emphasising once again the influence of the fundamental rights of providers, as well as of users (freedom of information)[49] and the balance that has to be struck. Like the AG, the court first discards the notion of monitoring all of the information transmitted, as it does not comply with Art. 15 (1) ECD.[50] Additionally, the court deems the complete shutdown of Internet connections as not consistent with the fundamental rights of the network operator (and going too far to remedy copyright infringements).[51] However, in contrast to the AG, the court found that a password restriction in combination with an obligation to identify the user could be required in a court order. The court argues that such a measure endangers neither the business model of the network operator[52] nor

[47] ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 78.

[48] Spindler (1998), pp. 178–179; Spindler and Volkmann (2003), p. 14.

[49] ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 81, 82.

[50] ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 87.

[51] ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 88.

[52] ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 91.

the freedom of information of users as it "constitutes only one of several means of accessing the internet".[53] Moreover, such a measure would not block any Internet site and would seriously discourage the misuse of the networks if "users are required to reveal their identity in order to obtain the required password and may not therefore act anonymously".[54] The ECJ emphasised the fact that denying any measures (like the AG) would "be to deprive the fundamental right to intellectual property of any protection, which would be contrary to the idea of a fair balance".[55]

As a first assessment, one of the main criticisms levelled against the AG's opinion has been taken up by the ECJ; that is, the total deprivation of protection of rightholders by granting liability exemptions even in the case of injunctions. However, the reasoning of the court gives rise to some doubts. For example, simply a password and an obligation to identify cannot really establish a link to the infringer using a WiFi network. To sue an infringer, it would be necessary to monitor the communication via the WiFi network; however, the court explicitly discarded this. Thus, a password may discourage an infringer initially—but not if infringers catch on to the fact that they cannot really be identified in the sense of causality. On the other hand, the court was restricted by the selection and facts presented by the lower court, thus it is yet to be resolved whether other actions may be suitable. Moreover, it remains unclear if the court upholds the doctrine of Telekabel whereby the provider may himself determine the actions; the ECJ restricted the analysis to the three measures envisaged by the lower regional court of Munich.

Impact on National Court Decisions

These decisions had—and will have—a huge impact on national jurisdiction. Two cases can highlight these tendencies, one in Germany, the other in UK:

Germany: The Goldesel Case

Rightholders deliberately filed three claims against the biggest access providers in Germany to obtain leading cases assessing the main blocking technologies such as the Domain Name System-block, blocking IPs, or blocking an URL by a mandatory proxy.[56]

---

[53]ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 92.

[54]ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 96, pursuing the approach of ECJ, Case C-314/12, 27 March 2014 – UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 62.

[55]ECJ, Case C-484/14, 16 March 2016 – McFadden v. Sony Music Entertainment, rc. 98.

[56]Regarding the functionality see Pfitzmann et al. (2008), pp. 42 f.; see further Sieber and Nolde (2008), pp. 182 f.; Frey and Rudolph (2008), pp. 78 ff.; summarising Leistner and Grisse (2015a), pp. 19–27, especially pp. 22 f.

Following the reasoning of the ECJ in the Telekabel case, in the "Goldesel" decision the German High Federal Court laid stress on the fact that a 100% successful technology is not necessarily required to obstruct access to illegal content.[57] The court also discarded the argument that infringers may easily change their servers, otherwise rightholders would not have a chance to claim for legal protection.[58]

Whilst the court also realised the danger of "overblocking", the court also emphasised that infringers may not hide away pretending that there is also legal content on their website if illegal content is clearly dominant.[59] However, it is still unclear what the specific relationship should be (4%?), or who has to prove that illegal content is outweighing the legal activities, especially with regard to the fact that a provider is not obliged to constantly monitor his website or other websites. Furthermore, what happens if after an injunction legal content will outweigh the illegal activities? How can third parties appeal the injunction? Closely related is the burden of proof for the issue regarding if and which technology is suited to block infringing websites. As rightholders (or other victims) cannot assess the specific circumstances of a provider,[60] the court shifts the burden of proof to the provider.[61]

One of the core elements of the decision of the German High Federal Court relates to the principle of subsidiarity concerning injunctions against access providers. Namely, whilst German jurisdiction does not usually acknowledge a subsidiarity for injunctions against host providers[62] the court accepts this principle explicitly for access providers. Thus, a rightholder first has to try to sue the infringer directly before turning to the access provider. However, the reasoning of the court

[57]German Federal Court of Justice, Case I ZR 174/14, 26 November 2015 – Goldesel, published in Gewerblicher Rechtsschutz und Urheberrecht (2016), pp. 268–278, rc. 48 pursuing the approach of ECJ, Case C-314/12, 27 March 2014 - UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, rc. 62 f.; furthermore, Leistner and Grisse (2015b), pp. 105–115, especially pp. 110 f.; concerning public law blocking orders already Spindler and Volkmann (2002), pp. 398, especially p. 406.

[58]German Federal Court of Justice, Case I ZR 174/14, 26 November 2015 – Goldesel, published in Gewerblicher Rechtsschutz und Urheberrecht (2016), pp. 268–278, rc. 47.

[59]German Federal Court of Justice, Case I ZR 174/14, 26 November 2015 – Goldesel, published in Gewerblicher Rechtsschutz und Urheberrecht (2016), pp. 268–278, rc. 55 in reference to J.B. Nordemann, in: Fromm and Nordemann, Urheberrecht, 11. Aufl. (2014), § 97 Rdnr. 170 "Spill-Over"-Effekt; Leistner and Grisse (2015b), pp. 105–115, especially p. 108.

[60]German Federal Court of Justice, Case I ZR 227/05, 10 April 2008, published in Gewerblicher Rechtsschutz und Urheberrecht (2008), pp. 1097–1099, rc. 20; Spindler (2011), pp. 101–108, especially p. 108; approved by Leistner and Grisse (2015b), pp. 105–115, especially p. 112.

[61]German Federal Court of Justice, Case I ZR 174/14, 26 November 2015 – Goldesel, published in Gewerblicher Rechtsschutz und Urheberrecht (2016), pp. 268–278, rc. 40; German Federal Court of Justice, Case I ZR 227/05, 10 April 2008, published in Gewerblicher Rechtsschutz und Urheberrecht (2008), pp. 1097–1099, rc. 19.

[62]German Federal Court of Justice, Case I ZR 18/04, 12 July 2007, published in Gewerblicher Rechtsschutz und Urheberrecht (2007), pp. 890–896, rc. 40; German Federal Court of Justice, Case VI ZR 101/06, 27 March 2007, published in Gewerblicher Rechtsschutz und Urheberrecht (2007), pp. 724–726, rc. 13; commented by Spindler (2007), pp. 511–514, especially pp. 513 f.

casts some doubt on this logic as the court stressed the fact that access providers are more "far away" from the infringement than the host provider—if we take the example of a large host provider such as cloud computing, this argument is more than doubtful. Moreover, it is still unclear if collections of links or search engines are to be treated like access providers.

The court then specifies the requirement for an unsuccessful attempt against infringers. One of the core elements regards attempts to identify the operator of the infringing website, in particular to follow hints concerning payments or other clues.[63] This corresponds to the "follow the money" approach of the EU-commission.[64] Furthermore, rightholders may claim disclosure of identity from marketing operators who have advertised on the infringing websites. Regarding the blocking technologies, only those that do not "overblock" are admissible.[65]

Moreover, as most blocking technologies require a considerable amount of effort, access providers do not want to bear the costs for blocking and thus the issue of expenses remains unresolved. As civil law (at least in Germany) does not provide for a sharing model of expenses, the costs are a considerable factor in the proportionality test of blocking injunctions.[66]

UK: Blocking Orders

Besides blocking injunctions against the famous web site "the Pirate Bay", in Italy, Sweden and Denmark[67] a case stemming from UK highlights the ongoing procedures. In the case of *Twentieth Century Fox & Others v Newzbin*[68] several Hollywood film studios sued Newzbin—a filesharing site—for copyright infringement by communicating to the public.[69] Newzbin obviously had specific knowledge of the infringement taking place on the site. Following the order against Newzbin, rightholders sued British Telecommunications (BT) to obtain an injunction to block content from Newzbin. The High Court of England and Wales ruled

[63]German Federal Court of Justice, Case I ZR 174/14, 26 November 2015 – Goldesel, rc. 87.

[64]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 9 December 2015, COM (2015) 626 final, p. 13 commented by Spindler (2016), pp. 73–81, especially p. 80.

[65]Likewise, Leistner and Grisse (2015b), pp. 105–115, especially pp. 108.

[66]This is assessed differently by Leistner and Grisse (2015b), pp. 105–115, especially pp. 113, who are only referring to voluntary cost absorption. In this case, the blocking would always be unreasonable and therefore inadmissible.

[67]See for example, Italian Supreme Court of Cassation, 29 September 2009 – Bergamo Public Prosecutor's Officer v Kolmisappi; Swedish Court of Appeal, 4 May 2010 – Columbia Pictures Industries Inc v Portlane AB; and Frederiksberg Court, 29 October 2008 – IFPI Danmark v DMT2 A/S.

[68]UK High Court of Justice, Case Ltd [2010] EWHC 608, 29 March 2010 – Twentieth Century Fox Film Corporation & Anor v Newzbin.

[69]Contemplated in s20 of the Copyright, Designs and Patents Act 1988.

that access to Newzbin should be blocked[70]; arguing that filtering and blocking is possible as charities such as the Internet Watch Foundation (IWF) are able to filter criminal material such as child pornography. However, the court did not address whether filtering and blocking is really an efficient means against infringing activities.

This injunction was followed by other court orders, such as by the High Court against Internet access providers facilitating access to the website "The Pirate Bay"[71] or in *EMI Records v B Sky B*[72] concerning torrent sites called KAT, H33T, and Fenopy. In the EMI Records case, the judge Arnold J stated that the efficacy of blocking technologies such as the effect of the Italian blocking order resulted in a 73% reduction in audience going to The Pirate Bay, and a 96% reduction in page views. On the other hand, these findings have been contested, such as for example within a report released by the UK's Office of Communications (Ofcom).[73] Further, this strand of court rulings is reflected by the Digital Economy Act 2010, which contains in section 17 and 18 regulations on secure blocking injunctions.[74]

3.2 Host Providers

Not only access providers were under attack, but also host providers. In a case based on trademark infringements, the ECJ accepted for host provider injunctions. The case of *L'Oréal v eBay*[75] was one of the most prominent cases and just the tip of the iceberg of all procedures—particularly in the German context—which targeted the trading platform eBay. The cosmetic manufacturer L'Oreal filed an action against the auctions website eBay for the actions of distributors of unauthorised sampler products, who removed the sampler package and then sold the products on the site. In contrast to passive trading platforms, eBay assisted traders with a set of services dedicated to foster their offers.

eBay allowed the placement of sponsored links to the infringing products or helped to purchase Google Adwords and other keyword search engine placement that directed to the pages on eBay. eBay claimed the safe harbour privilege

[70]UK High Court of Justice, Case [2011] EWHC 1981, 28 July 2011 – Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc.

[71]UK High Court of Justice, Case [2012] EWHC 1152 (Ch), 2 May 2012 – Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors.

[72]UK High Court of Justice, Case [2013] EWHC 379 (Ch), 28 February 2013 – EMI Records Ltd & Ors v British Sky Broadcasting Ltd & Ors.

[73]OFCOM. *"Site Blocking" to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act*. Official Advice, (2010), http://bit.ly/175vMBN.

[74]The Digital Economy Act 2010 is available at: http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf.

[75]ECJ, Case C-324/09, 12 July 2011 – L'Oréal SA and Others v eBay International AG and Others.

according to Art. 14 ECD but the ECJ rejected that defence. The ECJ upheld that Art 14(1) of the E-Commerce Directive could only be applied to passive operators who behave in a neutral manner and do not assist infringers. Moreover, the ECJ argued that one of the obligations for a provider might be the identification of traders. Hence, the distinction between active and passive, and between neutral and positive host providers has become crucial for the application of safe harbour privilege for host providers.

3.3 Consequences for Other Areas

The majority of the cases particularly on the national level, regarded copyright or trademark issues. However, it is important to note that the conception of safe harbour privilege applies to all kinds of liabilities and responsibilities, thus, also to defamation or privacy. However, whilst it might be easy to determine a copyright infringement, it is in fact hard to determine defamation or personality rights as these require a careful balance of freedom of speech (and press) on one the hand and protection of personality on the other hand.

4 Potential Reforms

Part of the digital agenda of the EU Commission concerns a review of the efficacy of enforcement procedures, in particular with regard to copyright.[76] Moreover, some notions of the ECD were differently implemented in the Member States, which gave rise to reflections on how to specify the safe harbour privileges, especially considering the ECJ decisions.

4.1 Notice-and-Take-Down and Actual Knowledge

One of the problems applying the ECD refers to the definition of actual knowledge as required by Art. 14 ECD, in particular its required level of awareness of facts and circumstances that suggest illicit content or activities (of third parties). Some Member States require a formal procedure and an official notification by authorities to assume actual knowledge of a provider, whilst others leave it to the courts to determine actual knowledge. A third approach may overcome these problems and

[76]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Dingle Market Strategy for Europe, 6 May 2015, Com(2015) 192 final, pp. 6 f.

specify what is required by the ECD, namely a notice-and-take-down approach,[77] following the US model of the DMCA.[78]

However, even a notice-and-take-down procedure yields some problems. On the one hand, providers do not want to be confronted with the legal problems of their users/clients (in particular their dealings with third parties). Providers, as technical intermediaries, cannot always handle and assess complex legal matters, which is quite obvious for defamation etc. as a careful balancing of rights should be done at all times, particularly concerning freedom of speech. Moreover, if providers are to act upon mere notifications there could be potential abuse by fictitious "victims" seeking to hamper a competitor or adversary. Thus, some Member States, such as the Netherlands, declare a simple notification—like a message by anybody - as insufficient, whilst a court order always meets the requirements of a notice.[79]

In contrast, right holders are interested that providers act as fast as possible given the enormous potential of disseminating illicit content via the Internet. It is hard for right holders (and the state) to enforce compliance with existing rules and norms. This is a result of the "anarchical" architecture of the Internet—designed to circumvent breakdowns of elements of the net—which hinders effective control. In most cases, it is only the provider who could be held responsible as the infringing parties are not known or are hard to reach.

To balance the competing interests noted above, two extremes should be excluded: mere reliance upon official notifications by authorities on the one hand; and assuming actual knowledge following simple notification on the other. The only reliance upon official notification would lead to a *de facto* exemption from liability of providers, even if they were clearly aware of illicit activities going on.[80] Official authorities often do not have the capacity or resources to pursue every infringement. In contrast, just a simple notification would invite anyone to inform providers of contents or activities, regardless of the reliability, of the quality, and of the accuracy of the notification. Even if the notifier could be held liable according to national legal systems, the probability of abuse is too high to accept a simple notification system. Moreover, simple notification places the burden of assessing the quality of the notification upon the provider. There is a greater likelihood that providers would take down content to avoid the risk of being sued or prosecuted rather that retaining it.

One potential solution to this conflict could be the adoption of a modified notice and take-down procedure combined with a counter-notice and put back option, like in Finland.[81] Similarly, the German High Federal Court developed a similar scheme

[77]Cf. 3rd Report Chapter C.III.3. See further Verbiest and Spindler (2007), pp. 15–17.

[78]For a detailed comment on the US-American role-model, see Holznagel (2007), pp. 971–986; Holznagel (2013), § 2 pp. 5 f.

[79]See for more details, 3rd Report C.III.3.c), in particular Country Report Netherlands.

[80]For more details, see 3rd Report C.III.3.c.) bb and in particular the Country Report Spain.

[81]Cf. 3rd Report Chapter H.I. and more details in Country Report Finland.

in the case of a blogger,[82] requiring the victim (right holder) to notify the provider about the infringement or defamation. Having received the notification, the provider would be required to act expeditiously in provisionally withdrawing the content and informing the customer about the notification, giving him the chance to react. Under such a scheme, it would be up to the customer to make a risk assessment regarding whether he should send the provider a counter-notice. Only after receiving such a counter-notice would the provider be obliged to put the content back online. If the provider does not receive an answer from the rightholder indicating that he will file an action against the client, the provider will be obliged to put the content back online again; if the rightholder files an action against the client, the provider is obliged to take down the content until the final decision of the court. This counter-notice system is in operation in Finland and in the US (operated by the Digital Millennium Copyright Act (§ 512 (g) (2) (C), DMCA)).

Moreover, to avoid any abuse of this procedure, Member States should be obliged to introduce rapid preliminary review proceedings. Thus, providers would not be placed in the invidious position of having to act as *de facto* judges. Moreover, the risk of abuse—in particular the danger to freedom of speech—is largely reduced, as the rightholder may well be entitled to file an action for injunctive relief.

The notification could follow certain rules, as provided for in French legislation, such as requiring the name and other details of the person tendering a notice and specifically identifying the incriminating content. To avoid any bureaucratic procedures, providers could be obliged to publish corresponding templates on their websites—as France already requires and most providers do.[83] Whilst the design of such a template could be left to self-regulation, an agreed European template would be preferable to avoid a situation where victims have to incur costs to inform themselves about the different procedural requirements on each occasion.

4.2 Duty of Care

In reality, the safe harbour rules privilege those providers who do not exercise any kind of control or monitoring of activities on their servers. In contrast, those who have implemented some sort of screening or use scouts cannot benefit from safe harbour privileges as these providers then have actual knowledge about illicit activities. Thus, Art. 14 ECD does not provide for any incentives for providers to take voluntary caution regarding legal content.

[82]German Federal High Court, Case VI ZR 93/10, 25. October 2011 – Blog-Eintrag, rc. 24, published in Gewerblicher Rechtsschutz und Urheberrecht (2012), pp. 311–314.

[83]For details cf. 3rd Report Chapter C.III.3.bb), in particular Country Report France.

One way to apply liability privileges to those providers who are voluntarily monitoring content could be the introduction of a Good Samaritan privilege.[84] Moreover, safe harbour privileges could be coupled with automated enforcement programmes, such as those in place for eBay; thus, enabling right holders to monitor websites themselves and file claims against infringers. In contrast, the general introduction of duty of care for providers would leave the successful approach of Art. 12–14 ECD as it ends up in a liability for negligence that would contradict the passive neutral stance of providers.

4.3 Follow the Money Approach

Most illegal websites require users to pay for the possibility to make use of illegal content, or they use advertising placement on these websites. As operators of the websites, as well as servers, are often not located in the EU, it is evident that marketing enterprises and financial institutions may be held liable, as without their assistance these websites could not easily survive. The EU Commission promotes this approach ("follow the money")[85] to render it harder for illegal foreign websites to continue their counterfeiting and piracy activities. However, the details are still unclear; whilst marketing enterprises are clearly aware of the character of those platforms where they are placing their advertisements (as they want to reach customers with specific interests), banking or financial institutions usually have to be considered like providers in the sense of neutral infrastructure providers. Thus, whereas marketing enterprises may be held liable for fostering the illegal activities of third parties, banking institutions can only be required to stop handling payments etc.

4.4 Hosting

Although the ECJ draws a line between providers who enjoy exemption from liability and those who are relatively actively involved in activities of infringing users or at least assist them (L'Oreal case), it is still unclear what specific criteria are required to assess the "neutrality" of a provider. However, it seems to be difficult to develop one-size-fits-all criteria for the qualification of an active role of a provider. One way to create more legal certainty would be the adoption of self-

[84]For example, the good Samaritan privilege in 17 U.S. Code § 512c (2), which was introduced by the DMCA in 1998 and which limits the liability of a service provider if the service provider has designated an agent to receive notifications of claimed infringement.

[85]European Commission, Enforcement of intellectual property rights, available at: http://ec.europa.eu/growth/industry/intellectual-property/enforcement/index_en.htm; see further Spindler (2016), pp. 73–81.

regulations by industry and relevant stakeholders. Although this may be an attractive way to specify abstract notions, it seems to be unlikely that those who are on the brink between active and passive roles would really been involved in such self-regulation. On the other hand, a formal court procedure, which would allow for a qualification of a provider,[86] would not reduce legal uncertainty, as these assessments have to be done implicitly when a court is asked for an order against a host provider. Hence, the benefits of such an abstract procedure to declare a provider "active" or "passive" are difficult to calculate and do not seem to outweigh the additional bureaucracy costs.

4.5 Information Location Tools (Links, Search Engines)

As the ECD deliberately left the liability regime for hyperlinks and search engines untouched, it is not surprising that most Member States have developed different rules to cope with this issue.[87] Information location tools generally serve a social need as they facilitate Internet use (and that of any other electronic network). This is true for search engines, as well as for hyperlinks. As information location tools are of social value, constraints on their use should be particularly justified and well-founded.

Liability exemptions should consider the different levels of control and awareness that a provider of information location tools has concerning the content to which the tool directs the user. Simply put, it is hard to control the websites to which a user is directed to via a search engine, not least because a search word may be used in several different contexts. An obligation to check and verify the contents of websites identified by a search engine would lead, ultimately, to an obligation to perform a manual review, which would hamper the automatic indexation of the web and significantly reduce the amount of information that is accessible. However, the degree of control required may vary in the future because of technical developments (e.g., such as indexing websites according to their level of respect of measures aimed to protect minors or data-protection safeguards). If the provider of the information location tool has actual knowledge of illicit activities or content to which the tool is directing users, there is no reason to exempt it from liability. If, for example, a setter of a hyperlink is clearly aware of the fact that the website to

[86]Such a procedure was favoured by SPD (German party for social democracy) Bundestagsfraktion Arbeitskreis Urheberrecht (Working Group Copyright). In the opinion of the working group, a Host Provider should have the option to legally classify its status as an approved or non-approved business model. If the Provider is classified as a non-approved business model the legal consequence would be the loss of limited liabilities privileges. The working group paper is available at: http://www.spdfraktion.de/system/files/documents/positionspapier_telemediengesetz_spd-bt-fraktion_06012016_final.pdf, 6 January 2016, p. 6.

[87]Cf. 3rd Report Chapter G.II.2.a) (search engines), G.II.3.a) (hyperlinks).

which the hyperlink directs the user contains illicit content, he facilitates the access to the illicit content and increases its dissemination.

On the other hand, knowledge of illicit content can only be assumed if the link (or the search engine reference) leads the user directly to the incriminating website and not merely to a root page, which would then enable the user to find the incriminated website. Another exception to the general rule of exemption from liability should apply in the case of abuse. Simply put, providers should be held liable if they advertise their information location tools with specific reference to illicit content, such as centres for hyperlinks that direct exclusively to such material.[88]

In light of these general reflections, rules should depend upon the degree of control and on actual knowledge. Moreover, copyright cases concerning hyperlinks clearly have to be distinguished from the issue of liability for third party content: If a hyperlink is being set to direct the user to a pirated content on the web (i.e. a content published on the internet without the consent of the author) this act may constitute an infringement on its own. As the ECJ ruled, the setting of the hyperlink itself infringes the right to make the content available to the public as a new public is being reached.[89] Hence, copyright cases have to be distinguished from cases of setting hyperlinks to—for instance—defamation content.

Hyperlinks

Some Member States provide an explicit liability exemption for hyperlinks modelled closely on those for host providers.[90] This seems appropriate, as it considers that the setter of a hyperlink is regularly aware of the content of the website to which he is directing users via his hyperlink. Put simply, unlike search engine operators that conduct mere automatic searches without taking notice of the search results at all, the placing of a hyperlink is a deliberate action by the person setting the hyperlink. However, the setter of the hyperlink cannot be held liable for changes to the linked website *after* he has set the link as he is not in a position to obtain knowledge of such changes (unless he is notified of modification). Again, any circumvention or abuse should not fall under the liability exemptions.

[88]As the case in Belgium when users could upload hyperlinks directing them to pornographic websites and the hyperlink centre was explicitly dedicated to such use, Cassation, 3 févr. 2004, *R.D.T.I.*, 2004, n° 19 ; En première et seconde instance : Corr. Hasselt, 1er mars 2002, *inédit* ; Anvers, 7 oct. 2003, *A.M.*, 2004, liv. 2, pp. 166 et s., for more details see the country report on Belgium.

[89]CJEU 8.9.2016 – C-160/15, ECLI:EU:C:2016:644, - GS Media.

[90]Cf. 3rd Report Chapter G.II.3.a).

Search Engines

In considering search engines, a distinction must be drawn between so-called "natural results" or simple references (i.e. automatically generated links to websites as the result of a search) and so-called "commercial links" (or "Adwords"), which are used by search engine operators to generate revenues via a personalised advertisement system. With regard to "natural results", the social benefits of search engines outweigh all the disadvantages resulting from the listing of unlawful content amongst other material. Hence, search engines could be compared to access providers—indeed, some Member States have acknowledged this by conferring on search engines the liability exemption contained in Art. 12 ECD.[91] The above-mentioned exceptions to the general rule (in particular regarding abuse), can also be addressed by a clause concerning circumvention or abuse—the existing provisions in Art. 12 ECD regarding collusive behaviour or selection of contents/addressees of content, which is transmitted do not incorporate this type of abuse, such as search engines exclusively programmed to refer to illicit content (e.g. child pornography search engines). With regard to search engines as with any other type of intermediary, the core issue is not liability for damages, but rather injunctions ordering the blocking of illicit search results and the prevention of the future visibility of those search results. Injunctions might almost lead to specific monitoring obligations (to be practically implemented, e.g. by filtering). These problems will be addressed in a broader context.

4.6 Injunctions and Filtering

As the ECJ cases show, injunctions—as well as filtering and blocking—are one of the outstanding problems in the EU left untouched by the ECD. Injunctions have evolved in major Member States such as Germany, the UK, or France as a key battlefield between Internet intermediaries and rightholders. Injunctions concern the conflict between general monitoring by providers—which is widely held to be unfeasible—and the interests of rightholders who should not be confronted with the same infringements again. Simply put, injunctions refer to the prevention of infringements and future damages, which cannot satisfyingly be achieved by a mere notice and take-down procedure. Thus, injunctions are notice-and-stay-down procedures.

However, injunctions pose certain common problems. First, in general it is hard to assess and specify the feasibility of techniques to filter and block. Injunctions have a dynamic character, as obligations ensuing out of the injunction concern a (specific) monitoring in the *future*. Hence, obligations (if at all) should meet industry standards that are widely accepted at the time the injunction is handed

[91] Cf. 3rd Report Chapter G.II.2.a).

down as the law cannot force a provider to undertake measures which are not feasible. Second, incentives for providers to develop filtering techniques largely depend on their capacities to do so. This may vary according to their character as a profit- or non-profit organisation. Put simply, a private website owner without any profit interest (and without resources) cannot be expected to be able to develop filtering techniques on his own. Third, and closely related to the assessment of filtering capacities, is the unresolved issue of who should be obliged to produce evidence that filtering techniques are being used—providers or right holders? Economic efficiency theory indicates that the cheapest cost avoider is the party who is "nearest" to the technical information and can therefore best control and manage it. It follows that the burden of proof should lie with that party. Hence, it should be the provider who is required to adduce evidence that filtering techniques do not exist. As this evidence may be hard to produce, citation of widely accepted industry standards[92] could serve as a *prima facie* proof- as in other legal areas such as product safety or product liability. Fourth, the extent of the infringements that are covered by injunctions is highly disputed. Whilst rightholders have a strong and legitimate interest to ban not only specific illicit content (or infringements) but rather all similar infringements in the future, providers are confronted with the problem that they cannot monitor all similar content. Assuming that there are no filtering techniques available to manage and control similar infringements, such an obligation would result in an overall monitoring obligation. Fifth, there is no certainty regarding a principle of subsidiarity which would force rightholders to first sue an infringer (if possible), and then may file actions against providers when their actions turns out to be unsuccessful. In the case of access providers, some jurisdictions accept this principle whereas for host providers such a principle is being rejected.

The ability to strike a balance between the interests of the parties is difficult. The starting point should be that providers would be given an incentive to develop and use filtering techniques to ban similar infringements in the future. However, they should not be held liable for the general absence (non-availability) of technical means to avoid such infringements. The availability of filtering techniques may vary largely according to the content to be monitored, such as copyrighted content or defamatory speech.

To solve this dilemma there are multiple possibilities. One solution could be to rely upon the principle of negligence in civil law (not strict liability) and leave it to the courts to develop the criteria—this is the case for instance in Germany, although injunctions are in question. However, this might lead to a fragmented European scene of different standards. Moreover, there is no guarantee that a balanced and dynamic standard would be established in time and provide legal security for both sides. It would be left to the courts to define these standards. There would be no guarantee at all that relevant cases would be brought before the courts allowing for the establishment of these standards.

[92]Such as CEN-Standards though these not yet have been adopted.

A co-regulatory model following the approach in Art. 13 ECD, and referring to industry standards (considering also the interests of stakeholders), may resolve the Gordian knot, perhaps restricted to some (prominent) sectors such as copyright or trademark infringements (such as in Finland for notice-and-take-down procedures). European standardisation committees (CEN) may be commissioned to develop standards. Thus, dynamic standards and legal security could be ensured, as courts would have to respect those standards. Under such a scheme, where filtering techniques according to those standards were available, providers could be ordered to filter and block similar infringements. This would still leave enough leeway for providers to develop their own technical solutions, as technical solutions of individual providers deviating from the recognised standards would not be prohibited. However, when deviating from standards, the onus of proof regarding the equivalence of individual technical measures and specifications in standards would lie upon the provider. Finally, such a model could be combined with incentives for providers to comply with these standards by giving rightholders the right to claim for broad injunctions against those who do not comply with industry standards.

References

Clark DL (2002) Digital millennium copyright act: can it take down internet infringers? Comput Law Rev Technol J 6:193–220

Frey D, Rudolph M (2008) Rechtsgutachten zur Evalierung des "Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien" im Auftrag des Bundesverband Digitale Wirtschaft (BVDW) e.V

Fromm F, Nordemann W (2014) Kommentar zum Urheberrecht, 11. Aufl. 2014, Kohlhammer Verlag

Haber E (2010) The French revolution 2.0: copyright and the three strikes policy. Harv J Sports Entertain 2:297–339

Heidinger R (2011) Die zivilrechtliche Inanspruchnahme von Access-Providern auf Sperreurheberrechtsverletzender Webseiten, Österreichische Blätter für gewerblichen Rechtsschutz (ÖBl), p. 37

Holznagel D (2007) Zur Poviderhaftung – Notice and Take Down in § 512 U.S. Copyright Act, Gewerblicher Rechtsschutz und Urheberrecht International (GRUR Int.), pp 971–986

Holznagel D (2013) Notice and Take-Down-Verfahren als Teil der Providerhaftung. Mohr Siebeck Verlag

Hughes J (2005) On the logic of Suing one's customers and the Dilemma of infringement-based business models. Cardozo Arts Entertain Law J 22:725–766

Leistner M, Grisse K (2015a) Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), Gewerblicher Rechtsschutz und Urheberrecht (GRUR), pp 19–27

Leistner M, Grisse K (2015b) Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2), Gewerblicher Rechtsschutz und Urheberrecht (GRUR), pp 105–115

Lucchi N (2011) Regulation and Control of Communication: the French Online Copyright Infringement Law (HADOPI). Max Planck Institute for Intellectual Property and Competition Law Research Paper No.11-07, available at http://s3.amazonaws.com/

Mantz R, Sassenberg T (2014) Rechtsfragen beim Betrieb von öffentlichen WLAN-Hotspots, Neue Juristische Wocheneschrift (NJW), pp 3537–3543

Mantz R, Sassenberg T (2015) Warum der Referententwurf die Verbreitung von WLANs nicht fördern wird. Computer und Recht (CR), pp 298–306
Nordemann J, Schaefer M (2009) Comment on EuGH Case C-557/07, Gewerblicher Rechtsschutzund Urheberrecht (GRUR), pp 583–584
Ohly A (2015) Die Verantwortlichkeit von Intermediären, Zeitschrift für Urheber- und Medienrecht (ZUM), pp 308–318
Peguera M (2009) The DMCA Safe Harbors and their European counterparts: a comparative analysis of some common problems. Colum J Law Arts 32:481–512
Pfitzmann A, Köüsell S, Kriegelstein T (2008) Sperrverfügungen gegen Access-Provider, Technisches Gutachten. Available at: http://www.kjm-online.de/fileadmin/Download_KJM/Service/Gutachten/Gutachten_Sperrverfuegung_Technik_2008.pdf
Saltarelli L (2002) The digital millennium copyright act and the functionality fallacy. Notre Dame Law Rev 77:1647–1689
Sieber U (1996) Strafrechtliche Verantwortlichkeit für Datenverkehr in internationalenComputernetzen (1), Juristen Zeitung (JZ), pp 429–442
Sieber U, Nolde M (2008) Sperrverfügungen im Internet: Nationale Rechtsdurchsetzung im globalen Cyberspace? (Strafrehtliche Forschungsberichte), Schriftenreihe des MPI für ausländisches und internationals Strafrecht
Spindler G (1996) Deliktische Haftung im Internet – nationale und internationale Rechtsprobleme. Zeitschrift für Urheber- und Medienrecht (ZUM), pp 533–563
Spindler G (1997) Haftungsrechtliche Grundprobleme der neuen Medien, Neue JuristischeWochenschrift (NJW), pp 3193–3199
Spindler G (1998) Störerhaftung im Internet, Kommunikation und Recht (K&R), pp 177–183
Spindler G (2007) Comment on German Federal Court of Justice Case I ZR 35/04, MultiMedia und Recht (MMR), pp 511–514
Spindler G (2011) Präzisierung der Störerhaftung im Internet; Besprechung des BGH-Urteils "Konderhochstühle im Internet", Gewerblicher Rechtsschutz und Urheberrecht (GRUR), pp 101–108
Spindler G(2012) Comment on ECJ Case C-70/10, Juristen Zeitung (JZ), pp 311–313
Spindler G (2016) Die Modernisierung des europäischen Urheberrechts, Computer und Recht (CR), pp 73–81
Spindler G, Volkmann C (2002) Die öffentlich-rechtliche Störerhaftung der Access-Provider, Kommunikation und Recht (K&R), pp 398–409
Spindler G, Volkmann C (2003) Die zivilrechtliche Störerhaftung der Internet-Provider, Wettbewerb in Recht und Praxis (WRP), pp 1–15
Verbiest T, Spindler G (2007) Study on the liability of internet intermediaries. Available at: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf

Chapter 13
Cyberspace v. Territory: Domain Names and the Problem of Protection for Geographical Indications

Theodore Georgopoulos

Abstract This chapter examines the protection of geographical indications (and designations of origin) against cybersquatting and other misuses and forms of exploitation of their reputation. Starting with European law, although it seems to offer enhanced protection for geographical terms, it appears that the challenges posed by the cyberspace to the legal principle of territoriality call for the regulation of the question at the international level. However, because trademark law, at both the international and comparative levels, is not sufficiently prepared to regulate the question of geographical indications with regard to domain name registration and use, we argue that an adequate protection of geographical indications can be based on the principle of distributive justice, as well as on the acknowledgement of an (international) right to local identity.

1 Introduction

Geographical identifiers and domain names are located in different spaces. Whereas geographical terms refer to the delimitated area bearing the name, domain names indicate a place in cyberspace. Yet, they cross paths when a domain name makes use of a verbal sign that is—partly or totally—homonymous to a geographical term.

A geographical identifier is not necessarily a geographical indication. The latter refers, a minima, to a term that indicates the origin of a product[1] and is protected by specific rules. The registration of these geographical terms in the domain name

[1]A geographical indication is not necessarily a geographical term. It may simply be a term of geographical significance, e.g. "feta", "grappa" and "ouzo" are not geographical terms, but they indicate a provenance and, as such, are protected geographical indications.

T. Georgopoulos (✉)
The Wine & Law Program - Jean Monnet Chair, Law School, University of Reims Champagne-Ardenne, 9 Boulevard de la Paix, 51100 Reims, France
e-mail: theodore.georgopoulos@univ-reims.fr

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_13

system by other than the authorised organisations of producers is a source of confusion for consumers. In fact, the registration of a geographical indication as part of a domain name by operators other than the concerned producers, acting collectively, is a major threat to geographical indication. As the ECJ stated, "for consumers, the link between the reputation of the producers and the quality of the products depends also on his being assured that products sold under the designation are authentic".[2]

The protection of geographical indications, especially in a legal system with enhanced integration, such as the European Union, entails the right to protect the name, as well as the interests associated with its use. This may appear to be an individual right to the use of a quality sign, but, in fact, it has little to do with intellectual property. The concept of geographical indications, at least its European version, refers to a wide range of conditions and factors that must be met during the production process. This interaction is supposed to give a product its specific characteristics and its proper identity, distinguishing it from other, similar products.[3]

The new programme for generic top-level domains (gTLD) further complicates the problem of the coexistence of domain names and geographical indications. Its development and initial implementation was launched in 2011 by ICANN, and it initiated new geographical gTLDs.[4] The scope of this programme was to release a vast number of new generations of gTLDs. In fact, a virtually limitless number of gTLDs are likely to be registered, including some closely related to geographical indications, e.g. ".wine" and ".vin". Moreover, it is possible to ask for the registration as gTLDs of protected names like ".champagne", ".cognac", etc. These new technical facts are likely to multiply the cases involving the misuse of geographical indications tremendously in the field of domain names.

Certainly, various solutions have been implemented to regulate the matter. A margin is left to States with regard to country-code-top-domain-names, because a link to the country may be required to accept the registration.[5] With regard to cities and regions, which can be used as an extension, ICANN wisely requires an application in this sense to be supported by the concerned local authorities. This condition neutralises many of the potential conflicts, but does not consider the legal and factual specificities of geographical indications. Local authorities are not necessarily the "owners" or the watchdogs of the homonymous geographical names. From the standpoint of geographical indications, the registration and the protection of the name are rather matters within the responsibility of the producers.

[2]ECJ, Case C-469/00, *Ravil Sarl v Bellon Import Sarl and Biraghi SpA*, ECLI:EU:C:2003:295, § 49.

[3]Berard (2016).

[4]Forrest (2013).

[5]E.g. Australian law requires that domain names ending in "com.au" must be derived from the business name of a registered Australian undertaking or a registered trademark. Omond and Waye (2014), p. 221.

In such cases, national law is incapable of offering satisfying solutions, mainly because of its territorial limits.[6] Domain names are assigned on a first-come, first-served basis, on the international scale. This stands as a major threat to geographical indications. Geographical names can be registered and used by natural and legal persons established abroad, whereas the domain name will be used in the cyberspace, worldwide.[7]

Indeed, the cyberspace creates situations "online" that cannot be efficiently regulated by legal instruments conceived for the "offline" world. The case of the protection of geographical indications in the field of domain names confirms this statement. The "technological requirement of absolute name uniqueness"[8] does not allow any possibility for the coexistence of identical domain names on the global scale. This means that, contrary to the "offline" world, there is no room for homonymous fully qualified domain names, equally protected either in the same or different legal orders.

This chapter examines the protection of geographical indications (and designations of origin) against cybersquatting, "typosquatting"[9] and other misuses and forms of exploitation of their reputation. Starting with European law, although it seems to offer enhanced protection for protected geographical terms (2), it appears that the challenges posed by the cyberspace to the legal principle of territoriality call for the regulation of the question at the international level. However, because trademark law, at both the international and comparative levels, is not sufficiently prepared to regulate the question of geographical indications with regard to domain name registration and use (3), we argue that an adequate protection of geographical indications can be based on the principle of distributive justice, as well as on the acknowledgement of an (international) right to local identity (4).

[6]Dinwoodie (2014).

[7]Forrest H.A. ibid, 159, notes that "prior to the introduction of the DNS, outside of the diplomatic context geographical names had a relatively limited, territory-bound scope of use that could effectively be controlled through domestic law...When they began to be used online, geographical names came unmoored from the territory, and thus the legal jurisdiction, that they identify. Now they are potentially registrable as domain names by anyone, anywhere".

[8]Forrest H.A ibid, 301.

[9]In *Shields v Zuccarini*, 254 F 3d 476, 483 (3d Cir., 2001), the US Court defined "typosquatting" as "the intentional registration of domain names that are misspellings of distinctive or famous names, causing an Internet user who makes a slight spelling or typing error to reach an unintended site"; see also Lindsay (2007).

2 The Enhanced EU Protection

2.1 Protection of GIs against "Commercial Use" by Domain Names

EU protection for geographical indications is arguably the most advanced system of protection for geographical terms. It is based on the traditional concern of European countries about "appellations of origin" and the historical evolution of legal rules that established a sophisticated system of control in favour of the protection of such geographical terms. In particular, the French system of Appellations of Origin ("appellations d'origine", AOC), applied first to the wine sector, had a strong influence on the unification of the system of protection for geographical indications in Europe.[10]

In fact, the European approach to the protection of geographical indications does not focus on the geographical identifier itself, but on the quality, the characteristics or at least the reputation of the products originating from the defined geographical area. The use of the name (or its prohibition) is subject to an assessment focusing on the product itself (especially for the "designations or origin", and up to a certain point, the "geographical indications").

Starting with Council Regulation (EC) 510/2006 of 20 March 2006 on the protection of geographical indications and designations of origin for agricultural products and foodstuffs,[11] repealed by Regulation (EU) 1151/2012 of 21 November 2012 on quality schemes for agricultural products and foodstuffs,[12] European integration has built a European system of protection for "protected designations of origin" (PDO) and "protected geographical indications" (PGI) based on common criteria and a centralised system of registration and control (although national authorities still have an important role to play).[13]

Article 13a of Regulation 1151/2012 protects registered names against:

> any direct or indirect commercial use of a registered name in respect of products not covered by the registration where those products are comparable to the products registered under that name or where using the name exploits the reputation of the protected name, including when those products are used as an ingredient.

Regulation (EU) No 1308/2013 contains a similar provision for wines,[14] as does Regulation (EC) No110/2008 for spirits.[15]

---

[10]On the evolution of the French system on appellations of origin, see Georgopoulos (2014a).

[11]OJ L 93, 31.3.2006, p. 12.

[12]OJ L 343, 14.12.2012, p. 1.

[13]Blakeney (2014).

[14]Article 103 § 2a of Regulation (EU) No 1308/2013 of the European Parliament and of the Council of 17 December 2013, establishing a common organisation of the markets in agricultural products (OJ L 347, 20.12.2013, p. 671).

[15]Article 16a of Regulation (EC) No 110/2008 of the European Parliament and of the Council of 15 January 2008, on the definition, description, presentation, labelling and the protection of geographical indications of spirit drinks (OJ L 39, 13.02.2008, p. 16).

However, despite these settlements, it remains unclear whether Protected Designations of Origin and Protected Geographical Indications are fully protected against cybersquatting. The registration of a protected name as a domain name for an undertaking does not seem to constitute a "commercial use" in the sense set forth under European law. The registration of a protected name as a domain name may indicate the intention for a future commercial use, but it is unlikely that the prohibition in question can constitute a breach of positive EU law as such.

Moreover, in various cases, the commercial use of the geographical name as a domain name by parties other than the producers does not constitute a clear exploitation or misuse of the protected name:

(i) if the domain name is used for non-profit activities, e.g. cultural activities, political purposes, etc. In such cases, it is not possible to establish a "commercial use", at least directly. Nonetheless, the extensive use of a protected geographical name for purposes other than the promotion of the products for which the term is protected may spoil its reputation and/or its distinctiveness.

(ii) if the geographical indication is used by the relevant local public authorities. In fact, although a geographical indication does not have an owner, at least in a way equivalent to trademarks,[16] its management is entrusted to the producers and their organisations. As for the local authorities, they may be associated with this management—and most of the time they are—but from a legal perspective, they are distinct legal entities. However, how can e.g. the name "Cognac" be refused to the City of Cognac because it is also a protected geographical indication for spirits? Moreover, in the case of homonymous geographical terms, it would be difficult to justify the denial of registration by the authorities of a city, region, etc., whose name is partly or totally homonymous to a protected name. Certainly, EU law provides for rules of settlement in the case of homonymous names, but they refer to registration as geographical indications or designations of origin, not to conflicts between protected terms and domain names.[17]

(iii) provided that the registered domain name is registered exclusively for the marketing of products legally using the protected designation of origin or geographical indication. In such cases, it is very difficult to deny the "commercial use" of the geographical term because it is not misleading. Still, it is used in a monopolistic way. Certainly, one may argue that in such case, the registration and the use of the protected name as a domain name exclude all other producers. Nevertheless, it remains unclear, in light of positive European law, whether this behaviour is prohibited because it stays within the spectrum of the protected products. This is even harder to assert when the protected geographical name is only part of the registered domain name.

[16]On the ownership of geographical indications: Audier (1993), Georgopoulos (2014b).

[17]See Article 6 § 3 of Regulation (EU) 1151/2012; Article 100 of Regulation (EU) 1308/2013; Article 19 of Regulation (EC) 110/2018.

(iv) in the case of a protected geographical indication not enjoying a specific reputation. Not all geographical indications have the chance to be followed by the reputation that accompanies names like "champagne", "cognac" or "gorgonzola". In this sense, it is a matter of proof to show that the "commercial use" of a domain name that includes a protected designation of origin or a protected geographical indication "exploits the reputation of the protected name". For names that have acquired a low reputation, their protection based on positive law seems compromised, unless one includes in the perimeter of protection for PDO and PGI the potential reputation the name may acquire in the future. In the *Abadia Retuerta v OHIM* Case,[18] the General Court of the EU extended the protection of a sub-regional PGO (Valencia) for wines to the names of villages located in that region and yet did not produce any renowned wine, by reckoning that the PDO must guarantee the perspective of the future development of local production, and thus, the name of those villages should also be protected. Arguably, the same protection may be granted to geographical indications with a limited reputation in case operators or entities other than the producers register them.

(v) if the protected name has already been applied for, registered or established by use, in good faith, as a trademark before the registration of the geographical term. In such cases, in compliance with articles 14 § 2 of Regulation (EU) 1151/2012, 102 § 2 of Regulation (EU) 1308/2013 and 23 § 2 of Regulation (EC) 110/2008, the trademark, used as a domain name, is out of reach.

From the aforementioned, it is clear that with regard to domain names, even in the case of European PDO/PGI, the enhanced protection granted is subject to a case-by-case assessment based on the "use" (and not the registration) of a protected name as part of a domain name.

2.2 *The Use of GIs in a Domain Name as Comparative and Misleading Advertising*

Directive 2006/114 /EC offer another legal basis for the EU's protection of geographical indications on misleading and comparative advertising.[19] According to its Article 3, to determine whether advertising is misleading, one should consider:

a) the characteristics of goods or services, such as their availability, nature, execution, composition, method and date of manufacture or provision, fitness for purpose, uses, quantity, specification, *geographical or commercial origin* or the

[18]Case T-237/08, *Abadía Retuerta, SA v OHIM*, ECLI:EU:T:2010:185.

[19]Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (OJ 2006 L376, p. 21).

results to be expected from their use, or the results and material features of tests or checks carried out on the goods or services; ...

c) the nature, attributes and rights of the advertiser, such as his *identity* and assets, his qualifications and *ownership of industrial, commercial or intellectual property rights* or his awards and distinctions (italics added).

Moreover, according to Article 4f, comparative advertising shall be permitted provided that

"it does not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing marks of a competitor or *of the designation of origin of competing products*" (italics added).

Here, the term "designation of origin" should be apprehended broadly and should include both the geographical indications and designations of origin protected at the European level.

These provisions apply in the case of domain names. In the *B.E.S.T. v Bert Peelaers* Case,[20] the ECJ ruled that the term "advertising" as defined in Article 2a of the Directive must be interpreted as covering the *use* of a domain name. Thus, it is prohibited for a domain name to use a designation of origin or geographical indication, or to evoke it, and either mislead the consumer about the origin of the products marketed or at least take unfair advantage of the reputation of this geographical term.[21] Nevertheless, the Court explicitly stated that the registration of a domain name, as such, is not encompassed by that term.[22] This approach converges with the requirement of a "commercial use" set by Regulations N° 1151/2012, 1308/2013 and 110/2008 to protect a geographical indication against misuse.

To sum up, EU law offers satisfactory protection for geographical indications against their misuse as domain names on a multitude of legal bases. This protection focuses on "commercial use" and "comparative" or "misleading advertising", and not on the registration or the mere use of the protected geographical term as a

[20]Case C-657/11, Belgian Electronic Sorting Technology NV v Bert Peelaers, Visys NV, ECLI:EU:C:2013:516.

[21]A similar protection is granted by Australian law. In the *C.I.V.C. v Rachel Jayne Powell* [2015] FCA 1110 Case, the Federal Court of Australia addressed the legality of the use of the designation of origin "champagne" in the domain name "champagnejayne.com". The term "champagne" is protected under Australian law from the bilateral Agreement between the European Community and Australia on the wine trade, signed in 2008. The domain name in question was used for a professional website and social media related to educational programmes, tastings, etc. of sparkling wines in general, including champagne. According to the Federal Court (Decision of 10 October 2015), the conduct of the respondent was likely to have reinforced and encouraged the perpetuation of the misconception of consumers who may believe that all the wines presented on the website were related to champagne (§ 227). This attitude was qualified as misleading under Section 18(1) of the 2010 Competition and Consumer Act (Cth), which provides: "a person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive".

[22]Case C-657/11, § 44: "the mere registration of such a domain name does not in itself contain any advertising representation, but constitutes, at most, a restriction on the communication opportunities of that competitor, which may, where appropriate, be penalised under other legal provisions".

domain name. This may leave blind spots in the protection. Nonetheless, the most significant weakness of the European system of protection lies in its territorial limits: Because the cyberspace knows no limits of jurisdiction, it is particularly difficult to fight against the misuse of European PDOs/PGIs by domain names registered by persons located outside the European market and yet operating in relation to it. For this reason, it is important to assess the protection guaranteed at the international level.

3 The Discrepancies in the Law of Trademarks

3.1 The Inadequacy of the UDRP to Protect GIs

With regard to domain names and cybersquatting, the scholarship focuses on the dispute settlement through the WIPO's Uniform Domain Name Dispute Resolution Policy (UDRP). This mechanism is designed to resolve disputes involving domain names and trademarks. It stands as a contractual policy developed by ICANN to be used by registrar operators in the administration of the issuance and the transfer of domain names.[23]

The UDRP offers an important mechanism for the resolution of disputes related to conflicts between trademarks and domain names. More precisely, Paragraph 4a allows any third party to assert to the applicable Provider that: (i) a registered domain name is identical or confusingly similar to a trademark or service in which the complainant has rights; (ii) that the one that has registered the domain name has no rights or legitimate interests in respect of the domain name; (iii) the domain name has been registered and is being used in bad faith. The success of UDPF with regard to the protection of trademarks against cybersquatting is significant.

Nonetheless, the Policy cannot guarantee an equivalent level of protection for geographical indications for various reasons. Indeed, the UDRP does not apply to the abusive registration of geographical identifiers. This position is fully justified, and it is the only one that can be accepted with regard to the specificities of geographical indications.

In the WIPO Final Report on the First Domain Name Process, the authors stated that registrations of domain names violating geographical indications would not fall within the definition of abusive registration. The Report of the Second WIPO Internet Domain Process confirmed this position and further explained the problems impeding the extension of the protection to geographical indications.[24] According to the Report's recommendation:

[23]Lindsay D. ibid, 95 *seq*.

[24]WIPO, *The Recognition of Rights and the Use of Names in the Internet Domain Name System*, Report of the Second WIPO Internet Domain Name Process, http://wipo2.wipo.int, September 3, 2001.

> [i]t is undeniable that there is widespread evidence of the registration and use of geographical indications and other geographical source identifiers by persons who have no connection whatsoever with the locality to which the identifiers refer. These practices are misleading and harm, first, the integrity of the naming systems in which those geographical identifiers operate and, secondly, the credibility and reliability of the DNS. The question for decision, however, is whether there is a solid and clear basis in existing international law which can be applied so as to prevent erosion of the integrity of geographical indications and enhance the credibility of the DNS.[25]

The Report stressed the two major problems in the development of international law for the protection of geographical indications with regard to the Domain Name System (hereinafter DNS): First, it drew attention to the fact that international law for the protection of geographical indications is built on the link between the protected geographical term and the goods whose origin is expressed by the name. The international instruments on the protection of geographical indications suppose the marketing of goods.[26] The registration of a geographical term in the DNS is not necessarily related to the commercialisation of goods. Put simply, according to the existing standards of international law, the prohibition of false and deceptive indications does not cover the mere registration of the name in the DNS by someone not related to the specific geographical area and the goods that are concerned.

Second, the Report underlined the discrepancies in the application of the law on geographical indications. This is mainly a national law problem or is rather related to the multitude of national laws. There are different perceptions of the concept of geographical indications. Moreover—and the Report insists on this point—a name can be considered a geographical indication in one country, and thus be fully protected, whereas in another, it may be a generic term.[27] Because of the absence of global registration and management of geographical indications, uniform treatment for all geographical terms cannot be ensured.[28] Nonetheless, this is exactly what is needed, given the deletion of the principle of territoriality in the cyberspace.

Subsequently, the administrative panels of the WIPO Arbitration and Mediation Center have constantly confirmed their incompetence in such cases. The objectives of the UDRP, its principles and provisions are inadequate to cover the question of the conflict between geographical indications and domain names. The Second Report of the WIPO also stressed the need that "the question of the protection in the gTLDs of country names and the names of administratively recognized regions and municipalities be further considered in the appropriate intergovernmental fora, in particular with a view to a discussion on the need for new international rules for the protection of country names".

---

[25]WIPO, § 238.

[26]In this sense, the level of protection granted for geographical indications at the European level is higher, as will be shown later.

[27]This is e.g. the case of the 16 semi-generic designations for wine names recognised by U.S. law (27 CFR 4.2.4); on this question, see Mendelson and Gerien (2011), pp. 217, 267; Josling (2006).

[28]Geuze (2016) ibid, 99.

Certainly, in the *City of Potsdam v Transglobal Network Inc* case,[29] the Panel confirmed that if a trademark includes, as part of the mark, a geographical term, such trademark can be invoked under the UDNR. However, as has been demonstrated in various cases before the administrative panel, such as the *Comité interprofessionnel du vin de Champagnev Vickers* case, this possibility quickly reaches its limits.

Mr. Vickers was running an IT consultancy and computer sales operator business in London. In 2010, he registered the domain name "champagne.co" (".co" for Colombia). The *Comité interprofessionnel du vin de Champagne* (hereinafter "the CIVC"), which is the inter-branch organisation for champagne wine and is in charge of the protection of the prestigious designation of origin, filed a complaint with the WIPO Arbitration and Mediation Center in accordance with the UDNR.

The complainant argued that it held unregistered trademark rights on the "champagne" mark and that, on that basis, the UDRP was applicable to protect the word "champagne" against cybersquatting. In response, several of the respondent's arguments contended that the complainant's arguments were far from convincing, because he even contended that champagne was a protected designation of origin according to Regulation (EU) 1234/2007 (now 1308/2013).[30] However, one particular argument was much graver. It consisted in underlining that the word "champagne" was not a trademark, as it was not registered and has not been used as such in practice.

The Panel's reasoning on this point is particularly interesting, showing the weaknesses of the UNDR with regard to geographical indications. It underlined that the complainant's rights in the word "champagne" were based on French law, as well as on European law. However, the Panel stressed that geographical indications were intentionally excluded from the scope of the UDRP. As for the argument that the CIVC held rights under English law as a common-law trademark, the Panel's decision noted that to be protected, a geographical term must have become distinctive of the goods or services of a trader.[31] This was not the case for "champagne".

The Panel's reasoning is particularly revealing in that it exposes the inadequacy of the UDRP for geographical indications: ""Champagne" may be among the world's most famous geographical indications, but that in itself is not enough for it to qualify as an unregistered "trademark or service mark" under the Policy. For a geographical indication to be found to have acquired such status, something more than potential eligibility to succeed in a passing off action would be required. In particular, it would be necessary to show distinctiveness as an identifier of an individual trade source".[32]

---

[29] *City of Potsdam v Transglobal Networx Inc*., WIPOCaseNo.D2002-0856 ("potsdam.com").

[30] Regulation (EU) 1308/2013 of the European Parliament and of the Council of 17 December 2013 establishing a common organisation of the markets in the agricultural products (JO L 347).

[31] The Panel's decision cites Lindsay D. ibid, 208; see also *Bollinger v Costa Brava Wine Co Limited* [1960] Ch 262; *Vine Products v MacKenzie* [1968] FSR 625, cited by D. LINDSAY.

[32] Ibid.

Thus, it is particularly difficult for geographical indications to acquire such distinctiveness because, by definition, they identify products on their origin and (for European standards) their quality characteristics as described and required by law. The only exceptions that could be admitted would be those situations in which a geographical indication would be subject to a monopoly maintained by one single producer.[33] If one follows the reasoning of the Panel, the requirement for "distinctiveness as an identifier of an individual trade source" can further exclude protection against cybersquatting for geographic indications that are simultaneously protected as collective marks or certification marks.

This was clearly demonstrated in two cases regarding the geographical indication of "prosciutto di Parma" before the Administrative Panel of the WIPO. In contrast to "champagne", the geographical indication in question was also registered as a certification mark. In this sense, the Panel had no problem in applying the UDRP.

In the *Consorzio del Prosciutto di Parma v Domain Name Clearing Company, LLC* case[34] of September 18, 2000, the WIPO Administrative Panel decided on the use of the domain name "parmaham.com", registered by a US undertaking. According to 4(a) of the UDRP, the complainant had to assert and prove the following:

(i) that the domain name registered by the Respondent was identical or confusingly similar to a trademark or service mark in which the Complainant had rights;
(ii) that the Respondent had no rights or legitimate interests in respect of the domain name; and
(iii) that the domain name registered by the Respondent had been registered and is being used in bad faith.

With regard to the last requirement, the Panel considered that the complainant had failed to prove the registration and the use of the domain name in bad faith. Its position was based on two main points.

First, the panel underlined that, contrary to the complainant's argument, the term "Parma ham", apart from being a registered trademark, had a secondary meaning for the consumer, meaning "ham from Parma". In this secondary meaning, the words could be registered as a domain name. This affirmation clearly shows the discrepancies between trademark law and the approach of geographical indications: The secondary meaning in question allowing the registration as a domain name is the precise meaning of a geographical indication (ham from Parma!). Simply put, the function of the geographical indication (linking a product to its geographical origin) justifies, in principle, its registration in good faith.

[33]This is legally possible, as Art. 95 § 1 of Regulation (EU) 1308/2013 provides: "[a]ny interested group of producers, or in exceptional and duly justifiable cases a single producer, may apply for the protection of a designation of origin or geographical indication".

[34]Case No. D2000-0629.

Second, and consequently, the good or bad faith of the respondent should be scrutinised based on the effective use of the domain name. In the case of an individual trademark registered as a domain name, bad faith is proven by the mere selling either of products bearing the trademark or by the action of selling products other than the ones bearing the trademark.[35] On the contrary, in the case of a certification mark (which also stands as a geographical indication), it is possible for a retailer to sell or resell products bearing this certification mark. According to the Panel, "a certification mark allows its holder to determine who may manufacture and put on the market for the first time products bearing the trademark. Once the products are on the market in a relevant territory, the exhaustion principle (applicable at least at the national level, if not at the international level) commands that any purchaser of the products is free to resell them. At the occasion of such second sale, the seller is entitled to use the trademark to describe the products that it offers".

The Decision reveals the specificities of geographical indications: their production, sale and resale by multiple economic players make it particularly difficult to establish (and defend) a monopoly in the registration and use of the protected geographical term in similar conditions to those applying for trademarks. Moreover, the Panel—very wisely—recognised that the questions of unfair competition related to the reselling of products under a (collective) trademark do not necessarily fall under the limited scope of the UDRP.

The second case regarding "prosciutto di Parma" is substantially different. In the *Consorzio del Prosciutto di Parma v Matthias Gasser* case,[36] decided on August 15, 2003, the Panel had to decide on a complaint filed by the professional organisation responsible for the protection of the geographical indication "Parma ham". The complaint was filed against the registration of the domain name "parma-schinken.com". Given that "Schinken" is the German translation of the terms "prosciutto" and "ham", the registered domain name was directly challenging the geographical indication. To establish its case, the complainant had to prove that the respondent had no rights or legitimate interests in respect of the domain name. To verify this, the panel checked the specific use of the domain name.

Certainly, a reseller of trademarked goods is not necessarily excluded from using the trademark at issue in its domain name. However, acceptable use is subject to specific conditions: (1) the respondent actually must be offering the goods or services at issue; (2) the site must be used to sell only the trademarked goods; (3) the relationship between the respondent and the trademark owner must be disclosed; (4) the respondent must not try to corner the market in all domain names.[37]

[35]See Telstra Corporation Limited v Nuclear Marshmallows, Case no. D2000-0003.

[36]Case No. D2003-047.

[37]Oki Dare Americas, Inc. v ASD, Inc., WIPO Case No. D2001-0903.

On this point, the decision is substantially different from the "parmaham.com" case, although it concerned the same certification mark. The respondent had not yet used the domain name at the time of the examination. Thus, it was still possible to use the domain name in good faith by limiting the use of the site to the exclusive sale of products covered by the certification mark (and consequently, the geographical indication). On the contrary, the "parma-schinken.com" website was selling multiple similar and competing meat products under other brands. It was thus clear that the respondent was in the position "to bait Internet users looking for "Parmaschinken" and then switch them to other goods". Consequently, the respondent had no rights or legitimate interests in respect of the domain name.

Moreover, Paragraph 4(a)(iii) of the UDRP requires the complainant to establish that the domain name has been registered and used in bad faith. Given the sale of products that were in competition with those marketed under the certification mark, bad faith was easily confirmed.

The practice of the Administrative Panels of the WIPO Arbitration and Mediation Center shows that the mechanisms established to fight against cybersquatting are not suitable for the specific needs of geographical indications. Trademark law cannot ensure adequate protection against cybersquatting in the field of geographical indications, as the latter differ from trademarks and cannot be treated as a "classic" IP right. The protection ensured is limited and depends on whether the geographical name is also protected as a trademark or if it has attained a secondary meaning.[38]

3.2 The Paradox of the Secondary Meaning for Geographical Terms

These difficulties are not exclusive to the WIPO system. Other decisions outside the WIPO system confirm the difficulty of protecting geographical names against cybersquatting through trademark law. In *Barcelona.com Inc. v Excelentisimo Ayuntamiento de Barcelona,*[39] the Fourth Circuit rejected the arguments of the City of Barcelona with regard to the registration of the domain name "barcelona.com" for a private tourist site containing information about Barcelona. The Court underlined the contractual character of the UDNR Policy, which could not replace the competence of the courts. On this basis, the Court admitted that U.S. law applied to determine whether unregistered trademark rights were founded. However, the Court underlined that the term "Barcelona" was a descriptive term, referring to the

[38] In *The Paris Pages v Woohoo T&C Ltd.* case of the National Arbitration Forum (NAF Case No FA110763 of July 10, 2002), a similar approach was adopted with regard to the geographical name of "Paris"; see also D. LINDSAY, note 9, 230.

[39] *Barcelona.com Inc. v Excelentisimo Ayuntamiento de Barcelona*, 330 F.3d 617, Civ. No. 02-1396 (4th Cir., June 2, 2003).

Spanish city. Given that, no secondary meaning was attributable to the term—because the consumer was not associating the term with anything other than the city—no trademark protection could be granted for the term. Subsequently, the registration of the domain name "Barcelona.com" by a business with no relation to the City of Barcelona did not breach the relevant U.S. law.[40]

Inversely, in the *Chiemsee* case,[41] the ECJ held that a geographical term bearing no association to the relevant location in the mind of the consumer could be protected as a trademark. Simply put, if the term has acquired a dominant secondary meaning as a term designating the manufacturer of a product, there is no reason to prevent the name from being exclusively used as a trademark.[42] Consequently, this monopoly may guarantee protection against the abusive registration and use of the term in a domain name. However, this secondary meaning is scarcely affirmed in the case of protected geographical terms. This may be the case of a geographical indication with a sole producer or of a trademark that is registered or used prior to the protection of the geographical indication. With the exception of these situations, the *Chimesee* case law is of no use in protecting geographical indications.

These decisions confirm the inadequacy of the law on trademarks to protect geographical names, as they teach us that to ensure protection for these names against cybersquatting, the geographical name must have a "weak" significance, a secondary meaning. However, this is inherently contradictory for geographical indications. In the aforementioned cases, the names at stake were geographical names, but not geographical indications. The latter are subject to specific rules defending their distinctiveness, or rather their uniqueness: It is in principle contradictory for a geographical indication to acquire a secondary meaning. The paradigm of EU protection for geographical indications (and designations of origin) is very clear on this issue.

4 The Quest for an Adequate Protection of GIS: Distributive Justice and the Right to Local Identity

4.1 The Need for a Specific Legal Protection for GIs

The difficulties in ensuring the protection of geographical indications through trademark law mechanisms call for a specific legal framework. However, one should establish the fundamental principles of this specific protection.

In my opinion, theory has not yet sufficiently explored the particularities of geographical indications, and especially, the entitlements they create. Traditionally,

[40]Lanham Act: Chapter 22 of Title 15 of the U.S. Code; see Clowers (2006), p. 1.

[41]ECJ, Case C-109/97, Windsurfing Chiemsee Produktions v Boots & Attenberger, 1999 E.C.R. 1-2779.

[42]Goebel and Groeschl (2016).

geographical indications have been apprehended as specific quality signs governed by the concepts and the methodology of intellectual property. The role played by the WIPO—and by the WTO through the TRIPS agreement over the last decades—in the development of the international law of geographical indications and the relevant case law[43] has largely contributed to the assessment of this approach.

Still, the key features of geographical indications call for their "emancipation" from the doctrine of classical IP concepts, and especially trademark law. The WIPO panel in the Vickers case was right in underlining the specific legal status of geographical indications. Although the Panel's decision refused to extend the Policy to geographical indications, and thus, rejected the idea of enhancing the protection of a name like "champagne", this approach is fully harmonised with the true nature of geographical indications: They cannot be fully apprehended through the fundamental rules of intellectual property, for neither the holder of a geographical indication nor the property rights obey the usual rules that apply to trademarks.[44] Nevertheless, there are potentially major elements in common between trademarks and geographical indications: One, they may both refer to quality standards; two, they may create added value for the consumers (and, thus, for the users). These elements generate the interest in cybersquatting and the need for adjusted legal protection.

Here is the crucial point: Given their structural differences compared to trademarks, adequate protection for geographical indications cannot be ensured by the rules that apply in the case of a conflict between trademarks and domain names. In the same way that the specificities of geographical indications are considered against their use by trademarks, cybersquatting must also be adapted to these specificities.

Certainly, this does not mean that the protection granted by the law of trademarks should be excluded in those cases where a geographical indication is also protected through trademark law (e.g. as a collective mark or as a certification mark). Nevertheless, this protection has a circumstantial character and cannot replace the need for efficient and adequate protection for geographical indications.

The problem of cybersquatting has further exacerbated these problems because it challenges at least two of the cornerstones of geographical indications, that is, territoriality and property. With regard to territoriality, as we have already underlined, the fact that names used in the cyberspace do not obey the rules (and constraints) of the link to a specific place and jurisdiction calls for a regulation that offers sufficient justification of the need to protect a name at the world scale, as part of the identity of a specific place and a narrow circle of producers. With respect to

[43] According to the ECJ, Case C-388/95 *Belgium v Spain* [2000] ECR I-3146, pt. 54: "[geographical indications] fall within the scope of industrial and commercial property rights. The applicable rules protect those entitled to use them against improper use of those designations by third parties seeking to profit from the reputation which they have acquired. They are intended to guarantee that the product bearing them comes from a specified geographical area and displays certain particular characteristics"; see also Case C-3/91 *Exportur S.A.*[1992] ECR I-5553.

[44] Georgopoulos (2014a), Audier (1993).

the question of property, if the nature of geographical indications raises a difficult question, the *brand new world* of domain names is no less ambiguous: The rights related to domain names concern the "use" rather than the "ownership" of the registered name.

4.2 Distributive Justice and Human Rights

In my opinion, the philosophical foundations for the protection of geographical indications in the cyberspace are to be found in the principle of distributive justice. In an individualist approach, the theory of distributive justice, as explained by John Rawls, is based on two major principles:

> a) Each person has the same indefeasible claim to a fully adequate scheme of equal basic liberties, which scheme is compatible with the same scheme of liberties for all; and
>
> b) Social and economic inequalities are to satisfy two conditions: they are to be attached to offices and positions open to all under conditions of fair equality of opportunity; and, second, they are to be to the greatest benefit of the least-advantaged members of society (the difference principle).[45]

These principles are also applicable at the collective level with regard to the access of geographical indications (and the producers using them) to the cyberspace. The passage from individual to collective is based on the cosmopolitan approach to the world (and its globalised economy). Arguably, individuals pursue happiness through the affirmation of their identity and their consciousness of belonging to a larger community, that is, the world itself.[46] Consequently, the cultural and economic interests related to the collective affirmation and protection of a geographical indication stand as the common denominator for a group of producers of a product originating from a delimitated zone of production and responding to the same standards. In other words, the belonging (which is more than a feeling, but rather a cultural, and by all means, an economic statement) to a circle of economic actors means the sharing of the same objectives under the use of a common name (and ultimately, related to the same quality characteristics).[47]

With regard to domain names, this can be described as a settlement for the access—simultaneously for all producers—to a competitive space in the pursuit of wealth based on the reputation of the products (as identified through the name). More precisely, the registration of a domain name is likely to open the perspective of the "online" world in terms of promotion, information and transactions for the members of the group, identified based on the geographical name (and ultimately, the quality characteristics and/or the accompanying reputation). Inversely, the prerogatives related to the registration and the use of a term as a domain name

[45]Rawls (2001), pp. 42–43.
[46]Sypnowich (2005), p. 55.
[47]Forrest H.A ibid.

may deprive the interested group of producers of the possibility to fully enjoy this access because of the "first come, first served" rule. Moreover, the usurpation of the name through cybersquatting practices is unfair based on the aforementioned approach: The reputation already built by the producers is usurped by actors having no relation to the specified area and its added value, or at least, the enhancement through the Internet of the reputation of the area of production and its products, and consequently, the development of the producers is compromised.

These difficulties dictate the need for the recognition at the international level of a right to a geographical name as part of a more general entitlement[48] to one's specific identity. This identity does not necessarily coincide with national identity, although local identities are components of a larger national identity and the State must play an important role in the recognition and protection of such an identity.[49]

The access to the cyberspace and the protection of a local identity through its name are intimately related to the theory of distributive justice. Groups of producers do not necessarily have the knowledge, the education or even the financial and technological means to ensure the full and timely protection of their name, and consequently, of their identity. In particular, the risks related to the "first come, first served" rule, as applied in the case of domain names, often come from operators with profound experience in marketing, if not in cybersquatting. Law intervenes to ensure an equal (or at least equivalent) opportunity to the access and the protection of one's name in the cyberspace. By defending the right to occupy equal space through the registration of that geographical name as a domain name, the law makes sure that the producers and their zone of production have the opportunity to be identified, promoted and accessible through the geographical domain name.

However, does international law guarantee a positive right to one's local identity? It is unlikely that a right to the protection of local identity exists as such, with the exception of the rights recognised for minority groups, which is a distinct problem. Nevertheless, the protection of geographical indications, at least in its European apprehension, is related to the identity of the group residing, producing and prospering in the specific area.[50] As D.S. Gangjee put it, "it is helpful to think of GI protection as a mechanism for indirectly, yet meaningfully, sustaining certain cultural practices".[51]

More generally, the local identity in question is related to a sum of cultural and economic interests.[52] As a corollary of cultural diversity,[53] local identity may also

[48]On the difference between "capabilities" and "rights", see Nussbaum (2006), p. 284.

[49]Forrest H.A. ibid, 259, refers to "national identity" to assert the link between positive international law and the need for protection for geographical indications, through the principle of self-determination. Yet it is unlikely that the right of (internal) self-determination could be used in this case; not only has it been shaped in the specific context of protection of minorities, but, furthermore, local identity is not necessarily expressed (at least in an authentic and sufficiently direct way) as part of a larger national identity.

[50]Wilson (2006), p. 11.

[51]Gangjee (2015), pp. 544, 549.

[52]Forrest H.A. ibid, 254.

[53]See Tredinnick-Rowe and Taylor (2015).

be affirmed through the production and promotion of local products, which call for an adequate legal protection. Simply put, local identity stands as a matrix for the enjoyment, individually as well as in community, of various rights, including the right to conduct a business, freedom of expression (especially through the use and the protection of one's language) and, certainly, the right to property, apprehended largely as the sum of interests, capabilities and established situations that are economically significant.[54] Arguably, the entitlement to local identity includes the protection of the producers' rights in the cyberspace.

The principal addressee of this entitlement is the State. National law must recognise an appropriate legal form for the incorporation of the groups of producers, allowing them to act collectively and effectively. Given the structure of international law, which is still based on the pattern of inter-state settlements, it is up to national law to express and protect local identity. The groups of producers should be involved in the procedures for the registration of domain names. Nonetheless, one should not neglect the discrepancies among countries in the establishment of institutions, principles and rules for groups of producers. In countries like France and Spain, law, politics and tradition ensure a clear and stable status for producers' organisations. In other countries, including within Europe, the establishment of this status remains a quest. Moreover, even in countries presenting an advanced legal system, the degree of sophistication, stability and visibility of the local institutional players in charge of the protection of the geographical indications depends on the reputation of the indication. Put simply, it is not possible to entrust the protection of the geographical indication to producers' organisations through a uniform, rigid and immutable system of allocation of powers: Local, as well as national organisations often suffer from internal problems and conflicts, and they may face major economic crises, and eventually, disappear. The protection of the geographical name cannot risk being subject to these issues. Thus, the role of the State remains crucial, as it ensures continuity and neutrality. For the protected names of geographical places under its jurisdiction, the State has a major role to play.

Surprisingly, it is the affirmation of the State's dominant role that enhances the importance of international law.

From the standpoint of substantive law, the assessment of an entitlement to local identity and to the protection of geographical indications against cybersquatting cannot be based on national rules because of the transnational character of the cyberspace. The possibility for protected geographical terms to oppose their registration or their misuse as domain names should be based on the entitlement to local identity. The same goes for homonymous names that may be confusing. Simply put, the existing international (including European) protection for geographical indications should cover cybersquatting. This statement seems to have been largely ignored from the standpoint of positive international law. This discrepancy in the present international system is quite surprising: Whereas international law ensures

[54]Forrest H.A. ibid, 288.

significant protection for geographical indications against trademarks, the latter are better protected with regard to domain names.[55]

In this sense, it is not realistic to consider a specific legal framework, e.g. a multilateral international treaty to assert the right to local identity and its implementation in the field of domain names. This supposes a convergence of the perceptions on the nature, the definition, as well as the level of protection to be granted to geographical indications. Undoubtedly, we are far from such an evolution. Nonetheless, the affirmation of a right to local identity in the field of cyberspace and mainly (though not exclusively...) with regard to the registration and use of domain names would facilitate the revision of the existing mechanisms for dispute settlement of conflicts between protected geographical indications and domain names. More precisely, this would supply the missing piece in legitimating the actions of States and/or organisations of producers in defending a geographical indication against misuse through domain name registration.

From the standpoint of procedural law, it is clear that the extension of the UDPR mechanism (or any similar mechanism) to the protection of geographical names could only partly compensate for the actual weaknesses of international law. The contractual character of the Policy does not guarantee full protection on the international scale. From the recognition of the entitlement to local identity in the cyberspace, it would be real progress if cybersquatting were integrated among the practices that may constitute an infringement of the protection for geographical indications. This should be accompanied by the capacity of producers' associations, incorporated according to the law of the country of origin—at least in cases in which the law of the State is sufficiently developed—to file an application against the registration and the use of the protected geographical indications or any similar and confusing name. The recognition of this "locus standi" would facilitate access to the mechanisms of dispute resolution, as the lesson from *CIVC v Vickers* shows.

However, such protection of geographical indications supposes a centralised system of registration for protected geographical names at the global level. This would ensure the visibility, as well as the legitimacy, of the terms that should be protected against cybersquatting. The reform of the WIPO system for the registration of geographical indications by the Geneva Act[56] may contribute to this objective, if massive participation of States is achieved.

Finally, exceptions could be tolerated following the paradigm of the settlements of conflicts between geographical indications and trademarks, especially for

[55]And yet scholars underline that the existing mechanisms for the resolution of conflicts between trademarks and domain names are far from being satisfactory; Wood (2014), p. 452, even proposes a general reform of applicable international law, mainly through the conclusion of an international domain name treaty. In such case, the right to a local identity could be included as a limit on the practice of the registration and use of domain names.

[56]WIPO, Geneva Act of the Lisbon Agreement on Appellations of Origin and Geographical Indications and Regulations Under the Geneva Act of the Lisbon Agreement on Appellations of Origin and Geographical Indications, (2015), http://www.wipo.int/meetings/en/details.jsp?meeting_id=35202; see Gervais (2015).

renowned names and domain names that are registered and used in good faith before the protection granted to the geographical term.

5 Conclusion

Domain names are recognised by law as assets, protected as part of (immaterial) property, in a way that brings them closer to trademark law, and up to a certain point, to geographical indications. Nevertheless, for geographical indications that are registered and used as part of a domain name, the relevant question is not the protection of the property rights related to domain names, but the enjoyment of the use of a geographical indication as a domain name. The case of European law demonstrates the limits of regional systems of enhanced protection. Cyberspace is global, as is the threat to geographical indications through misuse in the field of domain names. Negotiations on a case-by-case basis cannot guarantee equitable results, especially in light of the power of economic operators intervening in the market of domain names, compared to the weak or perhaps nonexistent capacities of local authorities and/or producers at the international level. The reform of international law based on the principle of distributive justice and the progressive assessment of a right to local identity, in opposition to the misleading and abusive registration and use of geographical indications as domain names, is both conceivable and necessary.

References

Audier J (1993) De la nature juridique de l'appellation d'origine. Bull de l'OIV 743–744:21

Berard L (2016) Terroir and the sense of place. In: Gangjee DS (ed) Research handbook on intellectual property and geographical indications. Edward Elgar, p 72

Blakeney M (2014) The protection of geographical indications – law & practice. Edward Elgar

Clowers J (2006) On international trademark and the internet: the Lanham's Act's Long Arms". Richmond J Law Technol 13:1

Dinwoodie GB (2014) (National) trademark law and the (non-national) domain name system. J Int Law 21:495

Forrest HA (2013) Geographical names, their protection in international law and ICANN domain name system policy. Kluwer Law International

Gangjee DS (2015) Geographical indications and cultural rights: the intangible cultural heritage connection? In: Geiger C (ed) Research handbook on human rights and intellectual property. Edward Elgar, p 544

Georgopoulos T (2014a) France. In: Waye V, Harvey M (eds) Global wine regulation. Thomson Reuters, p 361

Georgopoulos T (2014b) L'européanisation de la notion juridique de terroir. In: Georgopoulos T (ed) Les appellations d'origine vitivinicoles à l'épreuve de l'intégration européenne. Mare & Martin, p 13

Gervais D (2015) Irreconcilable differences? The Geneva act of the lisbon agreement and the common law. Houston Law Rev 53:339

Geuze M (2016) Geographical indications under WIPO-administered treaties. In: Gangjee DS (ed) Research handbook on intellectual property and geographical indications. Edward Elgar, p 95
Goebel B, Groeschl M (2016) Learning to love my PET – the long road to resolving conflicts between trademarks and geographical indications. In: Gangjee DS (ed) Research handbook on intellectual property and geographical indications. Edward Elgar, p 361
Josling T (2006) The war on terroir: geographical indications as a transatlantic trade conflict. J Agric Econ 57:337
Lindsay D (2007) International domain name law. Hart
Omond J, Waye V(2014) Labelling: Australian and United Kingdom perspectives. In: Harvey M, Waye V (eds) Global wine regulation. Thomson Reuters, p 189
Mendelson R, Gerien S (2011) Wine brands and appellations of origin. In: Mendelson R (ed) Wine in America – law and policy. Wolters Kluwer, p 217
Nussbaum M (2006) Frontiers of justice. Belknap
Rawls J (2001) Justice as fairness – a restatement. Belknap – Harvard
Sypnowich C (2005) Cosmopolitans, cosmopolitanism, and human flourishing. In: Brock G, Brighouse H (eds) The political philosophy of cosmopolitanism. Cambridge University Press, p 55
Tredinnick-Rowe J, Taylor T (2015) The use of local culture and sustainability in local food and beverage entrepreneurship. In: Sloan P, Legrand W, Hindley C (eds) The Routledge handbook of sustainable food and gastronomy. Routledge, p 96
Wilson TM (2006) Food, drink and identity in Europe: consumption and the construction of local, national and cosmopolitan culture. In: Wilson TM (ed) Food and drink identity in Europe, European studies, Vol 22. Rodopi, p 11
Wood L (2014) A name of thrones – why domain names should now be a separate intellectual property right. Eur Intell Property Rev 36:452

Part IV
Internet, New Media and Human Rights

Chapter 14
The Right of Journalists Not to Disclose Their Sources and the New Media

Costas Stratilatis

Abstract This chapter deals with the issue of whether the right of journalists not to disclose their sources should be extended to protect the various 'citizen journalists' of the New Media. After expounding some jurisprudential attempts to confront this issue in the USA and after tracing the restrictive tendencies in the available instruments of the Council of Europe, this chapter examines and criticizes a recent attempt to escape this problem focusing on the 'source' rather than on the 'journalist'. Returning back to the traditional context of the debate, in its last section, this chapter proposes an enlargement of the traditional concept of 'journalist' to provide protection to all persons who disseminate information to the public through the use of New Media, provided that these persons had the intent to do so (i.e. to disseminate information) already at the inception of the information-gathering process.

1 Introduction

Considered as essential to the freedom of the press and the right of the public to be informed,[1] the right of journalists not to disclose information that might lead to identification of their sources (i.e. the persons who provide them with information in the context of the newsgathering process) has acquired worldwide protection under specific international law instruments and domestic law provisions.[2]

[1] See in general Barendt (2005), pp. 435–441, and Sect. 4 of this chapter.

[2] For a comprehensive survey, see Banisar (2007). International law instruments include the Inter-American Declaration of Principles on Freedom of Expression (Principle 8), approved by the Inter-American Commission on Human Rights at its 108th regular sessions in October 2000; the Declaration of Principles on Freedom of Expression in Africa (Art. XV), approved by the African Commission on Human and Peoples' Rights at its 32nd session in October 2002; and Recommendation (2000) 7 of the Committee of Ministers of the Council of Europe, to which reference shall be made in Sect. 3. Domestic legal protection is provided either through constitutional (see e.g. Art. 38.2 of the Constitution of Portugal) or, most commonly, through legislative provisions

C. Stratilatis (✉)
University of Nicosia, 46 Makedonitissis Avenue, Engomi, Cyprus
e-mail: stratilatis.c@unic.ac.cy

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_14

Starting from the landmark *Goodwin* case in 1996,[3] the European Court of Human Rights (ECtHR) has recognized this right under Article 10 of the European Convention of Human Rights (ECHR), concluding that it could be invoked not only against orders of courts or of other public authorities, which are particularly directed to disclosure of sources,[4] but also against searches of journalists' homes or workplaces and/or seizure of their materials by the police,[5] as well as against secret surveillance of journalists' communications,[6] even when the aim of the investigative authorities is other than disclosure of the source.[7] Protection of journalistic sources under Article 10 of the ECHR is not absolute but qualified by certain conditions, which if met, can justify the interference. Such conditions include quality of the relevant law (accessibility and foreseeability, adequate safeguards against arbitrary interferences, limits on the discretion of the authorities)[8]; review by a judge or by any other independent and impartial decision-making body, having the capacity to decide upon the matter before the interference takes place[9]; pursuance of a legitimate aim under paragraph 2 of Article 10 of the ECHR, in a way that is deemed necessary in a democratic society—the typical balancing

(see e.g. the French Loi n° 2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes, also section 10 of the Contempt of Court Act 1981 in the UK).

[3]ECtHR (Grand Chamber), *Goodwin v. the United Kingdom*, App No 17488/90, 27 March 1996. All judgments of the ECtHR have been retrieved from the HUDOC database.

[4]Apart from the *Goodwin v. the United Kingdom* judgment, see also ECtHR (Grand Chamber), *SanomaUitgevers B.V. v. the Netherlands*, App No 38224/03, 14 September 2010, ECtHR, *Voskuil v. the Netherlands*, App No 64752/01, 22 November 2007; ECtHR, *Financial Times Ltd and Other v. the United Kingdom*, App No 821/03,15 December 2009; ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, App No 39315/06, 22 November 2012.

[5]See ECtHR, *Roemen and Schmitt v. Luxembourg*, App No 51772/99, 25 February 2003; ECtHR, *Ernst and Others v. Belgium*, App No 33400/96, 15 July 2003; ECtHR, *Tillack v. Belgium*, App No 20477/05, 27 November 2007; ECtHR, *Martin and Others v. France*, App No 30002/08, 12 April 2012; ECtHR, *Ressiot and Others v. France*, App No 15054/07 and 15066/07, 28 June 2012; ECtHR *Saint-Paul Luxembourg S.A. v. Luxembourg*, App No 26419/10, 18 April 2013; ECtHR, *Nagla v. Latvia*, App No 73469/10 16 July 2013; ECtHR, *Görmüş and Others v. Turkey*, App No 49085/07, 19 January 2016. Searches and seizure cases are sometimes examined under both Art. 10 and Art. 8 (respect for private life) ECHR.

[6]See ECtHR, *Ressiot and Others v. France*, also ECtHR (admissibility), *Weber and Saravia v. Germany*, App No 54934/00, 29 June 2006. In this latter case, the ECtHR held that surveillance of telecommunications constitutes a *prima facie* interference with protection of journalistic sources under Art. 10 ECHR (par. 144–146), but it rejected the applicants' complaint because the relevant provisions of German law contained adequate safeguards (par. 150–153).

[7]See on this particularly ECtHR (Grand Chamber), *SanomaUitgevers B.V. v. the Netherlands*., par. 65–72, with extended references to the relevant findings of earlier judgments, also ECtHR, *Telegraaf MediaNederland Landelijke Media B.V. and Others v. the Netherlands*,, par. 86–87.

[8]See e.g. ECtHR (Grand Chamber), *Goodwin v. the United Kingdom,* par. 81, ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, par. 89–91, ECtHR (adm.), *Weber and Saraviav. Germany*, par. 92–95.

[9]See e.g. ECtHR (Grand Chamber), *Sanoma Uitgevers B.V. v. the Netherlands*, par. 90–98, ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, par. 99–101; *Nagla v. Latvia*, par. 87–90.

exercise focuses on whether alternative measures existed for the authorities to acquire the information that was sought for,[10] and the authorities need to prove that the circumstances were of a sufficiently vital and serious nature and that an overriding public interest really existed, justifying the need for the disclosure.[11]

In the USA, where the right of journalists not to disclose their sources is commonly termed as 'reporter's' or 'journalist's privilege', the specification of the level of protection is more perplexed. In the landmark 1972 judgment *Branzburg v. Hayes,*[12] the Supreme Court refused to assert the journalist's privilege under the First Amendment, which as well-known guarantees freedom of speech and freedom of the press, and it has since then refused to hear such cases.[13] However, *Branzburg* was taken by a narrow majority of 5 to 4 judges, and the decisive, yet enigmatic, concurring opinion of Justice Powell left the space open for several federal courts to recognize a (more or less) qualified First Amendment protection of the privilege (the relevant trend in Federal Circuit Courts was initially favorable to the press, but it started to turn against it since late 1990s).[14] Besides, the majority of United States have up to now introduced legislative clauses, so called 'shield laws', providing for qualified or even absolute protection of the reporter's privilege, while in some other states the privilege is protected under common law or under courts' rules of

[10]See e.g. ECtHR, *Roemen and Schmitt v. Luxembourg*, par. 56; *Ernst and Others v. Belgium*, par. 102; *Martin and Others v. France*, par. 86; *Voskuil v. the Netherlands*, par. 58-62; *Saint-PaulLuxembourg S.A. v. Luxembourg*, par. 44.

[11]See e.g. ECtHR (Grand Chamber), *Goodwin v. the United Kingdom*, par. 39-40, ECtHR, *Tillack v. Belgium*, par. 60–67; *Naglav. Latvia*, par. 94–102.

[12]*Branzburg v. Hayes* 408 U.S. 665 (1972). For a detailed presentation of the litigation in *Branzburg,* see among others Andersen Jones (2013), pp. 1231–1237.

[13]Such refusal has recently been affirmed in the Risen and Sterling case. See Liptak (2014), *United States of America v. Sterling*, F.3d 482 (4th Cir. 2013), and Konarski (2014–2015), with a scholarly discussion to the effect that the Supreme Court should revisit *Branzburg* in view of the Risen and Sterling case. The latter concerned the refusal of Risen, a national security reporter of New York Times, to reveal the identity of Sterling, a former CIA employee, as his source for writing articles and a book on the plans and activities of CIA. Another famous case in which federal courts refused protection under the privilege was *In re Grand Jury Subpoena, Judith Miller*, 397 F.3d 964 (D.C. Cir. 2005).

[14]For presentation see among others Campagnolo (2002–2003), pp. 478–491, Fargo (2005–2006), pp. 1078–1102, Dalglish and Murray (2006–2007), Ugland (2010), pp. 17–34, Rosenbaum (2013–2014), pp. 1439–1446. For the assertion of the privilege under Federal Rule of Evidence 501, see Nestler (2005–2006), Papandrea (2007), pp. 559–564; but see also Campagnolo (2002–2003). The Federal Courts, which recognize a journalist's privilege under the First Amendment, qualify it following some variation of the three-factor test that the dissenting opinion of Justice Stewart in *Branzburg* had proposed. According to this test, 'the government must (1) show that there is probable cause to believe that the newsman has information that is clearly relevant to a specific probable violation of law; (2) demonstrate that the information sought cannot be obtained by alternative means less destructive of First Amendment rights; and (3) demonstrate a compelling and overriding interest in the information'. See *Branzburg v. Hayes*, 408 U.S. 665, 743 (1972).

procedure.[15] This variation, combined with the failure to pass a federal shield law through Congress, despite repeated attempts to do so after persistent calls by media organizations and scholars,[16] create an environment of uncertainty for journalists and sources, as well as for the courts and the legal system at large.[17]

Such uncertainty is enhanced by the rise of new types of public communication that are often labeled as 'citizen journalism'.[18] Relevant examples are 'wiki-news' created by persons not regularly engaged in journalism with the purpose of providing information (reporting material, video footages etc.) on the evolution of specific events, crises or issues; bloggers who are not associated with a media organization and who regularly post information, stories, comments etc. on topics of public interest; web-platforms, such as Wikileaks,[19] which host leaked governmental documents; the social media pages of non-journalists who regularly post the fruits of their research and/or their personal opinion on public interest issues; electronic newsletters by non-journalistic organizations; posts and comments under articles which are published on web-news portals; etc. Are these people, imparting information through the aforementioned media, entitled to claim the right not to disclose their sources, irrespective of their professional identity, regular activity and/or actual capacity as journalists?

Indeed, a lot depends upon the particular circumstances of each case, and upon the wording of the applicable legal provisions. Nevertheless, the literal or plain meaning of these provisions is often such that it cannot provide a definite answer. Some state statutes in the USA include terms such as 'electronic', 'Internet', 'digital' or 'online',[20] but in most cases such terms are absent. The legislature

[15]For a map with links to the relevant provisions and jurisprudence in each state, see the digital Compendium of Reporter's Privilege (2016). See also the comprehensive surveys of Martin and Fargo (2013), pp. 53–65, and Papandrea (2007), pp. 545–551, 564–567.

[16]See e.g. Stone (2005–2006), Alonzo (2005–2006), pp. 778–779, Gomsak (2006–2007), Turner (2011), Martin and Fargo (2013), pp. 93–94, Rosenbaum (2013–2014), Tursi (2014), Harris (2013–2014), pp. 1822–1824. However, see also Eliason (2006–2007) (arguing that a federal shield law would not alleviate the problem and that it would anyway provide for an overly qualified privilege, not suitable to carry out its assumed function), Castiglione (2007) (offering a 'structuralist' critique of the privilege and expressing doubts with reference to the risks of its legislative entrenchment). Attempts to pass a federal shield law were intensified once more after the refusal of the Supreme Court to hear the Risen case; see Gierhart (2014).

[17]See e.g. Stone (2005–2006), pp. 43, 45, Rosenbaum (2013–2014), p. 1458, Tursi (2014), pp. 224 et seq. For an empirical study on the effect of the absence of a federal shield law on the amount of subpoenas received by journalists and by media organizations, see Andersen Jones (2008–2009).

[18]See in general Wall (2012), Allan and Thorsen (2009), and for the manifesto of grassroots online journalism Gillmor (2004). The terms 'citizen journalism' and 'citizen journalists' are commonly used by legal scholars discussing the problem of the journalist's privilege; see e.g. Papandrea (2007), Turner (2011–2012), Rosenbaum (2013–2014).

[19]Wikileaks is a media-organization that specializes in on-line publication of "censored or otherwise restricted official materials" of public interest. See https://wikileaks.org/What-is-Wikileaks.html. Accessed 7 May 2017.

[20]See Martin and Fargo (2013), p. 65, Papandrea (2007), pp. 564–565.

typically adopts a relatively broad definition of the 'journalist' (standard definitions refer (a) to activities such as gathering, receiving, collecting, compiling, writing, editing, photographing, recording, processing etc. information; and/or (b) to the purpose of transmitting, disseminating and/or publishing this information to the public; and/or, less frequently, (c) to the type of engagement of the person to his/her activity, i.e. professional or not, freelance or not etc.), usually coupled by a definition of a 'news medium', which lists traditional means of dissemination (print, television, radio, broadcast, audiovisual etc.) in an exhaustive or, more often, in a non-exhaustive way, i.e. including an 'and any other means or medium' clause.[21] Thus, in many cases the prospect of acknowledging the right of a person who disseminates information through online periodicals or blogs not to reveal his/her source would remain open, despite the fact that this person is not a journalist as traditionally understood.

Besides, even in cases in which the definition of the 'journalist' and/or of the 'news medium' is quite restrictive (this is the case e.g. of the French Loi n° 2010-1 du 4 janvier 2010, which, notwithstanding its reference to online communication, defines the 'journalist' as a professional, that is, 'any person who, exercising his/her profession in one or more press enterprises, online communication, audiovisual communication or in one or more press agencies, exercises, in a regular and paid way, the practice of collecting information and disseminating them to the public'[22]), one could still vindicate the application of the relevant provisions to non-journalists through interpretation by analogy. In such cases, as well as in cases in which the relevant provisions leave, by themselves, open the prospect of protecting non-journalists, legal argumentation may appeal to considerations which have to do with the rationale behind the right of journalists not to disclose their sources traditionally understood (i.e. as such right refers to classic media journalists).

In the next section, this chapter reviews some jurisprudential attempts to deal with this problem in the USA, while in Sect. 3 the same issue is examined in the context of various Council of Europe's Recommendations. Although the problem has not arisen in the jurisprudence of the ECtHR, as it will be shown, these instruments indicate a restrictive approach regarding a possible extension of the right of journalists not to disclose their sources in the field of New Media 'citizen journalism'. In Sect. 4, this chapter shows that these restrictive tendencies can be connected with the famous 'chilling effect' doctrine, which underpins the traditional, functional-utilitarian and institutional justification of the right of journalists not to disclose their sources under the fundamental right of freedom of speech and of the press. In Sect. 5, a recent attempt to escape the traditional approach by

[21]See Compendium of Reporter's Privilege (2016), Martin and Fargo (2013), pp. 53–65, Papandrea (2007), pp. 564–567.

[22]Loi du 29 juillet 1881 sur la liberté de la presse, Art. 2, as amended by Loi n° 2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes, Art. 1, Free translation, Accessed 23 Nov. 2016.

focusing on the 'source' rather than on the 'journalist' is expounded. This source-oriented approach has important advantages, especially when the problem is treated at hand as a matter of judicial investigation. Nevertheless, as it is argued in Sect. 6, when the problem is treated in the broader context of public policy, one may not so easily sidestep the traditional framework of analysis and its focus on the journalist and its 'chilling-effect' concerns. This chapter concludes with a proposal regarding the possible legislative extension of the right of journalists to cover the 'citizen journalists' of the New Media.

2 The Journalist's Privilege and the New Media in USA Jurisprudence

2.1 Court Judgments

In the USA, the problem of the journalist's privilege in the New Media has been occupying the courts and legal scholarship for more than a decade.[23] In the 2006 judgment *O'Grady v. Superior Court*[24] the California Court of Appeal ruled that protection under the reporter's privilege covered two online-only news magazines, which were sued by Apple for misappropriating trade secrets related with the imminent release of a new product. The relevant clause of the California Constitution (Art. I, s. 2) reads as follows: 'A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication ... shall not be adjudged in contempt ... for refusing to disclose the source of any information procured while so connected or employed for publication in a newspaper, magazine or other periodical publication ...'. The Court held that the online periodical fell within this clause, noticing first that '[n]ews sites such as petitioners' reflect a kind and degree of editorial control that makes them resemble a newspaper or magazine far more closely than they do the primordial discussion systems that gave birth to the term "post" by analogy to the physical bulletin boards they were named and patterned after'.[25] Posting of material to the online periodical was found to be 'conceptually indistinguishable from publishing a newspaper',[26] and it should be distinguished from 'deposit of information, opinion, or fabrication by a casual visitor to an open forum such as a newsgroup, chatroom, bulletin board system, or discussion room',[27] which 'may indeed constitute something other than

[23] See among others Alonzo (2005–2006), Papandrea (2007), Toland (2009), Kirtley (2009–2010), Turner (2011–2012), Clark and Barnette (2012), Martin and Fargo (2013), Andersen Jones (2013), pp. 1270–1281, Rosenbaum (2013–2014), Harris (2013–2014).

[24] *O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006).

[25] *Ibid* at 91–92.

[26] *Ibid* at 99.

[27] *Ibid* at 99.

the publication of news'[28] and which could thus be dealt with differently.[29] However, this distinction should not be connected with the newsworthiness of the publication at hand. Indeed, the Court rejected Apple's contentions to this effect, finding that a distinction between 'legitimate' and 'illegitimate' news would have imperiled the protection of freedom of speech and of the press under the First Amendment.[30] Finally, using various methodological tools to interpret the phrase 'newspaper, magazine, or other periodical publication' of the California Constitution, the Court concluded that the absence of direct reference to digital media did not mean that these were and should be excluded from protection.[31] In reaching this conclusion, the Court held that websites as the petitioners' are 'highly analogous to printed publications'[32] (indeed, the Court found that web publications bear much more resemblances to traditional print media than radio and television do).[33] To assimilate the web site with traditional periodicals, the Court gave particular emphasis to the frequency of the publication.[34]

A similar line of argumentation was followed in the 2012 Illinois case *Johns-Byrne Co. v. TechnoBuffalo*,[35] which again concerned a digital-only news blog's publication of information that could be considered a violation of confidential trade secret rules. In this case the statutory definition of 'news medium' included the term 'electronic format', while the statute did not provide a definition of 'news'. This left open space for the Court to dismiss the attempt of the respondents to introduce a distinction between 'legitimate' and 'illegitimate' news (the Court cited the *O' Grady* judgment in this respect).[36]

Besides, in the 2010 case *Mortgage Specialists, Inc. v. Implode-Explode Heavy Industries, Inc.*,[37] the Supreme Court of New Hampshire held that a website which focused on the assessment and ranking of various businesses in the mortgage industry 'serves an informative function and contributes to the flow of information to the public',[38] thus, it 'is a reporter for purposes of the newsgathering privilege'[39]

[28] *Ibid* at 99.

[29] *Ibid.* at 100.

[30] *Ibid.* at 97.

[31] *Ibid.* at 100–105.

[32] *Ibid.* at 103.

[33] *Ibid.* at 102.

[34] *Ibid.* at 104–105.

[35] *Johns-Byrne Company v. TechnoBuffalo LLC, et al.*, Order, Case No. 2011 L 009161 (Ill. Cir. Ct. July 13, 2012),http://www.dmlp.org/threats/johns-byrne-company-v-technobuffalo. Accessed 15 May 2016.

[36] *Ibid.* at 5–6.

[37] 999 A.2d 184 (N.H. 2010).

[38] *Ibid.* at 189.

[39] *Ibid.* at 189.

under Part I, Article 22 of the New Hampshire Constitution.[40] Then, the Court followed the applicable Circuit Court of Appeals balancing test, which in civil cases qualified the reporter's privilege upon showing (a) that the information sought is critical to plaintiff's claim, and (b) that the information is not available from other sources.[41]

On the other hand, in the 2011 defamation case *Too Much Media v. Hale*,[42] the Supreme Court of New Jersey ruled that a person who had posted extended commentaries on an online message board was not covered by the privilege under the relevant state shield law. The commentaries were related with an investigation of online pornography that the defendant had undertaken in the past, and the defendant claimed that she had the intention to create her own news-oriented website, which would be dedicated to information on this issue, but her project was never launched.[43] This failure proved to be crucial, as the Court discarded the defendant's claim that she was involved in a 'journalism-in-progress' process for the privilege.

In *Too Much Media,* the relevant statutory provisions were indeed very broad as regards the level of protection[44] and the scope of the activities that were protected.[45] The Court held that 'some nexus, relationship, or connection to "news media"' is required for a person to be protected by the privilege',[46] and that the self-characterization of a person as a journalist would not be sufficient in this respect.[47] Besides, although the Court argued that the form of dissemination could not alone determine what may count as 'news medium', it concluded that there must be some similarity to 'newspapers, magazines and the like'.[48] With regard to the issue of similarity, the Court held that, although 'online message boards provide virtual, public forums for people to communicate with each other about topics of interest',[49] such boards 'are not the functional equivalent of the types of news media outlets outlined in the Shield Law. Neither writing a letter to the editor nor posting a comment on an online message board establishes the

[40] *Ibid*. at 189.

[41] *Ibid*. at 190–191, citing *Bruno & Stillman, Inc. v. Globe Newspaper Co*., 633 F.2d 583, 594.

[42] *Too Much Media v. Hale* 20 A.3d 364 (N.J. 2011).

[43] *Ibid.* at 369 et seq.

[44] The Court itself took the privilege to be absolute in civil defamation and libel cases, *ibid*. at 383. We believe that this played a role to the Court's hesitant stance as regards the expansion of the privilege to the activity of posting extended commentaries (indeed, in the form of articles) to the message board of another person.

[45] The Court assessed the shield law as one 'among the broadest in the nation', *ibid*. at 375.

[46] *Ibid*. at 376. According to the Court's interpretation of the relevant statutory provisions, such nexus need not be taken as equivalent to being employed by or to having a direct tie to a traditional medium.

[47] *Ibid*. at 377–378.

[48] *Ibid*. at 378.

[49] *Ibid*. at 378–379.

connection with "news media" required by the statute'.[50] Therefore, the defendant could not claim protection under the privilege, despite her intention to act as an online journalist.[51]

In this respect, the Court refused to apply the 'intent test', which several Federal Circuit Courts had adopted to determine the scope of the privilege.[52] According to this test, 'people seeking protection under the federal journalist's privilege ... [must] show "that they: 1) are engaged in investigative reporting; 2) are gathering news; and 3) possess the intent at the inception of the newsgathering process to disseminate this news to the public"'.[53] One should note that this test was used in cases in which courts firstly held that the type of medium was irrelevant for the privilege.[54]

The *Too Much Media* Court also proceeded into a more general call for caution and scrutiny in cases involving 'self-appointed journalists or entities with little track record who claim the privilege . . .[T]he popularity of the Internet has resulted in millions of bloggers who have no connection to traditional media [citation omitted]. Any of them, as well as anyone with a Facebook account, could try to assert the privilege. In those cases, a more probing hearing would likely be needed to determine if the privilege applies'.[55] Nonetheless, courts should apply the following standards: 'connection to news media; purpose to gather or disseminate news; and a showing that the materials sought were obtained in the course of professional newsgathering activities'.[56]

2.2 Scholarship

Analyzing the aforementioned cases, Martin and Fargo (2013) observe that 'these courts have made a central consideration of whether the website is gathering and disseminating news to the public versus blogs run by individuals that contain mostly personal reflection and opinion that more closely resembled interpersonal conversation'.[57] Thus, these scholars seem to favor the distinction adopted by *O'Grady* between (a) publications which reflect a process that could be assimilated

[50] *Ibid.* at 379. At this point, the Court distinguished *Too Much Media* from *O'Grady*, based on the distinction of the latter between news-oriented websites and the deposit of information or opinion by casual visitors to open fora. *Ibid.* at 379–380.

[51] *Ibid.* at 380 et seq.

[52] *Ibid.* at 373–374, 380–381.

[53] *Ibid.* at 380, quoting *In re Madden,* 151 F.3d 125, 131 (3d Cir. 1998).

[54] See *In re Madden*, at 129–130, *Schoen v. Schoen*, 5 F.3d 1289, 1293 (9th Cir. 1993), *von Bulow v. von Bulow*, 811 F.2d 136, 142–143 (2d Cir. 1987), retrieved from the LexisNexis database.

[55] *Too Much Media v. Hale* 20 A.3d 364, 383 (N.J. 2011).

[56] *Ibid.*, at 383.

[57] Martin and Fargo (2013), p. 85.

to journalistic work and (b) casual posting of personal opinions.[58] In general, Martin and Fargo (2013) favor a 'medium neutral, process-centered approach'[59]; one which will focus less on the definition of the persons and of the media that are covered and more on the newsgathering and dissemination process, with a view to achieve an adaptation of the constitutional rationale underpinning the journalist's privilege to the new realities of digital journalism.[60] Their final suggestion is a call for legislative action. The legislature should 'focus on the philosophical roots of the journalist's privilege and craft laws that reflect what actions are performed in newsgathering instead of who journalists are or with whom they are affiliated'.[61]

Earlier on, discussing the scope of the reporter's privilege in a more general context, Berger (2002–2003) had also rejected the relevance of criteria connected with (a) the employment status, the education, the professional training or the regular engagement of journalists with established news media; (b) the content i.e. the newsworthiness of the information that is disseminated; (c) and the type or format of the medium.[62] Instead, Berger advocated a functional definition of the journalist, focusing on the process of journalism and on the presence of elements such as (a) the regularity and the public character of the information that is disseminated; (b) internal evaluation and verification measures; and (c) availability of information regarding sponsors, ownership and editorial standards so as enable the readers to check the publisher's or the reporter's independence.[63]

Discussing the same problem in the more particular context of 'citizen journalism', Papandrea (2007) rightly noticed that Berger's approach 'unconstitutionally interfere[s] with the editorial process',[64] and that it is still excessively restrictive, insofar as it reserves the privilege only for 'those whose contribution to the public debate resemble those of the "ideal" journalist who is part of traditional, mainstream media. Although it is desirable for all those who contribute to public debate to have verification procedures, regular dissemination (rather than the haphazard publication of many online contributors), and transparency of ownership, motives, and editorial standards, regrettably even some professional journalists eschew these guidelines'.[65]

Papandrea (2007) adopted a medium neutral approach, and furthermore argued that, if we focus on the 'underlying purposes of the privilege' (which are taken to be connected with the increase of 'the amount of information in the public domain' and with avoidance of a situation in which all relevant actors would be turned into

[58] *Ibid,* p. 93.
[59] *Ibid*, p. 92.
[60] *Ibid*, pp. 89–93.
[61] *Ibid*, p. 93.
[62] Berger (2002–2003), pp. 1406–1411.
[63] *Ibid*, pp. 1411–1416.
[64] Papandrea (2007), p. 583.
[65] *Ibid*, p. 583.

'investigators for the government and private parties'), then we would be led to a 'broad conception' according to which 'the privilege should not be limited to those who are serving as traditional journalists; rather it should extend to anyone who is contributing to the marketplace of ideas by disseminating information to the public'.[66] More specifically, she argued that all these persons should 'have a presumptive qualified right'[67] not to disclose their sources unless the other party shows that '(1) the desired information is critical to the maintenance of . . . [his/her] claim, defense, or proof of an issue; (2) the information sought cannot be obtained by alternative means; and (3) there is a compelling interest in the information that outweighs the public's interest in the free flow of information'.[68]

However, qualifications do not stop at this point. Papandrea (2007) made a distinction between confidential and non-confidential sources, arguing that protection of the latter should be somehow less, insofar as '[f]orcing the unmasking of a nonconfidential source is less likely to discourage that source from speaking to a journalist in the future'.[69] Besides, 'the privilege should be defeated if a party seeking the information proves that the case falls within one of the following exceptions: (1) the subpoena is directed to someone who witnessed or participated in criminal or tortuous activity (excluding the crime of leaks of classified or national security information); (2) compelling testimony is warranted by a direct and imminent threat to national security; (3) the subpoena is directed to a person or entity that is a defendant in a defamation or invasion of privacy action, provided that the plaintiff makes a certain showing of necessity and likelihood of success; or (4) the subpoena is directed at an individual who engaged in publication solely in an effort to avoid a subpoena'.[70]

Such broad exceptions somehow relativize Papandrea's expansive approach as regards the scope of the privilege in reference to 'citizen journalism'. Especially, the national security exception could be abused by the government and by courts that might be afraid of being conceived as acting against the nation's interests.[71] This issue relates to Wikileaks, the well-known website which has been publishing classified government documents and whose inclusion or exclusion from protection

[66] *Ibid*, pp. 519–520.

[67] *Ibid*, p. 584.

[68] *Ibid*, p. 584.

[69] *Ibid*, p. 585.

[70] *Ibid*, p. 585.

[71] See Harris (2013–2014), p. 1847, referring to Davidson and Herrera (2011–2012), p. 1312. In a more recent publication, Papandrea (2011–2012, p. 129) argued that '[t]he dissemination of information by nongovernment actors should be punishable only if the offender acted with the intent to harm the United States or with reckless indifference to such harm. This sort of intent standard would provide protection for all responsible publishers acting in good faith, no matter who they are or what medium they use for communication'.

under the privilege has occupied a significant space in legal scholarship in the USA in recent years.[72]

2.3 The Wikileaks

The discussion here has been focused on the question of whether Wikileaks' agents and activities fulfill the Federal Circuit Courts' criteria regarding 'investigative reporting' and 'dissemination of news'.[73] Using relevant case law, Peters (2010–2011) argued that '[i]nvestigative reporting involves more than the mere dumping of documents'[74]; that is a process which includes in depth long-term research and/or multiple-article reporting, taking interviews, keeping notes, storytelling, interpretation or analysis of the facts which are presented etc. 'In contrast, the backbone of Wikileaks is a high-security drop box that allows people anonymously to submit documents for the site's staff to review'.[75] Despite the fact that Wikileaks verifies the authenticity of the documents which are received and then posts them along with a news story, the latter plays rather the role of a 'press release, announcing what the site has done, to enable an outside reporter to write about it'.[76] When some 400,000 classified documents about the Iraq War were released, Wikileaks offered just a short cover story that 'was not thorough. It did not feature any response from the U.S. government, it did not chronicle the life-and-death decisions lurking in the documents, or offer color or texture, or illuminate the human condition, other than the death toll. In addition, it failed to distinguish between opinion and news, not the first time the website had blurred that line'.[77] Thus, 'for privilege purposes the website is not engaged in investigative reporting'.[78]

In the same vein and reaching the same conclusion, Clark and Barnette (2012) contended that '[i]nvestigative journalist is often labeled "watchdog journalism," which generally involves the following, investigating, and development of a story over a period of time in order to ascertain the facts, uncover the truth, and disseminate that truth to the public at large…Wikileaks fails to undertake any journalistic or literary endeavor. Merely playing the role of a Xerox machine does not constitute creation. While Wikileaks verifies the stories and documents leaked

[72]See among others Peters (2010–2011), Davidson and Herrera (2011–2012), Clark and Barnette (2012), Harris (2013–2014). For a more general account of the legal problems and answers regarding Wikileaks under the First Amendment, see Benkler (2011).

[73]See the cases referred to in n54 above, and *Cusumano v. Microsoft*, 162 F.3d 708 (1st Cir. 1998). The relevant criteria have been presented in n53 above.

[74]Peters (2010–2011), pp. 676–683.

[75]*Ibid*, p. 679.

[76]*Ibid*, pp. 679–680.

[77]*Ibid,* p. 681.

[78]*Ibid*, p. 683.

to it, this alone is a far cry from the investigative journalism outlined by *Bulow* and *Madden*, as well as the subsequent cases that followed these decisions, in identifying the "legitimate press' the law was concerned in protecting'.[79]

This is indeed a traditional and, at the same time, an overly demanding portrayal of investigative reporting; one which even traditional media organizations could hardly fit with, at least as regards the bulk of their publications, which are often not based on in-depth, long-term research and following of a story, while it is debatable whether editorial judgment-making takes place in each and every case. From the standpoint of the First Amendment principles, the approach of Peters, Clark and Barnette falls into the 'trap' of distinguishing between 'worthy' and 'unworthy' journalism, conditioning protection upon assessments which are related, if not directly with the content of certain publications, with the evaluation of such content in accordance with standards of 'legitimate' newsgathering and dissemination. At the same time, these scholars underestimate the contribution of Wikileaks to the 'watchdog function',[80] which all media organizations, traditional or non-traditional, are supposed to fulfill under the First Amendment principles of the USA Constitution.

Avoiding these 'traps', other scholars have been favorable to the case of protecting Wikileaks under the journalist's privilege. For instance, Benkler (2011) argues that, for First Amendment purposes, we should focus on the intent to disseminate to the public, 'as distinguished from research for private use'[81]; while the more particular motivations of the person who disseminates information should taken to be irrelevant. According to Benkler (2011), '[a] journalist is not measured by whether she investigates and publishes in order to serve democracy, aggrandize her name, or make money . . . As a matter of First Amendment values, what is being protected by this continued refusal to privilege the *New York Times* over Wikileaks is the continued access of the public to a steady flow of a truthful, publicly relevant information about its government's inner workings. As the networked public sphere develops . . . the functional importance of divorcing the constitutional protection from the degree to which the actor is a familiar part of the twentieth century model of mass media increases'.[82] Medium neutrality is correctly taken here to help avoid undermining the First Amendment principles through the creation of 'classes of privileged speakers and press agencies, and underclasses of networked information producers whose products we take into the public sphere

[79]Clark and Barnette (2012), pp. 178–179.

[80]The term 'watchdog function' is a classic one in the jurisprudence and in the public debate which is related with the First Amendment and with freedom of the press in the USA. The term generally indicates the crucial role of the media in checking the Government, either directly (e.g. through investigative journalism, through interviewing of public officials, through fact-checking of their statements etc.) or indirectly (through creating an informed public).

[81]Benkler (2011), pp. 359–362.

[82]*Ibid*, pp. 361–362.

when convenient, but whom we treat as susceptible to suppression when their publication become less palatable'.[83]

Analyzing the case-law on the meaning of 'investigative journalism', Harris (2013–2014)[84] points out that, in contrast to what Peters believes, the core of it is concerned with the mere fact of reporting, and not with the question of whether the reporter provided an analysis or conducted in-depth research. Besides, according to Harris (2013–2014), even if we adopt the demanding image of journalism which is promoted by the scholars who deny protection to Wikileaks, the latter could still be regarded as falling under the term 'investigative journalism', insofar as it filters the documents received, to decide which ones deserve publication, it verifies their authenticity, thus there is some editorial overview, while the Wikileaks' spokesmen often publicly comment the material which has been published.[85]

The above discussions show that, although accepted by all in principle, the First Amendment values, and medium-neutrality as a background assumption for the realization of these values, are much harder to achieve when treating the case of 'citizen journalism' than is at first glance believed. Illegitimate distinctions between 'worthy' or 'unworthy' journalism lurk at every corner of the attempt to define the scope of the privilege. However, some distinctions seem to be unavoidable, if one attempts to draft a definition. Alternatively, could one avoid definitions in total? This chapter will come back to this question later on. For the moment, let us come to Europe.

3 Restrictive Tendencies Under the Council of Europe's Recommendations

To the author's knowledge, the issue of whether the scope of the right of journalists not to disclose their sources should be extended to cases of 'citizen journalism' has not yet been dealt with by the ECtHR.[86] Yet, what does exist regarding this issue is,

[83] *Ibid*, p. 362.

[84] Harris (2013–2014), pp. 1838–1840 (Harris' analysis refers to *Cusumano v. Microsoft*, 162 F.3d 708 (1st Circ. 1998), *Summit Tec., Inc. v. Healthcare Capital Grp., Inc.*, 141 F.R.D. 381 (D. Mass. 1992), *Blum v. Schlegel*, 150 F.R.D. 42 (W.D.N.Y. 1993), *U.S. Commodity Futures Trading Comm'n v. McGraw-Hill Cos.*, 390 F. Supp. 2d 27 (D.D.C 2005)).

[85] *Ibid*, p. 1840.

[86] In fact, none of the cases that were referred to at the beginning of this chapter questioned the quality of the person bringing the complaint as a journalist. Apart from our thorough research into the HUDOC database, our conviction is also based on the fact that there is no relevant indication in the recent factsheet of the Court on the protection of journalistic sources (European Court of Human Rights 2016). In a 2012 judgment, the Grand Chamber did not grant protection under its *Goodwin v. the United Kingdom* jurisprudence to a university professor who had refused to provide access to his research material to other researchers. See ECtHR (Grand Chamber), *Gillberg v. Sweden*, App No.41723/06, 3 April 2012, par. 95. The thoughts of the Court in *Gillberg v. Sweden* cannot provide guidance as regards a future treatment of the problem at hand, as the

firstly, the 2000 Recommendation on the right of journalists not to disclose their sources.[87]

The definition of journalists in the Appendix to this Recommendation is quite restrictive. The term 'journalist' includes 'any natural or legal person who is *regularly or professionally*[88] engaged in the collection and dissemination of information to the public via any means of mass communication'.[89] Principle 2 of the Recommendation extends the protection to persons who collaborate with journalists in the context of the newsgathering and dissemination process, but the extension stops there. In the Explanatory Memorandum (par. 10) it is clearly stated that: 'The protection of the confidentiality of sources of information is limited to journalists, *due to their role and importance*[90] in the information process and the public's right of information by the media and hence indirectly via the work of journalists. Subject to Principle 2, individuals who are not journalists are not covered by this Recommendation'. Below, at par. 13 of the Explanatory Memorandum, it is clarified that, while no official accreditation is needed for a person to be qualified as a journalist, there must necessarily exist 'a *certain occupational tendency*[91]. . .i.e. a journalist typically works regularly and receives some form of remuneration for his or her work. . .This must not exclude, however, journalists who work freelance or part-time, are at the beginning of their professional career, or work on an independent investigation over some time. . . Nevertheless, *individuals who otherwise would not regard themselves as being journalists*[92] shall not qualify as journalists for the purposes of this Recommendation. The latter category may include, for example, individuals who write letters to the editor in the print media, appear as guests on broadcasting programmes or *participate in discussion fora in computer-based media'*.[93] Such delimitation considers 'the history of this protection and paid attention to the fact that the protection of sources is a vital prerequisite for the work of the media in a democratic society, *but not for all forms of communication by*

Court considered that the relevant information (i.e. the research material) already belonged to the public domain, and that refusal to grant access to it constituted a hindrance to the free exchange of opinions and ideas.

[87]Recommendation (2000) 7 of the Committee of Ministers on the right of journalists not to disclose their sources. Adopted on 8 March 2000 at the 701st meeting of the Ministers' Deputies, available via the official website of the Council of Europe.

[88]Emphasis added.

[89]A similar qualification appeared in the 2011 bill, which unsuccessfully attempted to pass a federal 'shield law' provision through the Congress in the USA. This provision would protect only persons who '*regularly*' engage in several news- or information-gathering and dissemination activities '*for a substantial portion of . . . [their] livelihood or for substantial financial gain*'; see Rosenbaum (2013–2014), p. 1450.

[90]Emphasis added.

[91]Emphasis added.

[92]Emphasis added.

[93]Emphasis added.

individuals.[94] A limitation of this protection to journalists in the above sense will also facilitate the balancing of possible conflicting rights and values'.

Similarly, the recent 2011 Recommendation on the protection of journalists' sources[95] is also cautious of the prospect of endorsing protection to non-journalists engaged in Internet-based communications. While it is recognized that 'the media landscape has changed through technological convergence' and that 'the professional profile of journalists has changed over the last decade",[96] it is again clarified (par. 15) that: 'the right of journalists not to disclose their sources of information is a *professional privilege*,[97] intended to encourage sources to provide journalists with important information which they would not give without a commitment to confidentiality. *The same relationship of trust does not exist with regard to non-journalists*, *such as individuals with their own website or web blog*.[98] Therefore, non-journalists cannot benefit from the right of journalists not to reveal their sources'.[99]

Lastly, reference shall be made to the 2011 Recommendation on a new notion of media.[100] This Recommendation calls Member States to 'adopt a new, broad notion of media which encompasses all actors involved in the production and dissemination, to potentially large numbers of people, of content . . . and applications which are designed to facilitate interactive mass communication (for example social networks) or other content-based large-scale interactive experiences (for example online games), while retaining (in all these cases) editorial control or oversight of the contents'.[101] Member States are then invited to apply a set of criteria 'when considering a graduated and differentiated response for actors falling within the new notion of media'.[102] These criteria, as stated and specified in Part I of the Appendix to the Recommendation, include 'intent to act as media', 'editorial control', 'professional standards', and 'public expectation' for 'reliability', 'respect for professional and ethical standards', 'transparency' and 'accountability', among else. Such criteria, along with the mass of the relevant indicators (e.g. the indicators for 'intent to act as media' include 'working methods which are typical for media'), make up a quite demanding threshold so as to claim falling within the notion of 'new media'. Certainly, it is clarified that not all criteria should be met for an entity

[94]Emphasis added.

[95]Recommendation 1950 (2011) of the Parliamentary Assembly of the Council of Europe on the protection of journalists' sources. Adopted by the Assembly on 25 January 2011 (4th Sitting), available via the official website of the Council of Europe.

[96]Par. 11 of the 2011 Recommendation on the protection of journalists' sources.

[97]Emphasis added.

[98]Emphasis added.

[99]Par. 15 of the 2011 Recommendation on the protection of journalists' sources.

[100]Recommendation (2011) 7 of the Committee of Ministers on a new notion of media. Adopted on 21 September 2011 at the 1121st meeting of the Ministers' Deputies, available via the official website of the Council of Europe.

[101]Par. 7 of the 2011 Recommendation on a new notion of media.

[102]Par. 7 of the 2011 Recommendation on a new notion of media.

to fall within the notion of 'new media'.[103] However, certain criteria, editorial control being one of them, are taken to be decisive, insofar as absence of one of them 'would tend to disqualify a service from being regarded as media'.[104] Besides, Part II of the Appendix, which specifies the standards that are to be applied to new media activities, makes a direct reference to protection of sources, calling policy-makers to extend it 'to the identity of users who make content of public interest available *on collective online shared spaces which are designed to facilitate interactive mass communication (or mass communication in aggregate); this includes content-sharing platforms and social networking services*'.[105] Yet, within the same legislative instrument, individual bloggers are referred to as actors that 'may not qualify as media'.[106]

In general, the above references indicate restrictive tendencies regarding the application of the right of journalists not to disclose their sources, at least, to the most problematic but also widespread cases of 'citizen journalism', e.g. to the case of the individual blogger who is not regularly engaged in research and reporting activities that might resemble journalism as traditionally understood. Such restrictive tendencies could express doubts as to whether 'citizen journalists' genuinely contribute to the flow of *valuable* information within the 'marketplace of ideas' on which modern democratic societies are based. Besides, the expansion of protection to individuals who are not controlled by the regular standards and processes of traditional news-media organizations could distort the proper functioning of other important pillars of a rule-of-law state, most importantly delivering of justice by the courts and combating of crime by police or by other investigative authorities.[107] One should notice that it was precisely this fear, coupled with the fear that a working definition of the 'journalist' might never be provided, which led the majority of the USA Supreme Court to rule out the constitutional status of the journalist's privilege in *Branzburg*.[108]

---

[103]Par. 11 of the Appendix of the 2011 Recommendation on a new notion of media.

[104]Par. 11 of the Appendix of the 2011 Recommendation on a new notion of media.

[105]Par. 73 of the Appendix of the 2011 Recommendation on a new notion of media. Protection of sources is also mentioned at par. 42 of the Appendix, and it is listed among the rights, privileges and prerogatives whose assertion 'can be very revealing' as an indicator of meeting criterion 4: 'professional standards'.

[106]Par. 71 of the Appendix of the 2011 Recommendation on a new notion of media. Bloggers are also mentioned in the section of Part I of the Appendix, which specifies the criterion of 'professional standards'. There (par. 41) it is stipulated that bloggers 'should only be considered media if they fulfil the criteria to a sufficient degree'.

[107]In the Appendix to Recommendation (2000) 7 it is pointed out (par. 37–41) that the most important aims which may justify disclosure of journalist's sources are protection of human life, prevention of major crime and defense of a person accused or convicted of having committed a major crime.

[108]See *Branzburg v. Hayes*, 408 U.S. 665, 682–693, 701–702 (emphasizing the significance of testifying before a grand jury for crime investigation), 703–704 (stressing the conceptual difficulties which are related with defining a 'reporter' for a hypothetical privilege under the First Amendment), 705 (expressing concerns with regard to the fact that '[t]he informative function

4 The Doctrinal Background of the Restrictive Tendencies

A common thread in the jurisprudence of the ECtHR and in the 2000 Recommendation on the right of journalists not to disclose their sources, as well as within the traditional understanding of the journalist's privilege in post-*Branzburg* jurisprudence in the USA is that the image of a journalist, in the context of a traditional media organization fulfilling a particular role within a democratic society, encompasses a central role.[109] Such focusing is connected with the constitutional background of the journalist's privilege as traditionally conceived.

Although one can trace several grounds for the justification of the journalist's privilege, as derived from the more general right to press freedom,[110] the most usual and traditional justification obeys to a *functional-utilitarian* and, at the same time, *institutional* philosophy; i.e. one giving emphasis on the traditional 'watchdog' function and utility of 'the press' as a democratic institution, as a 'fourth estate' which checks the holders of political power by providing citizens with all necessary information so as to deliberate on matters of public interest and make informed political choices. For instance, in the landmark *Goodwin* case, the ECtHR justified the protection of journalistic sources under Article 10 of the ECHR as follows: 'Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest'.[111] In the same vein, the minority opinions in *Branzburg* connected the recognition of the constitutional status of the privilege with the need for a robust debate on issues of public interest, as condition of self-government, and with the need to avoid having the press in the service of the governors instead of the governed, being an 'investigative arm' of government

asserted by representatives of the organized press in the present cases is also performed by lecturers, political pollsters, novelists, academic researchers, and dramatists', so that all these persons could be 'silenced' before grand juries) (1972).

[109]For *Branzburg's* and consequent cases' focus on the reporter, see Andersen Jones (2013), pp. 1235–1237, 1239–1242.

[110]See among others Ugland (2010) (distinguishing between policy- and principle-based approaches), Nestler (2005–2006), esp. pp. 206–212 (offering a survey of different justifications of the privilege on First Amendment grounds), Andersen Jones (2013) and Stone (2005–2006) (to whose source-oriented approach we shall refer later on), Konarski (2014–2015) (endorsing a checks-and-balances-oriented approach).

[111]ECtHR, *Goodwin v. the United Kingdom*.

instead of fulfilling its democratically required 'watchdog function'.[112] More generally,'[s]upporters of the privilege insist that anecdotal evidence, common sense, and at least some empirical data all suggest that the privilege is vital to our system of investigative and watchdog reporting. They believe that without such protection for journalists, sources will in fact "dry up", chilling critically important speech on governmental and societal matters'.[113]

There is one doctrinal problem in this vein of thought: The argumentation depends on the empirical existence of a certain 'chilling effect' which non-recognition of the journalist's privilege might provoke on sources who would actually be willing to provide journalists with critical information; something which again is taken to produce a 'chilling effect' on the dissemination of valuable information that the public really needs to check the government and discuss on issues of public interest. The existence of such 'chilling effects' cannot easily be proved.[114] Thus, one could argue that, in the absence of conclusive empirical evidence, there is no normative necessity to connect the privilege with the freedom of the press and with any other fundamental rights derived from it. (This was actually what the majority in *Branzburg* could be taken to have held).[115] Alternatively, one could claim that, although depriving traditional journalists of protection under the privilege would entail an unbearable 'chilling effect', the same is not true with regard to 'citizen journalists'.

Within the premises of the utilitarian-institutional approach, reluctance to expand the definition of the journalist to cover new practices in the galaxy of New Media appears to be justified in view of the empirical uncertainties, which are related to the 'chilling effect' doctrine, coupled with the doubts and fears to which reference has been made in the previous section. At least, reluctance appears to be justified as much as the optimism of those who endorse the extension of the privilege to non-journalists. At last instance, why should we risk such an extension and all the consequent policy-making and normative-interpretative 'troubles'? Why should we not rest content with a strict definition of the 'journalist' to avoid all these 'troubles', as long as we can never be sure about the 'chilling effects' that

[112]See *Branzburg v. Hayes*, 408 U.S. 665, 713–725 (Justice Douglas, dissenting opinion, arguing for the constitutional recognition of the journalist's privilege based on effective self-government arguments, among else), 725–752 (Justice Stewart, dissenting opinion, joined by Justices Brennan and Marshall, stressing the importance of a free press within a democratic society and advocating that non-recognition of the privilege under the First Amendment would undermine the news gathering and dissemination process, to the detriment of the relevant fundamental rights of the press) (1972).

[113]Andersen Jones (2013), p. 1243.

[114]See Andersen Jones (2013), pp. 1242–1244, Eliason (2006–2007), pp. 417–418; see also the ambivalent conclusions of the empirical research of Andersen Jones (2008–2009); cf. Ugland (2010) pp. 45–46: 'The chilling effect on speech, the wariness of sources, the broader symbolic damage to the image of the press when it cooperates with government–none of these things is readily measurable, but they are no less real because of it'.

[115]Cf. *Branzburg v. Hayes*, 408 U.S. 665, 698–699 (1972).

non-extension of the privilege might bear on the so-called 'digital democracy' and on democratic societies at large?

5 An Alternative Approach: Focus On the Source?

At its heart, the problem is doctrinal; it is related with the empirical nature of the 'chilling-effect' speculations that support the one or the other policy choice as regards drafting of the relevant provisions and the one or the other interpretative-normative choice as regards the question of who might claim the privilege in the New Media galaxy. To deal with this problem, some USA scholars have proposed that, instead of focusing on the 'journalist', focus should be made on the 'source'. There is a sound constitutional background to do this, as the right to freedom of speech has a negative side: the right of each individual speaker not to exercise his/her freedom of speech, thus to remain silent and not to disclose his/her identity.[116] Certainly, this right is not absolute but qualified; protection under it may be lifted if the government shows that there is a compelling public interest to reveal the speaker's identity, an interest that cannot be satisfied in an alternative way.[117]

A first version of the source-oriented approach was offered by Stone (2005–2006),[118] followed by Harris (2013–2014).[119] According to Stone (2005–2006),[120] the goal of the journalist's privilege is to promote a certain type of open communication that is important for society. This aim is no different from the one of other similar privileges, such as the attorney-client's, the doctor-patient's or the priest-penitent's privilege. In all these relationships 'the privilege "belongs" to the person whose communication society wants to encourage'; keeping this communication confidential depends first and most importantly on the election of e.g. the client or the patient, while '[t]he attorney or doctor is merely the agent of the client or patient'; [t]he logic of the journalist-source privilege is similar to that ... Public policy certainly supports the idea that individuals who possess information of significant value to the public should ordinarily be encouraged to convey this information to the public'.[121] Thus, '[t]he focus should not be on whether the reporter fits within any particular category. Rather, the source should be protected

[116]For the assertion of this right under the First Amendment in USA case-law, for its qualification and for its possible application to the confidential-source situation, see among others Andersen Jones (2013), pp. 1249–1270. In the 2012 *Gillberg v. Sweden* case, and after it re-examined its scarce case-law on the subject, the ECtHR did 'not rule out that a negative right to freedom of expression is protected under Article 10 of the Convention', but it also found 'that the issue should be properly addressed in the circumstances of a given case' (par. 86).

[117]*Ibid*.

[118]Stone (2005–2006), pp. 39–41, 50–51.

[119]Harris (2013–2014), pp. 1856–1846, 1849–1851.

[120]Stone (2005–2006), pp. 39–41.

[121]*Ibid*, p. 41.

whenever he makes a confidential disclosure to an individual, reasonably believing that that individual regularly disseminates information to the general public, when the source's purpose is to enable that individual to disseminate the information to the general public'.[122]

This approach is still premised on the functional-utilitarian understanding of the constitutional background of the journalist's privilege. Besides, as regards its practical application, it gives too much weight on a factor, the source's purpose to use the journalist as an agent to disseminate information to the public, which would be difficult, if not impossible, to ascertain without compromising the silence of the journalist on the source's identity, that is, without compromising the journalist's privilege itself.[123]

Andersen Jones (2013) promotes a more radical version of the source-oriented approach. After having revealed the weaknesses of the traditional 'focus-on-the-reporter' doctrine,[124] this scholar analyzes in detail the recognition of the right to speak anonymously as a fundamental First Amendment value by the Supreme Court.[125] She then proceeds to argue for the application of the anonymous-speech doctrine to the confidential-source situation, as 'a more coherent and practically more workable' framework for the protection of the First Amendment values.[126] Such a paradigm shift 'would not represent a shift *away*[127] from recognition of the First Amendment's public information goals'; it would add to those values some other values ('speaker privacy', 'antiretaliation', and 'source bias') which are 'implicated by the reporter-confidential source dynamic' but 'only circuitously acknowledged in the *Branzburg* line of cases'.[128] Besides, the 'investigation of the anonymous-speech rights of a confidential source would pose no definitional problems because the approach, unlike that of *Branzburg*, does not rise and fall on the nature of the speaker, the nature of the audience, or the value of the information communicated'.[129] On the other hand, this approach would possibly help avoid inquiries into the presence of the 'deterrence of communication' and of the 'chilling effect' factors. 'The individual liberty to choose one's one message and to be free from a government dictate as to the content of one's communication, including the attribution of one's authorship, is a foundational First Amendment principle that requires no demonstration of ill effect or empirical showing of the creation of detrimental incentives'.[130]

---

[122] *Ibid*, p. 51.

[123] See Papandrea (2007), p. 582.

[124] Andersen Jones (2013), pp. 1238–1249.

[125] *Ibid*, pp. 1249–1259. The most important cases analyzed by Andersen Jones are *Talley v. California*, 362 U.S. 60 (1960), *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995), and *Buckley v. Valeo*, 424 U.S. 1 (1976).

[126] *Ibid*, p.1259 et seq.

[127] Emphasis added.

[128] Andersen Jones (2013), pp. 1264–1265.

[129] *Ibid*, p. 1261.

[130] *Ibid*, pp. 1262–1263, references omitted.

Escaping the definitional problem of the 'journalist' and side-stepping the empirical-speculation difficulties concerning the 'chilling effect' are, indeed, important advantages of the source-oriented approach.[131] The doctrinal background becomes then clearer. The judicial analysis focuses on a typical individual-autonomy right (the right of each person not to reveal his/her identity) and on the limits of this right in view of compelling public interest concerns (a typical proportionality analysis would suffice to identify these limits in each and every case). Such a shift would certainly make the life of courts easier.

Besides, the source-oriented approach would most probably lead to broader protection of quasi-journalistic sources in the New Media galaxy, because not only journalists but every person who would be invited by public authorities to disclose his/her source would be entitled to refuse to do so, asserting the fundamental right of the source not to have his/her identity disclosed.[132] One should also notice that the source-oriented approach seems to adjust better to the pragmatic context of anonymous online posts to news-oriented websites. This is so insofar as the agents of the latter tend to see protection of the anonymity of posts not so much as a matter of enhanced newsgathering and/or editorial capability (thus, as a matter that would fall within the traditional philosophy underpinning the protection of journalistic sources), but as a matter of principle relevant with protection of free flow of speech in general.[133]

Notwithstanding the advantages of the source-oriented approach, the traditional context of the debate (that is, focusing on the definition of 'the journalist' in relation with 'chilling effect') cannot so easily be sidestepped. The source-oriented approach tries to escape the definitional and the 'chilling-effect' problems by setting them aside mostly as a matter of judicial investigation. However, these pressing issues cannot be set aside in the wider context of policy-making concerns. The competent authority to deal with such concerns in a democratic society is foremost the legislature; the courts come second in this respect.[134] Besides, courts would more easily be willing to extend the protection of journalistic sources to New Media in deference to specific legislative provisions than as a matter of interpretative activism.[135]

---

[131]The emphasis on the protection of this right fits well with the current trends towards increased protection of 'whistleblowers'. See Recommendation CM/Rec (2014) 7 of the Committee of Ministers of the Council of Europe on the protection of whistleblowers, adopted on 30 April 2014 at the 1198th meeting of the Ministers' Deputies, available via the official website of the Council of Europe. Adjustment of the protection of journalistic sources is mentioned at par. 37 of the Explanatory Memorandum, as one of the measures that states could take towards improving the legal protection of whistleblowers.

[132]This scenario presents third-party-standing implications, with which we cannot here be concerned. See, in the context of USA jurisprudence, Andersen Jones (2013), pp. 1266–1270, 1273–1277.

[133]See Andersen Jones (2013), pp. 1275–1277, where relevant references; cf. Kirtley (2009–2010), p. 1508 and passim.

[134]Cf. the discussion in Tursi (2014), pp. 224–229, and in Harris (2013–2014), pp. 1841–1842.

[135]Cf. Stone (2005–2006), p. 48, referring to the Supreme Court granting deference to a possible federal shield law.

6 Back to Public Policy and to the Traditional Concerns: Our Proposal

The value on which the source-oriented approach focuses, i.e. the individual autonomy of the source, should certainly be considered not only by courts but also by public policy-makers. Nevertheless, the latter should also focus on broader questions regarding the development of journalism and the media in general, such as the following ones: What is the contribution of the New Media and of 'citizen journalists' to an informed citizenry, as compared with the relevant contribution of traditional media? Which is the role of each particular agent (the sources included) of the New Media within the news-gathering and dissemination processes? Which are the implications and the dangers of online anonymity? Is there any value in it? Moreover, what about the development of new surveillance techniques which are anyway posing a lethal threat to the protection of journalistic sources, even if such protection is legally guaranteed? The issue of a possible extension of the right of journalists not to disclose their sources to 'citizen journalism', which includes the traditional framework of 'chilling-effect' empirical speculations, should be dealt within the context of these questions. Besides, as a matter of 'legal technique', the extension of the protection of journalistic sources to New Media will most probably pass through appropriate adaptations of the definition of the 'journalist', and not through abandoning any reference to journalists altogether.

Nevertheless, even in the context of such traditional concerns, one may still argue that the right of journalists not to disclose their sources should be taken not as a privilege belonging to a particular professional group but as a fundamental right of whoever engages in specific activities within processes that are critical for the fulfillment of press freedom values. Such an argument calls, firstly, for a loosening of the institutionalist edges of the traditional 'watchdog' philosophy as regards the role of 'the press' in a democratic society.

Once upon a time the 'watchdog' and the other democratic functions of 'the press' had been fulfilled by specific organizations: traditional mass media organizations, which channeled the work of journalists through the application of valuable ethical-professional standards, but also through ambivalent, to say the least, agenda-setting or other tactics and politics. In our days a big part of the same democratic functions are being fulfilled by the 'citizen journalists' of the New Media, and there are strong indications that the contribution of these individuals to the dissemination of crucial information on public-interest issues is all but insignificant.[136] Although they 'tend to lack professional training and experience in the field, and they may not contribute to the marketplace of ideas on a regular basis',[137] citizen journalists may 'be faster than traditional journalists',[138] and they may also

[136]See e.g. the rich references in Turner (2011–2012), pp. 509–510, Alonzo (2005–2006), pp. 772–774, and Rosenbaum (2013–2014), pp. 1457–1458.

[137]Turner (2011–2012), pp. 510–511.

[138]*Ibid*, p. 510, note 47.

'be more likely to voice controversial concerns and even scrutinize the work of traditional journalists',[139] insofar as they 'are not tied to mainstream media organizations or other "potentially biased gatekeepers"'.[140] The vigilance of other users and the possibility of almost instantaneous correction of mistakes may play the role of a substitute for the potential lack of editorial control, while sometimes '[b]logs and digital platforms can even have more credibility than established news outlets'.[141] In any case, if what really matters for the protection of journalistic sources is free flow of information and democratic deliberation, then 'citizen journalism' has earned a sufficiently credible title to claim this right. Cases of inaccurate, offensive or 'dangerous' online reporting offer nothing to counterfeit this *prima facie* title, in the same way as such cases offered nothing in the past to counterfeit the fundamental rights of traditional press agents, including their right not to disclose their sources.

If the above remarks are correct, then policy-makers, when drafting the definition of the 'journalist', should dispense with criteria such as the professional status, the association with a media organization or the regular engagement of a person in journalism.[142] Medium-neutrality, which is in principle accepted as a *sine qua non* baseline for every attempt to handle the issue at hand,[143] entails the avoidance of other indicators, such as similarity to news media outlets[144] or editorial control, which may anyway be lacking even from traditional media.[145] Besides, other standards, such as the circulation or the 'visibility' record of a medium, its reputation for accuracy or even the newsworthiness of the specific publication at hand, would more generally run contrary to the fundamental value of neutrality as regards protection of freedom of speech and of the press.[146] The significance of the publication at hand for the right of citizens to be informed on topics of general interest could play a role at a later stage, when applying the qualifications of the right in view of compelling public interest concerns. However, such significance should not be taken as an indicator in deciding whether to allow 'citizen journalists' a *prima facie* standing under the right not to disclose their sources.

---

[139] *Ibid*, p. 511.

[140] *Ibid*, p. 511.

[141] Rosenbaum (2013–2014), p. 1457, referring to the SCOTUS blog's accurate reporting on a Supreme Court's ruling as compared with the relevant CNN's inaccurate report.

[142] Ibid, pp. 1461–1462, Papandrea (2007), p. 576, Turner (2011–2012), pp. 514–515.

[143] See e.g. Berger (2002–2003), pp. 1410–1411, Papandrea (2007), p. 574, Martin and Fargo (2013), pp. 89, 91–92.

[144] Such a 'similarity standard' was used by the *O'Grady* judgment of the California Court of Appeal and by the *Too Much Media* judgment of the New Jersey Supreme Court, to which we referred above. The adoption of such a standard is promoted by Toland (2009), pp. 484 et seq., and by Turner (2011–2012), pp. 515–518, leaving out of protection casual posting to social media, chat rooms or other messaging platforms.

[145] See Rosenbaum (2013–2014), p. 1462.

[146] See Papandrea (2007), pp. 575–581.

What should matter most for these purposes is the dissemination of information to the public, and a crucial question here is whether we should require the presence of intent to disseminate information already '"at the inception of the process of gathering the news or information sought"'.[147] Although it has been argued that mere dissemination of information should suffice for claiming a *prima facie* standing under the journalist's privilege,[148] there is at least one convincing reason why the aforementioned 'intent test' should be adopted: Without it every communicative act could retrospectively be translated into a journalistic act, and every person could thus refuse to disclose his/her sources, harming seriously the proper functioning of the courts, the crime-investigative authorities and the rule-of-law state at large.[149] The possibility of such an abuse could deter policy-making agents from even considering an enlargement of the scope of the right.

The above discussion was restricted to the issue of whether the right of journalists not to disclose their sources should be extended to non-journalists in the context of New Media communicative activities. The qualifications of this right have not been dealt with in here. As a matter of principle, these qualifications should be no different from the ones which apply to traditional journalism and to which reference has been made in Sect. 1 of this chapter. Besides, these qualifications could help alleviate the fears of those who would be reluctant to enlarge the scope of the discussed right in view of its potential abuse.

Indeed, the fear that an extended right not to disclose one's sources could be abused can never be eliminated. Such a fear is an inescapable element of every discussion on fundamental rights. The nature and role of the latter is precisely to guarantee in principle significant aspects of our individual and of our public autonomy notwithstanding the possibility that in specific cases such autonomy will be used to the detriment of the public interest or of the rights of others. The right of journalists not to disclose their sources safeguards public autonomy by protecting the fruitfulness of the crucial democratic processes of news-gathering and of dissemination of information to the public. Whether the empirical 'chilling-effect' speculations, to which reference has been made in Sect. 4 of this chapter, are sufficient to conclude that this right is a fundamental i.e. a constitutional one, can be an open question for democratic societies, as it is the case in the USA. What could

[147]Rosenbaum (2013–2014), p. 1460, adopting the phrasing of a proposed federal shield law that did not manage to pass through the Congress in 2009. Federal Circuit Courts used the same standard to afford protection under the journalist's privilege. See n 54 above.

[148]See Papandrea (2007), pp. 585–586. To be reminded, however, that Papandrea combines the expansive approach as regards the scope of the right with rather strict qualifications as regards its application. See Sect. 2.2 of this essay.

[149]Cf. Rosenbaum (2013–2014), pp. 1460–1461, requiring in addition that such an intent should actually be a 'journalistic' one, also requiring that '[t]his journalistic intent would need to be manifested outwardly to sources, as the information source would need to be aware that he was speaking to someone engaged in journalism, regardless of the platform used'. We believe that these additional requirements open the 'back door' to the restrictive tendencies which are related with the criteria that we dismissed above.

be argued is that if the answer to this question is a positive one, as the author of this chapter believes it should be, then the scope of this right should be extended so as to cover not only traditional journalists but also the 'citizen journalists' of the New Media.

References

Allan S, Thorsen E (eds) (2009) Citizen journalism: global perspectives. Peter Lang Publishing, New York

Alonzo JS (2005–2006) Restoring the ideal marketplace: how recognizing bloggers as journalists can save the press. NYU J Legis Public Policy 9:751–780

Andersen Jones RN (2008–2009) Avalanche or Undue Alarm? An empirical study of subpoenas received by the news media. Minn Law Rev 93:585–669

Andersen Jones RN (2013) Rethinking reporter's privilege. Mich Law Rev 111(7):1221–1282

Banisar D (2007) Silencing Sources: An International Survey of Protections and Threats to Journalists' Sources. Privacy International Global Survey Series. Available via SSRN. http://ssrn.com/abstract=1706688. Accessed 13 May 2016

Barendt E (2005) Freedom of speech, 2nd edn. Oxford University Press, New York

Benkler Y (2011) A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate. Harv CR-CL Law Rev 46:311–397

Berger LL (2002–2003) Shielding the unmedia: using the process of journalism to protect the journalist's privilege in an infinite universe of publication. Hous Law Rev 39(5):1371–1416

Castiglione JD (2007) A structuralist critique of the journalist's privilege. J Law Policy 23:115–146

Campagnolo T (2002–2003) The conflict between state press shield laws and federal criminal proceedings: the rule 501 blues. Gonz Law Rev 38(3):445–501

Clark KC, Barnette D (2012) The application of the reporter's privilege and the espionage act to Wikileaks. U Dayton Law Rev 37(2):165–183

Compendium of Reporter's Privilege (2016) Reporter's Committee for Freedom of the Press. Available via the website of the Reporters Committee for Freedom of the Press. http://www.rcfp.org/reporters-privilege. Accessed 14 May 2016

Dalglish LA, Murray C (2006–2007) Déjà Vu all over again: how a generation of gains in federal reporter's privilege law is being reversed. U Ark Little Rock Law Rev 29:13–42

Davidson S, Herrera D (2011–2012) Needed: more than a paper shield. WM Mary Bill RTS J 20:1277–1372

Eliason RD (2006–2007) Leakers, bloggers, and fourth estate inmates: the misguided pursuit of a reporter's privilege. Cardozo Arts Ent Law J 24:385–446

European Court of Human Rights (2016) Factsheet, Protection of journalistic sources. January 2016. Available via the website of the European Court of Human Rights. http://www.echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf. Accessed 18 May 2016

Fargo AL (2005–2006) The year of leaking dangerously: shadowy sources, jailed journalists, and the uncertain future of the federal journalist's privilege. WM Mary Bill RTS J 14:1063–1119

Gierhart C (2014) Media organizations urge Senate to vote on federal shield bill. Reporter's Privilege News, 13 June 2014. Available via the website of the Reporters Committee for Freedom of the Press. http://www.rcfp.org/browse-media-law-resources/news/media-organizations-urge-senate-vote-federal-shield-bill. Accessed 15 May 2016

Gillmor D (2004) We the media: grassroots journalism by the people, for the people. O'Reilly Media, Sebastopol

Gomsak M (2006–2007) The free flow of information act of 2006: settling the journalist's privilege debate. Brandeis Law J 45:597–622

Harris R (2013–2014) Conceptualizing and reconceptualizing the reporter's privilege in the age of Wikileaks. Fordham Law Rev 82:1811–1854
Kirtley JE (2009–2010) Mask, shield, and sword: should the journalist's privilege protect the identity of anonymous posters to news media websites? Minn Law Rev 94:1478–1513
Konarski AA (2014–2015) The reporter's privilege is essential to checks and balances being accessible to the American electorate. Seton Hall Cir Rev 11:258–283
Liptak A (2014) Supreme Court rejects appeal from times reporter over refusal to identify source. New York Times, 2 June 2014. Available via the electronic portal of New York Times. http://www.nytimes.com/2014/06/03/us/james-risen-faces-jail-time-for-refusing-to-identify-a-confidential-source.html?_r=0. Accessed 15 May 2016
Martin JA, Fargo AL (2013) Rebooting shield laws: updating journalist's privilege to reflect the realities of digital newsgathering. Univ Fla J Law Public Policy 24:47–96
Nestler JS (2005–2006) The underprivileged profession: the case for Supreme Court recognition of the journalist's privilege. Univ Pa Law Rev 154:201–256
Papandrea MR (2007) Citizen journalism and the reporter's privilege. Minn Law Rev 91:515–591
Papandrea MR (2011–2012) The publication of national security information in the digital age. J Nat'l Secur Law Policy 5:119–130
Peters J (2010–2011) Wikileaks would not qualify to claim federal reporter's privilege in any form. Fed Commun Law J 63(3):667–695
Rosenbaum KA (2013–2014) Protecting more than the front page: codifying a reporter's privilege for digital and citizen journalists. Notre Dame Law Rev 89(3):1427–1465
Stone GR (2005–2006) Why we need a federal reporter's privilege. Hofstra Law Rev 34:39–58
Toland CJ (2009) Internet journalists and the reporter's privilege: providing protection for online periodicals. Kansas Law Rev 57:461–490
Turner SB (2011–2012) Protecting citizen journalists: why congress should adopt a broad federal shield law. Yale Law Policy Rev 30:503–519
Tursi JW (2014) The reporter's privilege in the 21st century: the need for a qualified federal media shield law that balances freedom of speech with national security concerns. Santa Clara Law Rev 54:201–235
Ugland E (2010) The new abridged reporter's privilege: policies, principles, and pathological perspectives. Ohio St Law J 71:1–70
Wall M (ed) (2012) Citizen journalism: valuable, useless or dangerous? International Debate Education Association, New York

Chapter 15
The Legal Regulation of Hate Speech on the Internet

Ioannis Iglezakis

Abstract The Internet with its unique ability of communication of one-to-many and many-to-many and its potential for anonymous and mobile interaction has become the new frontier for the dissemination of hate speech. To deal with this issue, many countries have enacted legislation criminalizing hate speech, but international legal acts have also been introduced for the harmonization of national legislations. This chapter will engage in a detailed presentation of the regulations of hate speech on the Internet, on an international level, and will furthermore explore its conflict with the right to freedom of expression.

1 Introduction

As it is well known, the Internet is a decentralized international network of computer networks and computers, not owned and controlled by any government or private organization. Because of its particular characteristics, it is often depicted as a specific domain, called 'Cyberspace', which has no territorially-based boundaries and rises above the restrictions of national legislation.[1] It is also praised as 'the largest experiment in anarchy that we have ever had'[2] and as a network, in which 'nobody knows if you're a dog'.[3]

[1] See Johnson and Post (1996), pp. 1367 et seq,; Reidenberg (1996).

[2] According to the famous quote of Eric Schmidt, "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."

[3] See Fleishman (2000).

I. Iglezakis (✉)
Aristotle University of Thessaloniki, Thessaloniki, Greece
e-mail: iglezakis@hotmail.com

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_15

The Internet is also a means of communication that allows the spreading of free expression globally and for that, it is supported that it promotes a democratic culture.[4] However, there is a tension between free expression and hate speech being disseminated on the Internet.[5] In particular, the anonymity and ability of communication of one-to-many and many-to-many has made it an ideal instrument for the wide spreading of hate speech by extremists and hate mongers.[6]

Thus, the Internet has become the 'new frontier' for spreading hate[7]; it allows extremists and haters easier access to an unexpectedly big audience, which consists, on a high level, of young and gullible persons. The Simon Wiesenthal Center's Digital Hate and Terrorism project reported, in 2011, that there existed over 14,000 problematic websites, forums, blogs and social media postings.[8] Hate groups have also exploited Web 2.0 and developed their own sites such as New Saxon, "a Social Networking site for white singles" produced by the American Neo-Nazi group National Socialist Movement. Extremists are also represented on Facebook, e.g., Stormfront, National Socialist Life, Libertarian National Social Movement, Aryan Guard, FARC, Al Shabab Mujahideen, Hamas, Hezbollah, etc. Furthermore, Twitter is used as an online marketing tool for extremists, despite its efforts to remove terror postings, while online terrorist magazines proliferate in many languages.[9]

Greece was also affected by the surge in hate speech, particularly in the time of economic crisis. It has been documented in a Report drafted by the European Commission against Racism and Intolerance for Greece, in 2014, that speech attacking immigrants, Muslims, Roma, Jews, as well as homosexual and transgender persons is widespread in the mass media and on the Internet, particularly because of the lack of self-regulation mechanisms.[10]

To respond to the wave of online hate, many countries and international organizations have enacted legislation, providing for criminal sanctions against such practices. One striking exception is the United States, which have a long constitutional tradition of protection of freedom of expression and the introduction of criminal sanctions against speech would violate this right. In this paper, the peculiarities of regulating hate speech on the Internet on an international level will be examined and its conflict with the right to freedom of expression will be explored in greater detail.

[4]Balkin (2008).

[5]See Andrew Murray (2013), p. 135.

[6]See Banks (2010), pp. 233–239.

[7]Anti-Defamation League (2000).

[8]Digital Hate and Terrorism Project (2011).

[9]Digital Terrorism and Hate Report (2015).

[10]See ECRI Report (2015).

2 The Characteristics and the Definition of Online Hate Speech

2.1 Characteristics

Online hate speech has unique features, which distinguishes it from hate speech posted in traditional media. In particular, illegal content can stay online for a long time in different formats across multiple platforms that can be linked repeatedly. Thus, a posting in a social networking site, which goes viral, may have significant importance, compared to one that does not gain much attention.[11]

Obviously, the longer the content stays online, the more damage it can inflict, whereas if it is removed at an early stage, the moral damage of the injured person will be limited. At any rate, it depends upon the architecture of specific platforms, which may allow content to stay online longer or not. For example, Twitter's conversations are organized in threads or hashtags, whereas this allows the fast and wide dissemination of hateful messages, but also provides an opportunity to influential users to terminate such threads.[12] Facebook, on the other hand, has the functionality of a blog and presents posts in a chronological order. It also introduced hashtags, but these are not as popular as those on Twitter.

As it is the case with online content in general, hate speech online may be hard to eliminate. A post in a networking site, for example, may be removed, but it may be copied by other users and posted in the same or in other sites. Content which is deleted may also be archived and appear in the cached pages of search engines (Google, Yahoo, Bing) or in the WayBack Machine or similar services, which store older versions of web pages.[13]

According to UNESCO's guide to online hate speech: "*The endurance of hate speech materials online is unique due to its low cost and potential for immediate revival, ensuring its continued relevance in particular spheres of discourse. As the Internet is not governed by a single entity, concerned individuals, governments and non-governmental organizations may have to address Internet Intermediaries on a case-by-case basis, although leaving the owners of a specific online space to also decide how to deal with users' actions on an ongoing basis*".[14]

As the Internet offers haters the ability to communicate and publish illegal content anonymously or pseudonymously, this allows the wide dissemination of illegal hate speech. Governments and social media services, such as Facebook, have taken initiatives to enforce real name policies, but in fact, such efforts violate the right to privacy.[15]

---

[11] See UNESCO (2015), p. 13.

[12] See UNESCO, *ibid*, p. 14.

[13] See, e.g., https://consciousawarenessforall.wordpress.com/2015/09/08/View-Archived-Pages/.

[14] UNESCO (2015), 14.

[15] See Hasine and Galperin (2015).

2.2 Definition

The definition of the legal term "hate speech" can be found in various international legal texts. In particular, according to the Committee of Ministers of the Council of Europe, it covers all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.[16]

This term is also defined by the European Court of Human Rights (ECrtHR), which refers to hate speech as covering all forms of expression which spread, incite, promote or justify hatred based on intolerance (including religious intolerance),[17] but also as the speech which glorifies violence.[18]

Greek law adopts a more comprehensive approach. Law 4285/2014 refers to acts or actions, which may provoke discrimination, hate or violence against a person or a group of persons, determined based on race, color, religion, descent, national or ethnic origin, sexual orientation, gender identity or disability (Article 1 (1) and 2 (1)).

Evidently, there is no universally accepted definition of this key term, while national laws introducing penal law provisions prohibiting hate speech differ in the determination of what is being banned.[19] In the framework of the EU-Research project "Mandola",[20] a distinction is made between hate speech, in general, designating a "hostile verbal abuse", and illegal hate speech, as this is defined in Recommendation No. R (97) 20 of the Council of Europe.[21]

Owing to the lack of a generally accepted definition of unlawful hate speech, social networking services and websites provide their own definitions. So, e.g., Facebook defines the term 'hate speech' as "direct and serious attacks on any protected category of people based on their race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability or disease".[22] Similarly, in the Code of Conduct on Countering Illegal Hate Speech Online signed by Facebook, YouTube, Twitter and Microsoft, hate speech is defined as "all conduct publicly inciting to

[16]Recommendation No. R (97) 20 of the Council of Europe.

[17]ECtHR, *Gündüz v. Turkey*, No. 35071/97, § 40; *Erbakan v. Turkey*, No 59405/00, § 56.

[18]ECtHR, *Sürek v. Turkey(no. 1)*[GC], no.26682/95, § 62.

[19]See Weber (2009), p. 3.

[20]The MANDOLA project is aimed at monitoring the spread and penetration of online hate-related speech in Europe and in Member States using big-data approaches, providing policy makers with information which can be used to combat online hate speech, and citizens with tools to deal with online hate, transferring best practices among Member States and creating a reporting infrastructure which will connect citizens with police authorities.

[21]See D4.1: FAQ on responding to on-line hate speech, p. 20, online available at: http://mandola-project.eu/m/filer_public/1a/af/1aaf50d3-8a38-40f4-b299-9c343f16cea1/mandola-d41.pdf.

[22]https://www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054/.

violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin".[23]

Particularly as regards online hate speech, the Council of Europe in the Additional Protocol to the Convention of Cybercrime includes the definition of "racist and xenophobic material" as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors". This definition differs from other international legal texts, such as the 12th protocol to the European Convention on Human Rights (ECHR) and the United Nations (UN) International Convention on the Elimination of All Forms of Racial Discrimination, in that the additional protocol applies to the dissemination of racist and xenophobic material through computer systems, whereas the other international texts refer to racial discrimination or discrimination, generally.

For this paper, it seems more appropriate to adopt a universal definition, such as the one provided by the Committee of Ministers of the Council of Europe.[24]

3 The International and EU Legal Framework Against Hate Speech on the Internet

The issue of hate speech and the right to non-discrimination have been addressed in many international legal texts at international and European Union (EU) level.

The International Covenant on Civil and Political Rights (ICCPR) addresses hate speech indirectly. In particular, Article 19 ICCPR provides for the right to freedom of expression, while Article 20 expressly limits this right in cases of "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence". This can be interpreted as a regulation of unlawful hate speech.

The UN has also adopted the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), which entered into force in 1969. This Convention includes the obligation of its members to eliminate racial discrimination and to promote understanding among all races. It prohibits hate speech only insofar as it is related to race and ethnicity. Namely, Article 4 (a) stipulates that state parties: Shall declare as an offense punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of

[23]Code of Conduct on Countering Illegal Hate Speech Online; see also European Commission – Press release: European Commission and IT Companies announce Code of Conduct on illegal online hate speech, http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

[24]See above fn. 15.

persons of another color or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof;

> This obligation imposed by the ICERD on state parties is also stricter than the case of Article 20 of the ICCPR covering the criminalization of racist ideas that are not necessarily inciting discrimination, hostility or violence.

Furthermore, the Committee on the Elimination of Racial Discrimination has addressed the issue of hate speech in its General Recommendation 20, in which state parties are advised, *inter alia,* to:

> (r) Take measures against any dissemination of ideas of caste superiority and inferiority or which attempt to justify violence, hatred or discrimination against descent-based communities;
>
> (s) Take strict measures against any incitement to discrimination or violence against the communities, including through the Internet;
>
> (t) Take measures to raise awareness among media professionals of the nature and incidence of descent-based discrimination;

In Europe, the European Commission against Racism and Intolerance (ECRI) issued the General Policy Recommendation No. 6 on Combating the Dissemination of Racist, Xenophobic and Anti-Semitic Material via the Internet in 2000,[25] and in 2015 it adopted the General Policy Recommendation No. 15 on combating hate speech.[26]

The Council of Europe adopted, in 2003, the Additional Protocol to the Convention on cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. More generally, Article 14 of the ECHR prohibits discrimination when applying the other provisions of the Convention, while additional protocol no. 12 to the ECHR provides for a general prohibition of discrimination.

The EU has adopted the Joint Action (96/443/JHA) of 15 July 1996 concerning action to combat and xenophobia.[27] It further adopted the Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law, repealing the Joint Action of 1996.[28] Besides these legal acts, Articles 21, 22 and 23 of the Charter of Fundamental Rights of the EU prohibit discrimination and aim at promoting equality between genders and cultural, religious and linguistic diversity. In addition, Council Directive 2000/43/EC implements the principle of equal treatment between persons irrespective of racial and ethnic origin.

In this section, the legal acts, which are more relevant to online hate speech, will be presented in more detail.

---

[25] https://www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n6/Rec%206%20en.pdf.

[26] https://www.coe.int/t/dghl/monitoring/ecri/activities/GPR/EN/Recommendation_N15/REC-15-2016-015-ENG.pdf.

[27] OJ L 185/5, 24.7.1996.

[28] OJ L 328/55, 6.12.2008.

3.1 The Additional Protocol to the Convention of Cybercrime

The Council of Europe introduced the Convention on Cybercrime in 2001 (Convention on Cybercrime), a milestone in this area that was signed by big industrialist states such as the United States, Japan, Canada and Australia.[29] Any provisions on cyberhate were excluded from the Convention on Cybercrime because the United States would not have accepted them.[30] Therefore, the Council of Europe adopted the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (Protocol).[31] It extends the scope of the Convention on Cybercrime, including its substantive, procedural and international cooperation provision, to also cover offenses of racist or xenophobic propaganda. The purpose of the Protocol is to harmonize the substantive law elements of such behavior and furthermore, to improve the ability of the signatory states to make use of the means and avenues of international cooperation provided for in the Convention, in this area.

Thus, this Protocol is complementary to the provisions of the Convention on Cybercrime and is a point of reference regarding the criminalization of online hate, as it is the first international legal act in this field.

The purpose of the Protocol, defined in article 1, is "to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems".

The measures to be taken at a national level are provided for in Chapter II (Articles 3–7). In particular, Article 3 reads that each contracting Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system".

The Protocol moreover states in Art. 4 that each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offense as defined under its domestic law, (1) persons for the reason that they belong to a group, distinguished by race, color, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (2) a group of persons which is distinguished by any of these characteristics.

Furthermore, Art. 5 provides that each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its

[29]See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=61ZhEtVX.

[30]See Banks, ibid at 236.

[31]Council of Europe, Treaty No. 189, 28.1.2003; for details see https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (1) persons for the reason that they belong to a group distinguished by race, color, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (2) a group of persons which is distinguished by any of these characteristics.

Finally, Art. 6 reads that each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offenses under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognized as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognized by that Party.

The protocol intends only minimum harmonization of national law and thus, it provides in Articles 3, 5 and 6 that any Party may reserve the right not to apply, in whole or in part, these provisions, or that it may require additional elements for the fulfillment of the offense. Reservations and declarations made by a Party to the Convention on Cybercrime may also apply to this Protocol (Art. 12 (1)).

3.2 The EU Legal Framework on Hate Speech

The EU Council has adopted the Joint Action of 15 July 1996 concerning action to combat and xenophobia (96/443/JHA). This provides that EU Member States must ensure an effective judicial cooperation and, if necessary, for that purpose, take steps to punish as criminal offenses:

- public incitement to discrimination, violence or racial violence or racial hatred in respect of a group of persons or a member of such a group defined by reference to color, race, religion or national or ethnic origin;
- public condoning, for a racist or xenophobic purpose, of crimes against humanity and human rights violations;
- public denial of the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 April 1945, insofar as it includes behavior which is contemptuous of, or degrading to, a group of persons defined by reference to color, race, religion or national or ethnic origin;
- public dissemination or distribution of tracts, pictures or other material containing expressions of racism and xenophobia;
- participation in the activities of groups, organizations or associations, which involve discrimination, violence, or racial, ethnic or religious hatred.

It also adopted the Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law.

The purpose of the Framework Decision is to ensure that certain serious manifestations of racism and xenophobia are punishable by effective, proportionate and dissuasive criminal penalties throughout the EU, and it aims to improve and encourage judicial cooperation in this field.

The Framework Decision is considered as a follow-up legal act to Joint Action 96/443/JHA. It applies to offenses committed: (a) within the territory of the EU, including through an information system, (b) by a national of an EU country or for the benefit of a legal person established in an EU country, including criteria on how to determine the liability of legal persons. More particularly, it provides that EU Member States shall take the necessary measures to ensure the criminalization of the following acts:

(a) publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, color, religion, descent or national or ethnic origin;
(b) the commission of an act referred to in point (a) by public dissemination or distribution of tracts, pictures or other material;
(c) publicly condoning, denying or grossly trivializing crimes of genocide, crimes against humanity and war crimes as defined in Articles 6, 7 and 8 of the Statute of the International Criminal Court, directed against a group of persons or a member of such a group defined by reference to race, color, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group;
(d) publicly condoning, denying or grossly trivializing the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 August 1945, directed against a group of persons or a member of such a group defined by reference to race, color, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group.

However, Member States are given the discretion to punish only conduct which is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting (Article 1 (2)); and also, Member States may opt to make punishable the act of denying or grossly trivializing the crimes referred to in paragraph 1(c) and/or (d) only if the crimes referred to in these paragraphs have been established by a final decision of a national court of this Member State and/or an international court, or by a final decision of an international court only (Article 1 (3)). This is certainly not contributing to harmonizing the legislative framework on cyberhate in the EU and leads to legal uncertainty.

With regard to the criminal liability of legal persons, the Framework Decision provides that the penalties must be effective, proportionate and dissuasive and must consist of criminal or non-criminal fines. In addition, legal persons may be punished by:

- exclusion from entitlement to public benefits or aid;
- temporary or permanent disqualification from the practice or commercial activities;

- being placed under judicial supervision;
- a judicial winding-up order.

In addition to the criminalization of the above acts, racist and xenophobic motivation should be considered as an aggravating circumstance, or, alternatively, considered by the courts in the determination of the penalties.

Both legal acts are not referring specifically to the Internet, as the Additional protocol to the Convention on Cybercrime, but they find application to acts committed in the online environment.

3.3 The Transposition of International and European Legal Acts on Hate Speech by EU Member States

A recent study revealed a wide gap between legislations of EU Members States as regards the penalization of illegal hatred.[32] In particular, it was found that there is a big disparity between national laws implementing the provisions of European and international instruments, as not all of the constituent parts of the offenses are transposed, or additional conditions are imposed on the offenses. In this study, it is mentioned that some differences between national legislations might be unavoidable, as there is a certain margin of appreciation granted to Member States within the framework of the implementation of the provision of international and EU legal acts into national laws.[33] However, the disparities between the national laws are not because of the margin of appreciation, but to a lack of proper transposition, and to the differences that exist between international and EU legal texts.

The study also observes there is coexistence of different provisions targeting close behaviors at national level, but maintaining some differences between them.[34] This coincidence of similar rules is the result of divergent EU and international legal texts. So, e.g., the Council Framework Decision 2008/913/JHA provides for the criminalization of the action of "publicly inciting to violence or hatred", while the additional protocol to the Convention on Cybercrime refers to the action of publicly "advocating, promoting or inciting hatred, discrimination or violence". The transposition of those texts into national law may well lead to the co-existence of provisions sanctioning similar behaviors but with some differences between them.

The result of the divergences that exist between legal texts that target close behaviors in certain countries, and between each of these texts and those adopted in other EU Member States, is that a comparative analysis is a very intricate undertaking, insofar as it attempts to look into the details.[35]

[32]See MANDOLA (2016).

[33]See, *ibid*, p. 11.

[34]See, *ibid*, p. 12.

[35]See, *ibid*, p. 13.

As it is evident, there is a need to harmonize the national legislation of EU countries and therefore, it seems necessary to amend the Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law, and adopt an EU legal instrument with stringent provisions providing for maximum harmonization of national laws.

4 The Conflict with the Right to Freedom of Expression

Without a doubt, the punishment of online hate speech clashes with the right to freedom of expression, which is enshrined in Article 10 (1) ECHR and other international acts, such as Article 11 (1) of the EU Charter of Fundamental Rights, Article 19 (20) of the International Covenant for Civil and Political Rights and Article 19 (2) of the Universal Declaration of human Rights. The right to freedom of expression under Article 10 ECHR includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

It is notable that freedom of expression is recognized as constituting "*one of the essential foundations of (. . .) a (democratic) society, one of the basic conditions for its progress and for the development of every man*".[36] The protection provided by Article 10 ECHR extends to any expression notwithstanding its content, disseminated by any individual, group or type of media.[37] Most importantly, the ECrtHR clarifies that freedom of expression *is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society". This means, amongst other things, that every "formality", "condition", "restriction" or "penalty" imposed in this sphere must be proportionate to the legitimate aim pursued*".[38]

However, it is not an absolute right and it can be restricted, as certain principles should be respected; the relevant measures should be prescribed by law and be necessary in a democratic society, serve a legitimate aim, protect a pressing social need and be proportionate to the legitimate aim pursued.[39] Particularly, as regards hate speech, it is considered as a form of expression that is not protected within the framework of the right of freedom of expression.

[36]ECtHR, *Handyside v. The United Kingdom*, 1976, Application no. 5493/72, §49; *Lingens v. Austria*, 1986; *Sener v. Turkey*, 2000; *Thoma v. Luxembourg*, 2001; *Maronek v. Slovakia*, 2001; *Dichand and others v. Austria*, 2002.

[37]Macovei (2004), p. 17.

[38]ECtHR, *Handyside v. the U.K.*, ibid.

[39]ECtHR, *Sunday Times v. U.K.*, 26.4.1979.

More particularly, the ECrtHR has stated in the decision of *Gündüz v. Turkey* that it may be considered necessary in certain democratic societies to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance, including religious intolerance, provided that any "formalities", "conditions", "restrictions" or "penalties" imposed are proportionate to the legitimate aim pursued.[40] In a similar case, the Court stressed that concrete expressions constituting hate speech, which may be insulting to particular individuals or groups, are not protected by Article 10 of the Convention.[41]

The ECrtHR has issued a wide range of decisions covering different aspects of hate related speech and conduct, which are also relevant in the online environment and which may be summarized in the following categories[42]: ethnic hatred,[43] racial hate,[44] incitement to racial discrimination or hatred,[45] negativism and revisionism,[46] religious hate,[47] incitement to religious intolerance,[48] threat to the democratic order,[49] apology of violence and incitement to hostility,[50] homophobic activities,[51] condoning terrorism and war crimes,[52] denigrating national identity,[53] display of a flag with controversial historical connotations[54] and insult of state officials.[55]

Particular attention should be given to hate speech that is disseminated online. It is, thus, essential to study the case law of the ECrtHR, stressing the importance of the Internet as a means to promote freedom of speech. In particular, in the case *Ahmet Yildirim v. Turkey*,[56] the Court held that the blocking of access to all Google Sites that took place to restrict access to a particular web page that published content insulting the memory of Atatürk, the founder of modern Turkey, which had the effect of also blocking access to the applicant's website, constituted a breach of Article 10 of the Convention. The Court considered that the impugned

[40]ECtHR, *Gündüz v. Turkey*, No. 35071/97, § 40; Sürek v. Turkey (no. 1)[GC], no.26682/95, § 62.

[41]ECtHR, *Jersild v. Denmark*, § 35.

[42]See http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf.

[43]ECtHR, *PavelIvanov v. Russia*, 20.2.2007.

[44]ECtHR, *Glimmerveen and Hagenbeek v. the Netherlands*, 11.10.1979.

[45]ECtHR, *Le Pen v. France*, 20.4.2010; *Jersild v. Denmark*, 23.9.1994; *Soulas and Others v. France*, 10.7.2008; *Feret v. Belgium*, 16.7.2009.

[46]ECtHR, *Garaudy v. France*, 24.6.2003; M'Bala v. France, 20.10.2015.

[47]ECtHR, *Noorwood v. the U.K.*, 16.11.2004.

[48]ECtHR, *I.A.v. Turkey*, 13.9.2005; *Erbakan v. Turkey*, 6.7.2006.

[49]ECtHR, *Communist Party of Germany v. the Federal Republic of Germany*, 20.7.1957.

[50]ECtHR, *Surek v. Turkey* (no. 1), 8.7.1999.

[51]ECtHR, *Vejdeland and Others v. Sweden*, 9.2.2012.

[52]ECtHR, *Leroy v. France*, 2.10.2008; Lehideux and Isorni v. France, 23.9.1998.

[53]ECtHR, *Dink v. Turkey*, 14.9.2010.

[54]ECtHR, *Faber v. Hungary*, 24.7.2012.

[55]ECtHR, *Otegi Mondragon v. Spain*, 15.3.2011.

[56]ECtHR, *AhmetYildirim v. Turkey,* 18.10.2012, no. 3111/10.

measure amounted to "interference by public authority" with the applicant's right to freedom of expression, of which the freedom to receive and impart information and ideas is an integral part. Such interference did not satisfy the requirement of 'foreseeability' and did not afford the applicant the degree of protection to which he was entitled by the rule of law in a democratic society.[57]

The Court highlighted in that decision that the Internet has become one of the principal means by which individuals exercise their right to freedom of expression and information, providing essential tools for participation in activities and discussions concerning political issues and issues of general interest. This also means that the dissemination of racial and hate speech through the Internet is far more effective than though traditional means.

Thus, for example in the case of *Willem v. France*, a mayor in a French city was sentenced by a criminal court to a fine for announcing the boycott of Israeli products, to protest the anti-Palestinian policies of the Israeli Government.[58] The mayor was prosecuted for incitement to discrimination on national, racial and religious grounds. The ECrtHR found no violation of his right to freedom of expression, because he was prosecuted and convicted not for his political opinions, but for calling on the municipal authorities to engage in act of discrimination. The Court noted that the announcement of the boycott was not only made orally at the council but it was also posted on the website of the municipality and thus, the discriminatory nature of the mayor's decision was exacerbated.[59]

In another case, an Internet publication was also given an important role.[60] The case concerned the prohibition of the poster of the Raelian Movement, in which its website was mentioned. The Court examined whether it was appropriate, in examining the necessity of the disputed measure to consider, as the domestic courts did, the content of the Raelian Movement's website, whose address was indicated on the poster in question. In the Court's decision, it was mentioned that[61]:

> Having regard to the principle that the Convention and its Protocols must be interpreted in the light of present-day conditions (see Tyrer v. the United Kingdom, 25 April 1978, § 31, Series A no. 26, and Vo v. France[GC], no.53924/00, § 82, ECHR 2004-VIII), the Chamber took the view that the website did have to be considered because, as it was accessible to everyone, including minors, the impact of the posters on the general public would have been multiplied on account of the reference to the website address.

Subsequently, the Court noted that the impugned poster clearly had the aim of attracting people's attention to the website, as the address of that site was given in bold type above the slogan "The Message from Extraterrestrials". It would thus be illogical for the Court to look solely at the poster itself and consequently, it was deemed necessary to examine the content of the website in question.[62]

---

[57]ECtHR, op. cit., § 67.

[58]ECtHR, Willem v. France, no 10883/05.

[59]ECtHR, op. cit., § 36.

[60]ECtHR, Mouvement raëlien suisse v. Switzerland, No. 16354/06.

[61]ECtHR, op. cit, § 68.

[62]ECtHR, op. cit, § 69.

The ECrtHR dealt specifically with the issue of hate speech on the Internet and with the liability of Internet intermediaries for user-generated comments in two cases.

In the first case, *Delfi AS v. Estonia*, the applicant company, which runs a news portal on a commercial basis, complained that it had been held liable for the offensive comments posed by its readers, which were made about a ferry company in Estonia, although it had removed the comments after their publication.[63]

The Court considered that this case concerned the duties and responsibilities of an Internet news portal that provided a platform for user-generated comments, on previously published content, while some users engaged in speech, which infringed the personality rights of others, and amounted to hate speech and incitement to violence against them. The Court found that in such cases the protection of rights and interests of others, and of society as a whole, may entitle contracting states to impose liability on Internet news portals, without infringing upon Article 10 of the ECHR, if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties.

The second case, *Magyar TartalomszolgáltatókEgyesülete and Index.hu Zrt v. Hungary,* also concerned the liability of Internet intermediaries, and in particular the liability of a self-regulatory body of Internet content providers and an Internet news portal, for vulgar and offensive online comments posted on their websites following the publication of an opinion criticizing the misleading business practices of two real estate websites.[64] The applicants complained about the decision of the Hungarian courts against them, that effectively obliged them to moderate the contents of comments made by readers on their websites, and argued that they had gone against the essence of free expression on the Internet. The Court held that there had been a violation of Article 10 ECHR, as the Hungarian courts had not carried out a proper balancing exercise between the competing rights involved, namely between the applicants' right to freedom of expression and the real estate websites' right to respect for its commercial reputation, as the Hungarian authorities accepted, at face value, that the comments had been unlawful as being injurious to the reputation of the real estate websites.

The outcome of the aforementioned case was different from the *Delfi AS v. Estonia* case, as the facts of the cases were different. Namely, the comments in the former case were offensive and vulgar, but did not constitute clearly unlawful speech and particularly, hate speech and incitement to violence, as was the case in *Delfi AS v. Estonia*. Furthermore, one of the two applicants, Magyar TartalomszolgáltatókEgyesülete, was a non-profit self-regulatory association of Internet service providers, not having economic interests. Clearly, the Court seems to consider the content of comments and imposes restrictions on the right to freedom of expression as far as hate speech is concerned. It also accepted that a provider of internet services who has economic interests might be compelled to exercise more control on user-generated content.

[63]ECtHR, Delfi AS v. Estonia, 16.6.2015.

[64]ECtHR, Magyar TartalomszolgáltatókEgyesülete and Index.hu Zrt v. Hungary, 02.02.2016.

In conclusion, the case law of the ECrtHR offers a useful typology of hate speech and the interpretative tools to deal with the conflict with freedom of expression.

5 Conclusion

As it is evident, the prohibition and penalization of hate speech on the Internet should be without prejudice to the right of freedom of expression. The case law of the Strasburg Court provides guidance on how to strike a balance in cases of conflict.

Some of the countries that ratified the Additional Protocol to the Convention of Cybercrime have adopted a restrictive approach, providing that the act of disseminating racist and xenophobic material is only punishable if the perpetrator intended to commit a hate crime. Greek law, for example, states that the offense of public incitement to violence or hatred or any other act of discrimination against a person or group or persons identified in reference to race, color, religion, genealogical origin, national or ethnic origin, sexual orientation, gender identity or disability, is punishable under the condition that there is an imminent danger to public order or that it contains a threat for the life, the freedom or the bodily integrity of the above persons.[65] Similarly, the offense of the denial of genocide and crimes against humanity and war crimes are punished in case this behavior is presented in a way that can incite violence or hatred, or has a threatening aim or aims at defaming a group or a member of this group.

Particularly, regarding the denial or condoning of crimes against humanity and genocides, a recent decision of the ECrtHR in the case of *Perinçek v. Switzerland*[66] shows that a wise balance between conflicting rights should be struck. This case concerned the criminal conviction of a Turkish politician for publicly expressing the view, in Switzerland, that the mass deportations and massacres suffered by the Armenians in the Ottoman Empire had not amounted to genocide. The Court did not find necessary to subject Mr. Perinçek to a criminal penalty to protect the rights of the Armenian community. To reach this conclusion, the Court considered that his statements touched upon a matter of public interest and did not amount to a call for hatred or intolerance and that those could not be regarded as affecting the dignity of the Armenian Community, to the extent that a criminal law response in Switzerland was necessary.

It is understood that legal measures against hate speech may not prove sufficient to restraint the flood of such online publications. It would also take working together with ISPs, who should adopt a policy of removing offensive content, and use filtering techniques and other innovative technologies to detect and remove such content from the Web.

[65] Article 1 (1) of Law 4285/2014.

[66] ECtHR, *Perinçek v. Switzerland*, No 27510/08.

The EU Code of conduct signed by big internet companies, mentioned above, is an example of such an effort to tackle this thorny issue. It is a soft law instrument, which includes, *inter alia*, requirements to have in place clear and effective processes to review notification regarding illegal hate speech, upon receipt of a valid removal notification to review such request against their rules and community guidelines and where necessary national laws the EU's Framework Decision 2008/913/JHA, to review the majority of valid notifications for removal of illegal hate speech in less than 24 h, to raise awareness with their users and to make it easier for law enforcement to notify the firms directly, etc.[67] Such measures may well confront with the surge of online hate, as it is important to remove the infringing content as soon as possible to minimize any possibility of it becoming viral and having any influence in the online community.

An online reporting portal together with a repository of hate-related speech such as the Hatebase website[68] are also important steps to achieve the objective of combating online hate.

Reporting of hate speech by electronic means should take place at first hand, on national level and be addressed to national law enforcement authorities, but with due respect to privacy. In France, for example, an internet site has been launched, where citizens can report illegal hate speech anonymously, which is reported to law enforcement agencies.[69] On an international level, the Council of Europe has established the Hate Speech Watch, which is a user-generated repository with the objective to trace, share and discuss online hate speech content, but does not report hate speech instances to judicial authorities, regulatory bodies or internet providers.[70]

Hate-speech repositories can be used to identify and eventually filter illegal content. This is the case with the previously mentioned Hatebase.org, which is a big online database of hate speech containing a community-edited vocabulary of multilingual hate speech.[71]

However, restrictions on online speech should be imposed with caution.

It is notable that the Council of Europe Secretary General, Thorbjørn Jagland, following the publication of a relevant study[72], advised the European governments to ensure that their legislation and procedures in this area are clear, transparent and include safeguards for freedom of information and access to information. More particular, he stated that*: "Governments have an obligation to combat the promotion of terrorism, child abuse material, hate speech and other illegal content online. However, I am concerned that some states are not clearly defining what constitutes*

[67]https://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-code.

[68]See https://www.hatebase.org/.

[69]https://www.internet-signalement.gouv.fr.

[70]http://www.nohatespeechmovement.org/hate-speech-watch.

[71]See https://thesentinelproject.org/2013/03/25/introducing-hatebase-the-worlds-largest-online-database-of-hate-speech/.

[72]See http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet.

illegal content. Decisions are often delegated to authorities who are given a wide margin for interpreting content, potentially to the detriment of freedom of expression. On the basis of this study we will take a constructive approach and develop common European standards to better protect freedom of expression online".[73]

References

Anti-Defamation League (2000) Combating Extremism in Cyberspace: The Legal Issues Affecting Internet Hate Speech, 2000. Online available at: http://archive.adl.org/civil_rights/newcyber.pdf

Balkin J (2008) The future expression in a digital age. Pepperdine Law Rev 36

Banks J (2010) Regulating hate speech online. Int Rev Law Comput Technol 24(3):233–239

Code of Conduct on Countering Illegal Hate Speech Online, online available at: http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf; see http://europa.eu/rapid/press-release_IP-16-1937_en.htm

Digital Hate and Terrorism Project (2011) Simon Wiesenthal Center

Digital Terrorism and Hate Report (2015) Simon Wiesenthal Center

European Commission against Racism and Intolerance, (ECRI) Report (2015) Online available in Greek at: https://www.coe.int/t/dghl/monitoring/ecri/Country-by-country/Greece/GRC-CbC-V-2015-001-GRC.pdf

Fleishman G (2000) Cartoon Captures Spirit of the Internet. Online available at http://web.archive.org/web/20141030135629/http://www.nytimes.com/2000/12/14/technology/14DOGG.html

Hasine WB, Galperin E (2015) Changes to Facebook's "real Names" Policy Still Don't Fix the Problem. Online Available at https://www.eff.org/deeplinks/2015/12/changes-facebooks-real-names-policy-still-dont-fix-problem

Johnson DR, Post D (1996) Law and borders: the rise of law in cyberspace. Stanford Law Rev pp 1367 et seq, online. Available at https://cyber.law.harvard.edu/is02/readings/johnson-post.html

Macovei M (2004) Freedom of Expression. A guide to the implementation of Article 10 of the European Convention on Human Rights. Human Rights handbooks, No. 2. Online Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007ff48

MANDOLA (2016) D2.1 Intermediate report. Definition of illegal hatred and implications. Online available at: http://mandola-project.eu/m/filer_public/7b/8f/7b8f3f88-2270-47ed-8791-8fbfb320b755/mandola-d21.pdf

Murray A (2013) Information technology law. The law and society, 2nd ed (2013)

Reidenberg R (1996) Governing networks and rule-making in cyberspace. Emory Law J pp 911 et seq

UNESCO (2015) Countering Online Hate Speech (Iginio Gagliardoe, Danit Gal, Thiago Alves, Gabriela Martinez). Online available at: http://unesdoc.unesco.org/images/0023/002332/233231e.pdf

Weber A (2009) Manual on hate speech. Online available at: http://www.coe.int/t/dghl/standardsetting/hrpolicy/Publications/Hate_Speech_EN.pdf

[73] See http://www.coe.int/en/web/human-rights-rule-of-law/-/rules-for-blocking-and-removal-of-illegal-content-must-be-transparent-and-proportionate.

Chapter 16
Online Surveillance in the Fight Against Terrorism in France

Céline Castets-Renard

Abstract This article seeks to provide a critical analysis of recent French legislation (*loi de programmation militaire*, *loi anti-terroriste*, *loisur le renseignement*, *loisurl'étatd'urgence*), which tends to strengthen online surveillance as part of the fight against terrorism. It will question the efficacy of these measures from the point of view of state security, on one hand, whilst considering the protection of the fundamental rights of individuals, on the other hand, especially considering untargeted means of surveillance.

The balance of interests tilts most probably in favor of protecting the former and shows that there is a high risk of technology being used against people.

1 Introduction

Since January 2015, and the terrorist attacks perpetrated in France, the French legal arsenal has ***seen significant modification***. Several Laws on intelligence and on the fight against terrorism were adopted before *and* after the attacks of November 2015, while the state of emergency was declared for the first time on this date and has since been renewed several times. It would thus be a euphemism to say that the legal order has been subverted by these terrorist acts.

This article aims to realize a comprehensive presentation of the complex and fragmented French legal regulation in a sensitive context of terrorism. The legislator takes measures to increase national security but the risk is to attempt fundamental rights of citizens. For instance, the use of blind technologies to collect mass data is questionable. The legislator has to establish a relevant balance of interest. Firstly, we will present the legal regulation of terrorism in France (Sect. 1.1) and secondly the use of blind technologies to collect mass data (Sect. 1.2).

C. Castets-Renard (✉)
Toulouse Capitole University, 2 Rue du Doyen-Gabriel-Marty, 31042 Toulouse Cedex 9, France
e-mail: Celine.Castets@ut-capitole.fr

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_16

1.1 Legal Regulation of Terrorism in France

Acts of Terrorism

First, we need to define *what terrorism is*. The French Criminal Code (Article 421-1) states that: "The following offenses constitute acts of terrorism where they are committed intentionally in connection with an individual or collective undertaking the purpose of which is seriously to disturb public order through intimidation or terror".[1]

This definition applies to two different types of offense: On one hand, existing general offenses appointed in connection with organizations of terrorist character. It is thus about general offenses committed in particular circumstances which confer them a specific character;- On the other hand, several breaches defined in an autonomous way, without reference to an existing offense.

In the first case, the Article 421-1 points out seven categories of breaches:

1. willful attacks on life, willful attacks on the physical integrity of persons, abduction, and unlawful detention, and the hijacking of planes, vessels or any other means of transport;
2. theft, extortion, destruction, defacement and damage, and computer offenses;
3. offenses committed by combat organizations and disbanded movements;
4. the production or keeping of machines, dangerous or explosive devices (. . .);
5. receiving the product of one of the offenses set out in paragraphs 1–4 above;
6. money laundering offenses;
7. insider trading offenses.

Furthermore, autonomous terrorist offenses are mentioned in the following articles. ~~A~~rticle 421-2 of the French Criminal Code is related to "ecological" terrorism and adds: "The introduction into the atmosphere, the ground, the soil, in foodstuff or its ingredients, or in water, including territorial waters, of any substance liable to imperil human or animal health or the natural environment is an act of terrorism where it is committed intentionally in connection with an individual or collective undertaking whose aim is to seriously disturb public order through intimidation or terror".

Additionally, is a terrorist act, "the participation in any group formed or association established with a view to the preparation, marked by one or more material actions, of any of the acts of terrorism provided for under the previous articles shall in addition be an act of terrorism" (Criminal Code, Article 421-2-1).

The legal qualification is the same in the situation where the act is perpetrated "to finance a terrorist organization by providing, collecting or managing funds, securities or property of any kind, or by giving advice for this purpose, intending

[1]Criminal Code, Art. 421-1: "Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur".

that such funds, security or property be used, or knowing that they are intended to be used, in whole or in part, for the commission of any of the acts of terrorism listed in the present chapter, irrespective of whether such an act takes place" (Criminal Code, Article 421-2-2).

Additionally, the French Criminal Code (Article 212-1) states that: "deportation, enslavement or the massive and systematic practice of summary executions, abduction of persons followed by their disappearance, of torture or inhuman acts, inspired by political, philosophical, racial or religious motives, and organized in pursuit of a concerted plan against a section of a civil population" constitute a crime against humanity punished by criminal imprisonment for life. This crime is imprescriptible.

France was confronted to successive waves of terrorist actions from the 1970s, which led to the adoption of various laws to fight against these kinds of attacks. The law n° 86-1020 (relative à la luttecontre le terrorisme) was promulgated on September 9th, 1986. This text defines the notion of terrorism and mentions more severe procedural rules, incrimination of the praise of terrorism, compensation for victims of terrorism, exemption of punishments for criminals who prevent the realization of an attack, etc. Terrorist activity escapes ordinary jurisdictions because the text creates a body specialized with investigating judges and prosecutors, the central service of counter-terrorism, collectively called "14^{e} section of the parquet" (public prosecutor's department) to treat all cases of terrorism. For acts of terrorism, trials before the magistrates of the Paris Criminal Court have been established. This is an exception to the rule of trial of criminal court before a popular jury. Therefore, the choice was made to apply common rules in criminal procedures of terrorism with exceptions to the means of investigation. For the moment, the creation of an antiterrorist Security Court, which would apply different rules, has been ruled out, at the risk of violating the European Convention on *Human Rights*.

On July 10th, 1991, the law concerning the secrecy of correspondences emitted by way of telecommunications (Law of 10th, 1991, the law concerning the secrecy of correspondences emitted by way of telecommunications) was promulgated. The interception of information or wiretaps for safety reasons can be authorized exceptionally, particularly to prevent terrorism.[2]

The law of July 22nd, 1992, reforming the French Criminal Code (Law of July 22nd, 1992, reforming the French Criminal Code), added terrorist acts to punish them more severely. The exceptional procedure applicable to terrorist acts is maintained indefinitely.

In 1995, another series of attacks occurred in France. The governmental plan Vigipirate was established. The Law of January 21st, 1995 (Loid'orientation et de

[2]Article 4: "Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées". These measures were codified in Domestic Security Code.

programmation pour la sécurité) planned to develop the appeal to video surveillance to increase the protection of the public, as well as sensitive locations. Besides that, the law of February 18th, 1995 (Loirelative à l'organisation des juridictions et à la procédurecivile, pénale et administrative) extended the prescription of crimes and terrorist offenses. In the 2000s, other texts were voted in, in reaction to September 11th, but also to the Madrid (2004) and London (2005) attacks.

Special Laws Covering Cyberterrorism

The Law has also undertaken the development of cyber-terrorism, starting in 2006. The Law of January 23rd, 2006 (Loirelative à la luttecontre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôlesfrontaliers) requires that telecom operators, Internet access providers but also any public institutions providing internet access, such as cybercafés, keep the data of connection (logs) for 1 year. The Law mentions that the access to these logs by the police authorities is no longer submitted to a judge's authorization, but only by a police officer named by the National Commission of Control of the Security Interceptions (CNCIS). We thus have switched from ~~a~~ judicial to administrative control. The Law of March 14th, 2011 (Loid'orientation et de programmation pour la performance de la sécuritéintérieure) (LOPPSI II) now allows the collection of IT data. The Law of December 21st, 2012 (Loirelative à la sécurité et à la luttecontre le terrorisme) extends the authorization, given in 2005, to access connection data (from internet, location, phone bills) in a preventive purpose.

More recently, several other laws related to personal data collection, in a purpose of national security or domestic intelligence, were adopted. Law n° 2013-1168 of December 18th, 2013 (loi de programmationmilitaire) provides for rules concerning connection data collection. Law n° 2014-1353 of November 13th, 2014 (loirenforçant les dispositions relatives à la luttecontre le terrorisme) was adopted prior to the attacks and provides new powers in the battle against terrorism. For instance, Article 5 of that law added a new Article 421-2-5 to the French Criminal Code allowing the prosecution of those inciting or justifying acts of terrorism and increasing sanctions if any such violation was committed using the Internet. The sanctions for inciting or justifying acts of terrorism are up to 5 years in prison and a fine of up to €75,000. If such prohibited speech—are communicated using a public online service, the penalties are increased to up to 7 years in prison and a fine of up to €100,000.[3] The law mentions the ban on the territory of the candidate suspects in the jihad and creates an offense of individual terrorist undertaking. Law n° 2015-912 of July 4th, 2015, the so-called French Surveillance Bill (loisur le renseignement) was adopted following the terrorist attacks of January 2015. This law defines a framework to allow intelligence services to use exceptional ***access means*** to information, such as security-Related Interceptions or use of a technical device allowing the real time

[3] Voss (2015).

location of a person, a vehicle, or an object. Before this Law, these means were used in practice but without legal framework. The utilization of such means of surveillance will be required to respect a procedure defined by the law: written requests will be sent to the Prime Minister who will or will not give his agreement after receiving the National Commission of Control of Means of Surveillance's (CNCTR, formerly the National Commission of Control of Security Interceptions) opinion. This law was completed by the Law n° 2015-1556 of November 30th, 2015 (relative aux mesures de surveillance des communications électroniquesinternationales) concerning surveillance of international electronic communications. Finally, the Law of June 3rd, 2016 (renforçant la luttecontre le crime organisé, le terrorisme et leurfinancement, et améliorantl'efficacité et les garanties de la procédurepénale) creates some measures regarding the financing of terrorism and the efficiency and guarantees of criminal procedures. The law gives judges and prosecutors new investigative means: for instance, technical devices to get connection data directly (IMSI catcher). Moreover, it creates a new offense: regular consultation of jihadist websites (Art. 421-2-5-2 of the Domestic Security Code). The sanctions for consulting these websites are up to 2 years of imprisonment and a fine of up to €30,000.

"State of Emergency" Legal Status

The state of emergency is a form of a state of exception allowing the authorities (prefect, police) to adopt measures restricting freedoms, such as: circulation bans, house arrests, the closure of certain places and administrative searches, both day and night. Therefore, it relieves judges of some of its privileges. The legal regime is organized by a simple law: the Law N° 55-385 of April 3rd, 1955 concerning the state of emergency, adopted before the French Constitution of the Fifth Republic (1958) to face the events connected to the Algerian War (1954–1962). The state of emergency was applied three times to overseas territories during 1980s, then in 2005 during riots in the suburbs. On November 14th, 2015, following the multiple Islamist terrorist attacks committed in Paris over the night of the 13th–14th of November, French President François Hollande declared the state of emergency across all French territory. After other attacks (last one in Nice), the state of emergency was renewed three times by: the Law of February 22th, 2016, the Law of May 20th, 2016, and the Law of July 21th, 2016. It completes the legal regime and increases the administrative authorities' powers.

1.2 Fundamental Rights and Use of Blind Technologies to Collect Mass Data

The growth of laws in the aim of combating terrorism is intended to improve security. Nevertheless, the used means commonly have the effect of restricting

human rights without necessarily increasing security.[4] At the beginning, the goal was essentially to create an exceptional procedure by using targeted technologies against dangerous individuals spotted by the police. However, in a period of serious threat, efficiency may seem insufficient. Consequently, we have seen a political change, which has the effect of questioning the freedoms of the entire population. Two main ways are observable: the state of emergency, which confers more powers to the administrative authorities to the detriment of the judicial authorities, as well as the use of blind technologies to collect mass data on everybody. With this change of scale, the goal is to take better account of the departure of young people born in France for training camps in Syria, with the intention of returning to France to commit terrorist acts. The threat is then inside and outside the country and it is amplified by the digital means of communication, especially via social networks and the *darknet*. The technology became a tool of terrorist propaganda. The police and intelligence services try to take on this reality and provide answers with new technical means. The collection of digital data became an essential tool. Nevertheless, we can wonder if it is a positive change in comparison with information from field agents, which shows its efficiency, even recently in the terrorist attacks in Paris and Brussels.

In any case, the change of scale in the gathering of information is far from being harmless because not only are the liberties of each person reduced, regardless of any reprehensible behavior, but also the efficiency of these devices remains to be proven. Indeed, it is not enough to detain a mass of information. It is still necessary to have the ability to process it and to make connections to recognize the real threat, even when faced with increasingly unpredictable individual profiles.

The legitimacy of this new policy can thus be questioned, from the point of view of the implemented technological means of surveillance and of actors participating in this surveillance, especially on the Internet and in a context of a "state of emergency". Indeed, if the law traditionally refers to targeted information collection (2), massive information collection has been recently allowed to increase the efficiency of the counter-terrorism policy, without democratic control (3).

2 Technology with the Aim of Targeted Surveillance

The means of use to collect information is defined by the French Domestic Security Code (code de la sécuritéintérieure). The 1st Article of the Law N° 2015-912 of July 24th, 2015 on Surveillance, adopted following the terrorist attacks of *Charlie Hebdo* in January, 2015, adds an Article L. 801-1 in the Domestic Security Code: "the respect for private life, in all its components, in particular the secrecy of correspondences, the personal data protection and the residence immunity, is guaranteed by the law. Public authorities can revoke such respect only when

[4]Solove (2011), Tzanou (2015).

necessitated by statutory cases of public interest, in the limits fixed by this law, and in respect for the principal of proportionality".

The authorization and the implementation within national territory of the means of collecting information can be decided only if:

1. they are carried out by an authority having legal competence to do it;
2. they result from a procedure in compliance with the title II of the Code of Domestic Security;
3. they respect missions entrusted to the relevant services;
4. they are justified by the threats, the risks and the stakes linked to the fundamental interests of the Nation mentioned in the Article L. 811-3 of the Code of Domestic Security;
5. the infringements on the respect for private life are proportionate to the aforementioned reasons.

The invoked reasons to use these means of collecting information are mentioned in the Article L. 8113 of the French Domestic Security Code which states that Specialized Services can use the techniques mentioned by the law to defend and promote the fundamental interests of the Nation, such as in the prevention of terrorism.

Disclaimer The aim of this chapter is not to make an exhaustive presentation of all the means of targeted surveillance to prevent terrorism, but to merely analyze the technical processes, especially the ones used on the Internet. Firstly, it will be demonstrated that the law especially the French Domestic Security Code, covers targeted surveillance (Sect. 2.1). Secondly, some rules have been adopted since the proclamation of the state of emergency, which authorized to use in specific circumstances technical means of surveillance of targeted persons (Sect. 2.2).

2.1 Targeted Surveillance as Mentioned by the French Law

The ways of collecting information submitted to authorization are defined in the Title V of the Book VIII of the French Domestic Security Code concerning intelligence. These ways refer to: administrative access to connection data (Article L. 851-1 to L. 851-7); interceptions for safety reasons (Article L. 852-1); audio recording of certain places and vehicles and capture of images and computing data (Article L. 853-1 to L. 853-3); surveillance measures of international electronic communications (Article L. 854-1 to L. 854-9). Theses means of surveillance (Sect. 2.1.1.) are questionable (Sect. 2.1.2.).

Means of Surveillance

The Article L. 851-1 lists the means of surveillance: the collection, by electronic communications operators, as well as Internet access providers and web hosts, of information or documents treated or kept by their networks or electronic communications services, including technical data relative to the identification of the subscription numbers or to the connection of electronic communications services, to the inventory of all the subscription numbers or the connection of a designated person, to the location of the terminal equipment used, as well as the communications of a subscriber concerning the list of the called numbers and the calling numbers, the duration and the date of the communications (meta data).

A service of the Prime Minister is in charge of collecting information and documents with operators. The National Commission of Control of the Techniques of Surveillance (Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR)) has permanent, complete, direct, and immediate access to the information and collected documents. It controls the regularity of the procedure but it gives only an opinion.

According to the Article L. 851-2 of the French Domestic Security Code and for the sole purpose of the prevention of terrorism, the real time collection of information and documents relative to one, previously identified person, capable of being connected to a threat may be individually authorized.

When there are serious reasons for assuming that one or several people belonging to the circle of acquaintances of the concerned person by which the authorization may supply information in conformance with the purpose which motivates the authorization, this one can be individually also tuned for each of these people.

Geo-location Article L. 851-5 of the French Domestic Security Code states that: The use of a technical device allowing the real time location of a person, a vehicle, or an object may be authorized. This measure authorizes the use of geo-location technologies, already admitted in criminal procedure by a law adopted on March 28th, 2014. For instance, the technologies that can be used are: beacons, triangulations of antennas-relay, global positioning systems (GPS), global positioning systems on cameras allowing to locate the place where the photo was taken, and RFID (Radio Frequency Identification).

Security-Related Interceptions Article L. 852-1 of the Domestic Security Code states that: "The interception of correspondence emitted via electronic communications, capable of revealing information, in particular regarding terrorism, may be authorized. When there are serious reasons for believing that one or several people belonging to the circle of acquaintances of a concerned person by the authorization may supply information in conformance with the purpose which motivates the authorization, this one can be also granted for these people".

It inserts the same extension in the circle of acquaintances of the concerned people regarding access to the connection data. This rule is also questionable.

This article adds that: "in the aim of preventing terrorism, can be authorized, for a renewable duration of forty eight hours, the use of a device allowing to open, to delete, to delay or to divert sent or unsent correspondences addressed to third parties, or to acquaint with it deceitfully or still to intercept, to use or to reveal emitted correspondences, transmitted or received by electronic means or to proceed to the installation of devices likely to allow the realization of such interceptions. The correspondences intercepted by this device are destroyed as soon as it seems that they are without link to the delivered authorization".

The means of security-related interceptions used are: wiretaps, microphones and cameras, the interception of correspondences (e-mails, SMS. . .). In these cases, the means allow a targeted surveillance.

Capture of Images and Words in a Private Situation or Place Article L. 853-1 of the Domestic Security Code states that: "the use of technical devices allowing the capture, the fixation, the transmission, and the recording of words pronounced in a private or confidential situation, or of images in a private place may be authorized, when the information cannot be collected in another legally authorized way". The authorization is granted for a maximal duration of 2 months, renewable in the same conditions of duration. Only the authorized agents can use the technical devices. These captures of data are reported at the National Commission of Control of the Techniques of Surveillance (CNCTR).

Capture of Computing Data Article L. 853-2 of the Domestic Security Code states that: "when the information cannot be collected by another way legally authorized, the use of technical devices allows:

1. to access computing data stored in a computer system, to register it, to keep it and to transmit it;
2. to access computing data, to record it, to keep it and to pass it on, such as the display on a screen for the user of an automated treatment of data system, such as he introduces them by seizure of characters there or such as they are received and emitted by audiovisual ring roads.

In the first case, the implementation of authorization of the technique is delivered for a maximal duration of thirty days and, in the second case, for a maximal duration of two months. The authorization is renewable in the same conditions of duration. Sworn agents, belonging to services indicated by decree, can only use these technical devices. The service authorized to turn these reports in to the National Commission of Control of the Techniques of Surveillance (CNCTR) upon its implementation. The Commission can send at any time a recommendation that the operation be interrupted and that the collected information be destroyed.

Breaking Into a Vehicle or a Private Place Article 853-3 of the Domestic Security Code states that: "when the information cannot be collected in another legally authorized way, the breaking into a vehicle or a private place with the intention to set up, to use or to remove technical devices of geo-location, capture of images, sounds or computing data may be authorized. Sworn agents, belonging to

services indicated by decree, can only use these technical devices. The authorization, especially motivated, is delivered for a maximal duration of thirty days and is renewable in the same conditions of duration as the initial authorization. It is valid only for acts of installation, use, maintenance, or withdrawal of technical devices. The service authorized to turn to these techniques reports its implementation to the National Commission of Control of the Techniques of Surveillance (CNCTR). The Commission can send at any time a recommendation that this operation be interrupted and that the collected information be destroyed.

Critical Analysis

These measures are questionable because they particularly endanger human rights, especially Article 8 of European Convention on Human Rights (right to respect for private and family life) and Articles 7 (respect for private and family life) and 8 (protection of personal data) of Charter of Fundamental Rights of the EU. It is indeed a question of watching one or several individuals in real time, not only the suspected person or people themselves but also their circle of acquaintances, simply based on "serious reasons". This surveillance is questionable, in consideration of the European Court of Human Right[5] and European Court of Justice Case Law[6] concerning national framework on surveillance. This Case Law imposed common standards of protection based on the principles of necessity, proportionality, and effectiveness of a judicial control. Its efficiency is also doubtful but the situation is certainly worst in case of use of blind technologies to collect massive data. Besides, these measures are based on the cooperation of digital service providers, which take a major place in monitoring systems.

As we see, these technical measures are meddling and breaching personal privacy, secrecy of correspondence, personal data protection and immunity of the personal residence. Though the Article L. 801-1 of the Domestic Security Code reminds us of a commitment to respect these rights, personal liberty has nevertheless been dealt a blow.

The principles of necessity and proportionality must be respected, but the compliance with these rules shall be subject to control by an independent authority (the CNCTR) whose powers are extremely limited. Besides that, the technical measures are stringent. They can only be implemented by the identified authorities and according to a procedure, under the control of Prime Minister. We note a strong concentration of power in the hands of Prime Minister, without counter-power.

[5]ECHR, 4 déc. 2008, *S et Marper c. Royaume-Uni*, Req. n° 30562/04 et 30566/04; 18 avril 2013, *M.K. c. France*, Req. n°19522/09; 4 déc. 2015, *Roman Zakharov c. Russie*, Req. n° 47143/06; 12 janv. 2016, *Szabo et Vissy c. Hongrie*, Req. n° 37138/14, §73.See also: Korff et al. (2017).

[6]CJEU,8avr. 2014, *Digital Rights Ireland et Seitlingere.a.*,aff.JtesC-293/12 et C-594/12, EU: C:2014:238; CJEU 6 oct. 2015, *Schrems*, aff. C-362/1; 21 décembre 2016, CJEU *Tele 2 Sverige AB c/ Post-ochtelestyrelsen*, aff.C-203/15 etC-698/15.

Moreover, the reasons for using these technical processes, such as expressed in the Article L. 811-1, are unclear and imprecise. If we concentrate here on the facts of terrorism, it is necessary to keep in mind that these motives are wider and numerous. The invoked reasons regard:

1. national independence, the integrity of the territory and national defense;
2. the major interests of foreign policy, the execution of the European and international commitments of France and prevention of any form of foreign intervention;
3. the major economic, industrial, and scientific interests of France;
4. the prevention of terrorism;
5. the prevention of:
   (a) infringements on the republican form of institutions;
   (b) actions aiming at the preservation or at the reconstruction of dissolved groupings;
   (c) collective violence likely to seriously disturb public order;
6. the prevention of crime and organized crime;
7. the prevention of the proliferation of weapons of mass destruction.

Consequently, these measures should, in theory, be taken in exceptional circumstances and in a strictly regulated frame, considering precise purposes and strong suspicions. However, a remarkable flexibility is allowed in reality, without giving the CNCTR the power to exercise real control to prevent misbehavior or abuse. In this way, criticisms abound in France during the adoption of the Law of Surveillance.[7] Thirteen complaints would have been put down.[8]

2.2 Targeted Surveillance in a "State of Emergency"

Data Collection within the Framework of Administrative Searches After the terrorist attacks in Paris in November 2015, the first law concerning the "state of emergency" was adopted on November 20th, 2015 (Loi n° 2015-1501). This law extends the state of emergency for 3 months and plans measures of strengthening of its efficiency. Specifically, this law grants the Minister of the Interior (Ministre de l'intérieur) and the Prefects (Préfets) the ability to order administrative searches in any place, including place of residence, day and night, when there are serious reasons for thinking that this place is frequented by a person whose behavior establishes a threat to safety and public order, except in a place allocated to the exercise of a parliamentary mandate or to the professional activity of lawyers, magistrates or

[7] Latour (2016).

[8] https://www.nextinpact.com/news/99109-devant-cedh-13-plaintes-contre-france-et-sa-loi-renseignement.htm.

journalists. These administrative searches are made by police officers and can apply to access to the stored data in a computer system or a present terminal equipment on the scene where the search takes place or in another computer system or terminal equipment, if this data is accessible from the initial system or available for this initial system. This data can be copied onto any medium. When a breach is noticed, the police officer establishes a report, proceeds to perform any useful seizure, and immediately informs the public prosecutor about it.

The second law concerning the "state of emergency" was adopted on February 19th, 2016 (Loi n° 2016-162). This law (Loi n° 2016-629) once again extended the state of emergency for 3 months. The third Law concerning the "state of emergency" was adopted on May 20th, 2016 and extended the "state of emergency" for 2 months. In this law, administrative searches are no longer authorized, due to the decision of the Constitutional Council.[9] The Council considered that legal requirements allowing administrative authority to copy all the computing data without limit during searches do not comply with the Constitution. The Council decided that: "the legislator did not put in place legal guarantees capable of ensuring a reasonable balance between the objective of constitutional standing of safeguarding public order and the right to respect for private life".

New Rules Concerning the Data Collection Within the Framework of Administrative Searches The latest law related to the "state of emergency" was adopted on July 21st, 2016 (Loin° 2016-987). This law extends the "state of emergency" for six months and enshrines some measures for strengthening counter-terrorism. In particular, there are again some rules concerning administrative searches. However, in the new legislation, the rules are different from the administrative searches mentioned in the first law on the "state of emergency", adopted on November 20th, 2015. Some guarantees were added. It is permitted to proceed to the seizure and subsequent treatment of data, which is contained in a computer system or a terminal equipment present at the scene of the search, if (and only if) the search reveals the existence of elements in the behavior of the concerned person, including IT relating to a threat to public security. The data in any computer system or terminal equipment present at the scene of the search can be seized either by copying or by entering the device, when the copy cannot be performed or completed during the time of the search. The data copying or the seizure of computer systems or terminal is realized in the presence of a judicial police officer. A report of seizure indicating the motives and the inventory of the seized materials is drafted. The data and seized supports are kept under the responsibility of the head of the service that carried out the search. As for the seizure, nobody obtains access before obtaining the judge's authorization. At the end of the search, the authority asks the judge of the Administrative Court (juge des référés) to authorize their exploitation. This judge is in charge of the administrative court in the place of the search. Within 48 h,

[9]Déc. N° 2016-536, DC February 19th, 2016, QPC: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-536-qpc/decision-n-2016-536-qpc-du-19-fevrier-2016.146991.html.

the judge pronounces to the legality of the seizure. In case of reject by the judge, the copied data is destroyed and seized supports returned to their owner. If the data exploitation and seized devices lead to the observation of an offense, this data and devices are kept according to the applicable rules regarding criminal procedure. Decisions are subject to appeal before the judge of the Conseild'Etat within forty-eight hours (en référé). The Conseild'Etat rules within 48 h.

Critical Analysis The administrative judge plays a main role here because he is solely in control of the administrative searches and seizures. In the context of the "state of emergency", the administrative judge is a substitute for the judicial judge, although the judicial judge is the guard of the public liberties, which is very questionable. It is certainly the main criticism, which could be formulated against the rules established by the "state of emergency".

3 Technology with the Aim of Mass Surveillance

The law provides for data collecting concerning the Passenger Name Records (PNR) data (Sect. 2.1) and a mass of data with the aim of analyzing them automatically by algorithmic processing (Sect. 2.2).

3.1 The Massive Collection of Passenger Name Record (PNR) Data

French Law Articles 16 and 17 of the Act n° 2013-1168 of December 18th, 2013 (loi de programmationmilitaire) and Article 1st of the Act n° 2014-1353 (loi de lute contre le terrorisme) concern PNR (Passenger Name Record) data. These measures are codified in several articles, from Article L. 232-1 to Article L. 232-8 of the French Domestic Security Code (Code de la SécuritéIntérieure) (Livre II, Titre III on "automated processing of personal data and public inquiries"). Chapter II is related to "automated processing of data collected on the occasion of international travels".
Article L. 232-1 of the French Domestic Security Code states that: "in the purpose of controlling the borders and fighting against illegal immigration, the Minister of the Interior (Ministre de l'intérieur) is authorized to proceed to the implementation of automated processing of personal data, collected on the occasion of international travels in origin or aimed at States not belonging to the European Union, except sensitive data (Act n° 78/17, Art. 8). He is authorized to collect data:

1. which is on the boarding pass of passengers of airline companies;
2. which is collected from the band of optical reading of the documents of travel, the national ID card and the visas of the passengers of airline, maritime or railroad companies;

3. which is relative to the passengers and registered in systems of reservation and control of the departures when they are held by the airline, maritime or railroad companies.

Article L. 232-2 of the French Domestic Security Code states that: this data processing can be also operated in the same conditions, to prevent and to repress terrorist acts, as well as infringements on the fundamental interests of the Nation.

Their access is then limited to the individually indicated agents and duly authorized:

1. police and National Gendarmerie services especially in charge of these missions;
2. police and National Gendarmerie services, as well as customs, in charge of the safety of international transport;
3. intelligence services of the Ministry of Defense, in the only purpose of the prevention of acts and infringements mentioned in the first paragraph.

Moreover, Article L. 232-3 of the French Domestic Security Code states that: this data processing can be the object of an interconnection with the file of the wanted persons and the Schengen Information System (SIS).

As the above-mentioned Act n° 2013-1168, Article L. 232-7 of the French Domestic Security Code states that: "I. For the needs of prevention and discovery of terrorist acts and infringements on fundamental interests of the Nation, and for gathering of the proofs of these breaches and infringements, and the search of their authors, Minister of the Interior, Minister of Defense, Minister of Transport and Minister responsible for customs are authorized to operate automated processing by data", except for sensitive data (Act n° 78/17, Art. 8).

II. The airline and maritime companies collect and transmit the data relative to the passengers of the travels with destination to and from the national territory, except the travels connecting two points of metropolitan France.

The airline and maritime companies must also communicate the data relative to the passengers registered in their systems of reservation. This data can be kept only for a maximal duration of 5 years.

Finally, Article L. 232-5 of the French Domestic Security Code states the penalties: the fact of any airline, maritime or railroad company not respecting the obligations defined in the Article L. 232-4 is punishable by a 50,000 euro maximum amount for every voyage.

Moreover, the above-mentioned Act n° 2014-1353 (First Article) states that: when the authority notices that the transmitted data in application of the present chapter allows identifying a person as the object of a ban on exit of the territory, they notify the concerned party of the decision of the ban of transport, considering the urgency of the situation. In case of misunderstanding, the penalties of the Article L. 232-5 are applicable.

EU Directive on PNR Data Furthermore, PNR data are also collected in relation with other countries inside and outside the European Union. The Directive 2016/681/EU of the European Parliament and of the council of April 27th, 2016 concerns the use of passenger name record (PNR) data for the prevention, detection,

investigation and prosecution of terrorist offenses and serious crime. These measures regard the Treaty on the Functioning of the European Union, and in particular point (d) of Article 82(1) and point (a) of Article 87(2) concerning the establishing of an area of freedom, security, and justice. Without doubt, the aim of security is the most important here.

According to recital 20, "taking fully into consideration the right to the protection of personal data and the right to non-discrimination, no decision that produces an adverse legal effect on a person or significantly affects that person should be taken only by reason of the automated processing of PNR data. Moreover, in respect of Articles 8 and 21 of the Charter, no such decision should discriminate on any grounds such as a person's sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation". Furthermore, "taking fully into consideration the principles outlined in recent relevant case law of the Court of Justice of the European Union, the application of this Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality. It should also genuinely meet the objectives of necessity and proportionality in order to achieve the general interests recognized by the Union and the need to protect the rights and freedoms of others in the fight against terrorist offenses and serious crime. The application of this Directive should be duly justified and the necessary safeguards put in place to ensure the lawfulness of any storage, analysis, transfer, or use of PNR data".

Finally, recital 36 states that: "this Directive respects the fundamental rights and the principles of the Charter, in particular the right to the protection of personal data, the right to privacy and the right to non-discrimination as protected by Articles 8, 7 and 21 thereof; it should therefore be implemented accordingly".

Nevertheless, these considerations are unclear and lack enforcement. In fact, when we consider the embodied rules we can have much doubt about the respect of privacy and fundamental rights of European citizens.

Subject Matter and Scope Firstly, the scope is wide. The Directive provides for: (a) the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights; (b) the processing of data referred to in point (a), including its collection, use and retention by Member States and its exchange between Member States (Art. 1§1). If a Member State decides to apply this Directive to intra-EU flights, it shall notify the Commission in writing (Art. 2§1). The PNR data transferred by the air carriers shall be collected by the relevant Member State (Art. 6) and even if the Member States shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards (Art. 5), the risk of privacy breach is significant here. Indeed, according to recital 7, "assessment of PNR data allows identification of persons who were unsuspected of involvement in terrorist offenses or serious crime prior to such an assessment and who should be subject to further examination by the competent authorities. By using PNR data it is possible to address the threat of terrorist offenses and serious

crime from a different perspective than through the processing of other categories of personal data".

It seems ambiguous because we consider the "threat" of "unsuspected" people. Moreover, the relevant crimes are non-specific because the Article 1§2 states that: "PNR data collected in accordance with this Directive may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offenses and serious crime". Nevertheless, the annex II specifies a list of offenses, which is long (26 offenses!), not limited to terrorism. Some offenses are considered as "serious crime" but we can have some doubt regarding them, especially concerning: the illicit trafficking in cultural goods, including antiques and works of art; counterfeiting and piracy of products or industrial espionage. Some industrial interests are protected here. If they are significant, we have to ask if it is necessary to include them in an untargeted system of personal data collection, to the detriment of fundamental rights protection.

Collected PNR Data Secondly, the collected data are voluminous (19!) and not related to the personal behavior or the risk created by the data subject, as the collection system is untargeted and concerns all passengers. For instance, this includes: all forms of information payment, including billing address; any advance passenger information (API) data collected (including the type, number, expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time). This intrusive surveillance is not sufficiently justified.

Retention Period for Data Thirdly, the retention period for personal data is long. Article 12§1, concerning the period of data retention states that: Member States shall ensure that the PNR data provided by air carriers is retained in a database for a period of 5 years after its transfer by the Member State on whose territory the flight is landing or departing. There is no explanation to justify this choice. According to recital 25, "The period during which PNR data is to be retained should be as long as is necessary and proportionate to the purposes of preventing, detecting, investigating and prosecuting terrorist offenses and serious crime. Because of the nature of the data and its uses, it is necessary that PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations". However, this is an affirmation, and not proof of the necessity to retain this data.

Personal Data Protection Fourthly, the reference to the Framework Decision 2008/977/JHA concerning the personal data protection is surprising. Article 13§1 states that: "each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress as laid down in Union and national law and in implementation of Articles 17, 18, 19 and 20 of Framework Decision 2008/977/JHA". Nonetheless, this framework decision was repealed by

the Directive 2016/680/EU of the European Parliament and of the Council[10] adopted on April 27th, 2016, the same day as the previously mentioned PNR Directive. Thus, we do not understand this link with the Framework Decision. We can say that the main goal is not really the protection of personal data, and guarantees a higher level of protection in favor of the data subject.

Transfers PNR Data to Third Countries According to recital 31, "To ensure the protection of personal data, such transfers should be subject to additional requirements relating to the purpose of the transfer. They should also be subject to the principles of necessity and proportionality and to the high level of protection provided by the Charter and by the ECHR".

But we have some doubts about it when we consider the Article 11§1, according to which: a Member State may transfer PNR data and the result of processing such data in accordance with Article 12 to a third country, only on a case-by-case basis and if: (a) the conditions provided in Article 13 of Framework Decision 2008/977/JHA are met; (b) the transfer is necessary for this Directive referred to in Article 1 (2); (c) the third country agrees to transfer the data to another third country only where it is strictly necessary for this Directive referred to in Article 1(2) and only with the express authorization of that Member State; and; (d) the same conditions as those provided in Article 9(2) are met. We believe these conditions are not strict enough so there is a high risk for the breach of privacy.

EU-Canada PNR Agreement This risk of breaches of privacy in relation to non-EU countries is confirmed by the PNR agreement between Canada and the EU.[11] This agreement allows the transfer and processing of PNR data concerning passengers flying between EU and Canada. However, in application of Article 218§11 TFEU, the European Parliament has requested the Court to deliver an opinion on the agreement envisaged between Canada and the European Union on the transfer and processing of Passenger Name Record data to enable it to answer the Council of the European Union's request, of July 2014, that the Parliament should approve the proposal for a decision on the conclusion of this agreement.

Opinion of CJEU's General Advocate The General Advocate Mengozzi delivered his opinion on September 8th, 2016 (Opinion 1/15). He suggested that the CJEU reply to the Parliament's request for an opinion along the following lines:

1. The act of the Council concluding the agreement envisaged between Canada and the European Union on the transfer and processing of Passenger Name Record (PNR) data, signed on 25June 2014, must be based on the first subparagraph of

[10]On the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[11]Suda (2013).

Article 16(2) TFEU and Article 87(2)(a) TFEU, read in conjunction with Article 218(6)(a)(v) TFEU.

2. The agreement envisaged is compatible with Article 16 TFEU and Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union, provided that:

   (a) the categories of Passenger Name Record (PNR) data of airline passengers listed in the annex to the agreement envisaged are clearly and precisely worded and that sensitive data, within the meaning of the agreement envisaged, are excluded from the scope of that agreement;
   (b) the offenses coming within the definition of serious transnational crime, provided for in Article 3(3) of the agreement envisaged, are listed exhaustively in the agreement or in an annex thereto;
   (c) the agreement envisaged identifies in a sufficiently clear and precise manner the authority responsible for processing the Passenger Name Record data, in such a way as to ensure the protection and security of those data;
   (d) the agreement envisaged expressly specifies the principles and rules applicable to both the pre-established scenarios or assessment criteria and the databases with which the Passenger Name Record data is compared in the context of the automated processing of that data, in such a way that the number of 'targeted' persons can be limited, to a large extent and in a non-discriminatory manner, to those who can be reasonably suspected of participating in a terrorist offense or serious transnational crime;
   (e) the agreement envisaged indicates, stating the reasons, precisely why it is objectively necessary to retain all Passenger Name Record data for a maximum period of 5 years;
   (f) where the maximum 5-year retention period for the Passenger Name Record data is considered necessary, the agreement envisaged ensures that all the Passenger Name Record data that would enable an airline passenger to be directly identified is 'depersonalized' by masking;
   (g) the agreement envisaged makes the examination carried out by the Canadian competent authority relating to the level of protection afforded by other Canadian public authorities and by those of third countries, and also any decision to disclose Passenger Name Record data, on a case-by-case basis, to those authorities, subject to *ex ante* control by an independent authority or a court;
   (h) the agreement envisaged systematically ensures, by a clear and precise rule, control by an independent authority, within the meaning of Article 8(3) of the Charter of Fundamental Rights of the European Union, of respect for the private life and protection of the personal data of passengers whose Passenger Name Record data is processed.

Moreover, the General Advocate Mengozzi adds that this agreement envisaged is incompatible with Articles 7 and 8, and Article 52(1) of the Charter of Fundamental Rights of the European Union in so far as:

- Article 3(5) of the agreement envisaged allows, beyond what is strictly necessary, the possibilities of processing Passenger Name Record data to be extended, independently of the purpose, stated in Article 3 of that agreement, of preventing and detecting terrorist offenses and serious transnational crime;
- Article 8 of the agreement envisaged provides for the processing, use and retention by Canada of Passenger Name Record data containing sensitive data;
- Article 12(3) of the agreement envisaged confers on Canada, beyond what is strictly necessary, the right to make disclosure of information subject to reasonable legal requirements and limitations;
- Article 16(5) of the agreement envisaged authorizes Canada to retain Passenger Name Record data for up to 5 years for, in particular, any specific action, review, investigation or judicial proceedings, without a requirement for any connection with the purpose, stated in Article 3 of that agreement, of preventing and detecting terrorist offenses and serious transnational crime; and
- Article 19 of the agreement envisaged allows Passenger Name Record data to be transferred to a public authority in a third country without the Canadian competent authority, subject to control by an independent authority, first being satisfied that the public authority in the third country in question to which the data is transferred cannot itself subsequently communicate the data to another body, where relevant, in another third country.

We are waiting for the decision of the CJEU but, if we consider the preceding cases,[12] we think the Court should follow the opinion of the General Advocate Mengozzi. In addition, this opinion proves the high risk for privacy and the protection of personal data with the gathering and processing of PNR data. Especially, the issue of the non-targeted method is raised that confirms the supposed above-mentioned risks. Moreover, the question of the efficiency of such non-targeted data collection is not raised but it is an essential question, because it is useless to collect mass data if we are not able to sort it out and analyze it. We would hope the democratic control of the Judge and the European Parliament[13] will prevent an excessive breach of fundamental rights.

3.2 The Massive Collection of Other Data

Black Box The French Law n° 2015-912 of July 4th, 2015, the so-called "French Surveillance Bill", adds some articles to the French Domestic Security Code. According to the new Article L. 851-3 I:, the law may impose upon electronic

[12]Especially: CJEU, 8 avr. 2014, *Digital Rights Ireland Case* (aff. C-293/12); CJEU, 6 oct. 2015, *Schrems Case*, aff. 362/14.

[13]See the rejection of the EU PNR Directive Proposal by the European Parliament in 2014: https://www.neweurope.eu/wires/background-eu-passenger-name-record-pnr-proposal-an-overview. See also Fahey (2015).

communications operators, internet service providers and web hosts the implementation of automated processing on their networks, which, according to specified parameters in the permit, may detect connections likely to reveal a terrorist threat.

This automated processing exclusively uses the data mentioned in the Article 851-1 (information or documents processed or kept by their networks or services of electronic communications, including technical data related to the identification of the subscription or connection numbers to services of electronic communications, all the subscription or connection numbers of a person, the location of the used terminal equipment, as well as the subscriber communications concerning the list of the called numbers and calling numbers, the duration and the date of the communications). The Prime Minister defines the technical scope of the data processing in regards to the principle of the proportionality. The National Commission of Control of the Techniques of Surveillance (CNCTR) delivers a mere opinion.

IMSI-Catchers However, according to Article L. 852-1 of the Domestic Security Code, the technologies concerning the interceptions for safety reasons evolve and it is now legal for the surveillance services to use the IMSI-catcher, which is a system of false antennas allowing the interception of phone conversations. This device uses a security breach of the 2G. The IMSI is a unique identifying number contained in the SIM card. The IMSI-catchers imitates the functioning of an antenna-relay of mobile telephones, in such a way that devices situated nearby connect there. This equipment then receives the communications of these telephones and can, in certain cases, reach their contents. In turn, it then passes on the communications to the operator and the call takes place normally. The IMSI-catchers can look like suitcases, but some of them may be positioned behind a vehicle or even transported in backpacks. However, this device is not designed for targeted listening and this false antenna intercepts all nearby telephones.

Critical Analysis The rules concerning the "black box" mean that a system of automatic data analysis created by intelligence services has to be installed on the Internet, the access of which is provided by the access providers and major websites. According to the law, this system is supposed "to reveal a terrorist threat" automatically. This measure is very questionable and its opponents called it the "black box" system.[14] Indeed, there is no transparency on this untargeted system of surveillance. We do not really know what is happening: what data is collected? What data is subject to collection? For what reasons? For what period of retention? In the end, everyone's personal data can be collected, regardless of the information on or the behavior of the concerned person.

Concerning the IMSI Catcher The infringement on personal freedoms is also denounced the feeble power granted to the independent authorities. On one hand, the control of the CNIL (National Commission for Information Technology and

[14]Pasquale (2015).

Civil Liberties) is not planned and the power of CNCTR is inadequate because in many legal measures, the Commission only has an opinion power. However, on the other hand, we can note the greater powers of the Prime Minister who is the real decision-maker in the implementation of the techniques of surveillance aimed by the Law (for instance: Article 821-1 of the Domestic Security Code). Moreover, the Conseild'Etat, an administrative judge, exercises the judicial control of these measures. On the contrary, the judicial judge, guard of the public liberties, has been swept under the carpet. Nevertheless, the Constitutional Council validated these measures in its Decision n° 2015-713 DC of July 23th, 2015.[15] In particular, the Council considered that these provisions, which relate to the issue of authorizations for administrative policing measures by the Prime Minister after consulting with an independent administrative authority, do not deprive individuals of the right of judicial relief against the decisions to use intelligence gathering techniques against them; that the requirements of Article 16 of the 1789 Declaration have thus not been violated. Moreover, these provisions do not violate individual freedom.

4 Conclusion

To conclude, we can say that these new untargeted measures to once again fight terrorism are very worrying for French democracy, especially because judicial control is too often far-removed. Even if the threat of terrorism is real and strong in France, we do not have to forget our values. If not, we risk losing everything.

References

Fahey E (2015) Of one shotters and repeat-hitters: a retrospective on the role of the European parliament in the EU-US PNR litigation, May 13, 2015, Forthcoming. In: Davies B, Nicola F (eds) EU law stories. CUP, Cambridge

Korff D, Wagner B, Powles J, Avila R, Buermeyer U (2017) Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490

La lutte contre le terrorisme, Revue Pouvoirs, n° 158

Latour X (2016) Premiers enseignementssur le contrôlejuridictionnel des activités de renseignement. JCP n° 46, 14 Nov. 2016, 1199

Mastor W (2015), AJDA p 2018

Pasquale F (2015) The black box society: the secret algorithms that control money and information. Harvard UniversityPress

[15] http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/version-en-anglais.146958.html.

Solove J (2011) “The all or nothing choice”, in nothing to hide: the false tradeoff between privacy and security. Yale University Press
Suda Y (2013) Transatlantic politics of data transfer: extraterritoriality, counter-extraterritoriality and counter-terrorism. JCMS J Common Market Stud 51(4):772–788
Tzanou M (2015) The war against terror and transatlantic information sharing: spillovers of privacy or spillovers of security? Utrecht J Int Eur Law 31(80):87–103
Voss WG (2015) After google Spain and Charlie Hebdo: the continuing evolution of European Union Data Privacy Law in a time of change, Bus Law 71(1), 2015/2016

Chapter 17
Economic Fraud Crimes on the Internet: Development of New 'Weapons' and Strategies to Annihilate the Danger

Margarita Papantoniou

Abstract Advanced methods of electronic crime have developed in recent years and perpetrators' motive remains mainly the gain of economic profit. The use of the internet and networks as tools to achieve their purpose and the disguise they offer, render their use ideal for the commission of a 'perfect crime'. States and international organisations seem unable to respond equally fast or effectively to the danger of the development of new crimes. However, there is more awareness of the issues involved and legal measures and proposals have been advanced at EU-level and internationally.

1 Introduction

For this chapter, emphasis will be given to specific forms of crime committed on the internet, with an analysis of electronic fraud and the inclusion of a more specific type of cyber-attack (hacking for economic or fraudulent purposes). Although some of these types of cases have not always been characterised as 'crimes', the responses advanced at EU level and internationally use the criminal law as the main forum to fight them and habitually prescribe criminal sanctions, such as imprisonment, for their disposal by Member States.

Fraud has been established as a crime for many years, and different forms of fraud have been stipulated in the legislation as incriminating acts that carry out imprisonment and monetary sentences. Traditionally, fraud involved physical documents or contact with other people. With the development of new technologies, either new forms of crimes have appeared or traditional crimes have been transformed, fraud being one of them. Fraudulent sales, identity crimes, spam and

M. Papantoniou (✉)
School of Law, European University Cyprus, 6, Diogenis Str., Engomi, P.O. Box: 22006, 1516 Nicosia, Cyprus
e-mail: m.papantoniou@euc.ac.cy

T.-E. Synodinou et al. (eds.), *EU Internet Law*, DOI 10.1007/978-3-319-64955-9_17

advance-fee frauds are common examples of electronic fraud. As there is a rapid spread of these crimes and an increasing number of criminals that exploit the anonymity and transnationality offered by the internet, the states should be taking action as quickly as possible and multiplying their efforts to identify existing frauds and prevent the creation of new forms of fraud before they appear. A factor which is of crucial importance in the combat of electronic fraud is the co-operation and co-ordination of actions between Member States.

Another form of economic crime on the internet is the attacks on networks and systems by hackers who use their expertise for money. This has led to the commission of very serious incidents, with huge amounts transferred from banks to offshore accounts in third countries and incidents where companies lose money because of DDoS attacks. This form of crime will also be referred to in this chapter but will be limited only to cases of hacking that is effected for the perpetrator to gain economic profit.

Finally, it is noted that certain legal responses have been advanced at EU-level and internationally but they are not deemed sufficient. The purpose of this chapter is therefore to critically assert the various legal responses to present a general framework to fight economic cybercrime and to discuss whether other non-legal responses would be more efficient in this regard.

For this chapter, electronic fraud is not strictly or narrowly defined as it includes almost all kinds of criminal activity on the internet that result in some financial profit for the offender. However, this analysis has focused mainly on two types of computer-related fraud, the identity fraud/identity theft and phishing/pharming. This analysis has also included hacking for economic purposes as a type of economic cyber-crime. In the first part, these types of offences are presented, in the second part a number of legislative instruments adopted by the EU and the Council of Europe are analysed and finally, the third part sets out the challenges in fighting electronic fraud and outlines some recent measures and case law that several countries adopted to this effect.

2 Forms of Economic Fraud and Cyber-Attacks For Economic Profit on the Internet

2.1 Identity-Related Crimes

Identity-related crime is a compound concept referring to a range of methods used to commit specific forms of deception and fraud but does not include crimes that proscribe the misuse of personal information per se. The creation and misuse of identification evidence lies at the heart of the concept, and the crimes involved entail fraud or obtaining a financial advantage by deception.[1] The terms identity

[1] Smith (2010), pp. 273–301.

crime, identity theft, identity fraud are used interchangeably and without any coherence. The UK Home Office defines identity theft as when sufficient information about an identity is accessed to facilitate identity fraud, irrespective of whether the victim is alive or deceased.[2] The U.S. Department of Justice explains the terms identity theft and identity fraud '(to) refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain'.[3]

There are some commentators that distinguish identity fraud as a crime directed against institutions whereas identity theft as a crime directed against a person.[4] In the U.S., after the enactment of the Federal Identity Theft and Assumption Deterrence Act(Identity Theft Act),[5] identity theft offenders were defined as anyone who '...knowingly transfers or uses, without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law'. In the context of this definition, it has been supported that identity theft includes almost any situation where a person uses the personal information of another for any reason and it has rendered the prosecution of this kind of offences easier.[6]

According to the taxonomy used by the Australasian Centre for Policing Research and the Australian Transaction Reports and Analysis Centre, identity fraud is where a false identity is used to gain money, goods, benefits or services and identity crime refers to offences where the defendant uses a false identity to perpetrate the crime.[7] Perpetrators of fraud usually use the identity of other persons without their consent to obtain advantage (usually financial advantage) for themselves. According to the Internet Crime Complaint Center, identity theft is the third crime type by victim count with an amount loss of USD 57,294,589,[8] rendering it one of the most profitable types of electronic fraud.

It is still an issue that a generally agreeable definition of identity theft remains elusive amongst practitioners, experts and academics,[9] as is the case for the definition of cybercrimes. Sproule & Archer list a number of activities as

[2] http://www.actionfraud.police.uk/fraud_protection/identity_fraud.

[3] https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

[4] McNally and Newman (2008).

[5] 18 U.S. Code 1028(a).

[6] Roberson (2008), p. 3.

[7] 'Results of the Second Meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Crime Misuse and Falsification of Identity' (E/CN.15/2007/8), 2 April 2007.

[8] https://pdf.ic3.gov/2015_IC3Report.pdf, 2015 Internet Crime Report.

[9] Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime:Final Report TR-982-ECNEIL ROBINSON, HANS GRAUX, DAVIDE MARIA PARRILLI, LISA KLAUTZER AND LORENZO VALERIJune 2011 Prepared for DG Home Affairs.

potentially subsumed under identity theft including hacking, phishing and pharming, theft of data storage devices and trafficking in personal information.[10]

The object of any identity fraudster is to use a victim's name and reputation for financial gain and their modus operandi used to be simpler i.e. searching though rubbish to find bills or bank statements, steal from the mailbox and search through unattended bags. Their method is now more sophisticated, and sometimes hackers can use their skills to break into a system and steal the personal information of a large number of individuals. This has been done in various situations resulting in big scandals such as the attack on JPMorgan Chase in 2014 when hackers broke into its network and stole data from 83 million customers. The appearance of social networks provides a fertile field for 'identity thieves' to publicly access and take possession of data from numerous users accounts to thereafter use it for fraudulent purposes.

Identity theft is one of the most potent methods through which the internet has been utilised for fraudulent purposes and draws on other types of cybercrimes. It has found a fertile ground online, where individuals willingly submit personal data to make purchases, participate in social networks and develop digital identities.[11]

On the same note it has been estimated that in Australia there were 2.620 dating & romance scams reported to the Australian Competition and Consumer Commission (ACCC) in 2015 and 32.9% reported losing money.[12] It has been argued that scammers are usually sentimentally intelligent and they spend a lot of time approaching the victim and gaining his trust. When they achieve their goal, it's easier for them to ask for financial 'help', ranging from medical emergencies to failed business ventures to needing to rebook flights to visit the victim.[13]

In the EU, there is no specific offence of identity theft that was enforced by EU legislation, therefore the Member States usually handle these cases by invoking more general concepts or existing crimes set out in their criminal legislation. It can be said that some aspects of the offence are dealt with by other provisions concerning privacy, hacking, fraud, and organised crime.[14] Consequently, the EU's fraud prevention expert group in 2007 pointed out that the penalties provided for identity-related crimes in Europe are so low that cannot be said to be dissuasive. In addition to that, the creation of a new specific offence for these crimes might make successful prosecution 'more worthwhile and easier'.[15]

The Cybercrime Convention also does not include identity theft as a prescribed offence but it covers only elements of it by addressing computer-related fraud,

[10]Sproule and Archer (2006).

[11]Summers et al. (2014).

[12]www.scamwatch.gov.au.

[13]www.scamwatch.gov.au/news/227-million-lost-to-dating-scams-in-2015.

[14]Summers et al. (2014). It refers to Directive 95/46/EC as an example, which protects the rights of individuals 'to privacy with respect to the processing of their personal data' and which places a duty of care upon those holding personal data.

[15]Supra n. 11, p. 247.

illegal access to information systems, data and system interference, and computer-related forgery. Identity theft for fraud has been identified as the fastest growing crime of our time,[16] and victims often suffer financial loss and even worse, they are left with bad credit report or criminal record.

2.2 Phishing and Pharming

Phishing is the creation and use by criminals of e-mails and websites in an attempt to gather personal, financial and sensitive information. According to a report by the Anti-Phishing Working Group, in March 2014, there were 44,212 unique phishing sites detected with 362 unique brands victimised and payment service being the most targeted industry sector[17] Identity theft can also be perpetrated using schemes that employ social techniques, known as 'phishing', where the 'phisher' acquires personal information through fraud by duplicating a trustworthy webpage or impersonating a trustworthy person or business.[18] Phishing has also been said to describe attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person in an electronic communication.[19]

Another technique, 'pharming' uses the way in which internet domain names are resolved to direct unsuspecting users to the false website. When a particular IP address is entered, such as a financial institution, the request is automatically directed to the phishing website mimicking that of the financial institution.

Phishing and pharming are more specific in nature than identity theft and may arise because of identity theft but can also be self-contained acts.[20] Phishing can be used to gain access to the personal data of an individual.

Recent cases involve romance scams where the offender communicates with the victim through social media, acquires personal photographs and other personal material that thereafter threatens to publish on the internet unless a sum is given to him/her[21] or cases where the offender steals credit card details that are used for

[16]By the Federal Trade Commission of the United States, in Parliamentary Assembly, "Europe's fight against economic and transnational organised crime: progress or retreat?", 2001, available at http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewHTML.asp?FileID=9242&lang=en.

[17]Anti-Phishing Working Group, 'Phishing Activity Trends ReportQ 1st Quarter 2014 (2014) 2–7.

[18]Supra n. 17.

[19]Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a general policy on the fight against cyber crime (COM(2007) 267 finalof 22.5.2007), Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14560.

[20]www.microsoft.com/protect/yourself/phishing.

[21]http://www.astynomia.gr/index.php?option=ozo_content&lang&perform=view&id=65601&Itemid=1757.

online sales with the purpose of acquiring goods that are thereafter sold for profit.[22] Another case that concerns electronic fraud that was perpetrated recently in Greece was the advertisement of free supermarket coupons that the user could claim after completing a form and providing personal information. The information was thereafter used to acquire their mobile number and if this was provided by the user he would automatically subscribe to a mobile phone service, incurring further charges. The use of known supermarket chains was making this fraud more convincing for innocent users.[23]

Another popular method used by fraudsters is the approaching of the victim through dating websites, where they obtain personal information of the victim and sometimes they manage to obtain photographs or videos displaying sexual content of the victims. Afterwards they send a link to the victim that takes him/her to a webpage showing his/her photographs and his/her full personal information and extorting him/her to pay a sum to the scammer to take the page down. Usually the methods used for payments are Western Union and MoneyGram, as these services are more difficult to trace.[24]

2.3 Hacking for Economic Purposes

Hacking, DDoS attacks and virus infections are also quite novel terms that describe a variety of criminal behaviours in an online environment. Hacking has been included as a type of cyber-attack and for this section, a more restrictive approach of this term is preferred, by defining it in terms of economic motives and economic consequences. Generally speaking, banks and other financial institutions pay huge amounts to ensure the security of their systems, but in reality they still remain vulnerable and a profitable target for hackers. A fairly recent example was the breach of JPMorgan Chase in 2014, when hackers broke into its network and stole data from 83 million customers. The Bangladesh Bank has also fallen victim of several transactions issued by hackers, worth $101 million[25] and hackers have also stolen UKP 650 million in the world's biggest bank raid through the use of computer viruses to infect networks in more than 100 financial institutions worldwide.[26]

[22]http://www.astynomia.gr/index.php?option=ozo_content&lang&perform=view&id=63854&Itemid=1725.

[23]http://www.safer-internet.gr/sklavenitis-ab/.

[24]http://fraud.laws.com/fraud-news/scam-targeting-women-on-dating-websites-35975.html. https://www.fbi.gov/contact-us/field-offices/sandiego/news/press-releases/fbi-warns-of-online-dating-scams.

[25]Zetter (2016).

[26]Evans (2015).

It has been said that nowadays hackers break into networks to either steal information or make money and it is very difficult to catch them because hacking takes place cross-border and done via proxy servers that mask IP addresses.[27]

Another way for a hacker to obtain money is through ransom ware, which is yet another type of cyber attack. It has been defined as a case where a hacker installs a piece of malware on a computer and then causes a disruption or closure of the entire network. Consequently, the owner of the files has to pay a ransom to the hacker to retrieve and take back his files, although there is no guarantee that the hacker will re-instate/restore the files to the true owner.[28] This malware is quite profitable for hackers or group of hackers, who have developed and spread it from Eastern Europe to the rest of Europe, United States and Canada with approximately 2.9% of compromised users paying the ransom.[29] It is estimated that over $5 million dollars a year is extorted from victims and the real number is probably higher, as there are several gangs exercising this practice.[30]

Finally, DDos attacks are now on the rise, and are defined as attacks to make an online service unavailable by overwhelming it with traffic from multiple sources. Experts can be paid as little as $150 to launch a week-long DDoS attack which will take a small organisation offline.[31] Attacks that exceed 100 Gbps are not easily handled by small organisations and recently it has been observed that attacks to this scale have been effected using booter or stresser botnets that are easily found and cheap to rent.[32] A recent trend is also to blackmail businesses to launch a DDoS attack, therefore extorting huge amounts without even initiating an attack.[33]

From the aforementioned, it can be seen how cyber attacks have now turned into a lucrative business for many computer experts who use their skills and techniques to extort money from people and businesses. There have been attempts to regulate this type of behavior, but more actions need to be taken to hamper this highly destructive activity. Criminal law will only be one of the weapons to use in this regard and the classification of certain cyber-attacks as economic cyber-crimes is recommended as it will have the result of enabling the use of criminal law provisions to deter and punish hackers.

It is therefore evident that computer crime may involve "illegal intrusion into computer networks; extortion using threats to destroy information systems; or penetration of computer data banks for theft or fraud".[34] Attacks against e-mail recipients and commercial web-sites are now the norm of illegal activity on the

[27]Borzykowski (2016).

[28]Microsoft Malware Protection Centre, https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx.

[29]O'Gorman and McDonald (2012).

[30]Supra, note. 27.

[31]http://www.digitalattackmap.com/understanding-ddos/.

[32]Constantin (2016).

[33]Supra n. 32.

[34]Supra n. 16.

internet and the expanding use of the Internet for e-commerce and direct banking, offers more opportunities for criminals to exploit it and requires more effort and proactive steps from international organisations to ensure the trust of consumers.[35]

3 International Legislative Initiatives by the EU and the Council of Europe

3.1 Council of Europe: The Budapest Convention on Cyber Crime: A Leading But 'Old' Piece of Legislation

The predominant international instrument in the field of cybercrime is the Council of Europe's 2001 Convention on cyber crime.[36] The Convention, which was adopted and entered into force in 2004, contains common definitions of different types of cyber crime and lays the foundation for a functioning judicial cooperation between contracting states. It is a binding international treaty that provides an effective framework for the adoption of national legislation. It has to be noted that the majority of Council of Europe's members ratified the convention, as well as numerous non-members, most notably the USA and Canada.[37]

The Convention proposes that Member States adopt legislative provisions to proscribe for various cyber-offences against the confidentiality, integrity and availability of computer data and systems[38] and describes a number of such offences, such as illegal access, illegal interception, data and system interference, misuse of devices, computer-related forgery and computer-related fraud.[39] The terms used to describe such offences are relatively general and require Member States to further define them and set out the subjective and objective elements of the crime prescribed. This means that the characteristics of national legal systems are respected and considered, however such general construction of the offences leads to adoptions of different fault elements for the crimes transposed and therefore different interpretations and constructions of the substantive criminal offences in accordance with the tradition of each Member State.

Additionally, although there is some guidance regarding the mental element of the offences, as it is set out that the offences should be committed intentionally, it is argued that instances where such offences are committed recklessly or negligently are left out of the scope of the Convention's regulation. The inclusion of these forms of 'mensrea' is important, for example when the offence concerns individuals

[35] Supra n. 16.

[36] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[37] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=5Yj3Fo4M.

[38] Supra n. 37, Chapter II, Section 1.

[39] Supra n. 37, Articles 2–8.

who are responsible for the storage and processing of personal data, or when administrators of a website that is used by fraudsters to defraud victims are personally prosecuted.

In relation to the fraud offences prescribed in the Convention, it is concluded that the offence of "computer-related fraud" should be seen 'as a specific application of the offences of cyber attack, when the fraudulent intent of economic benefit is established'.[40] It has also been said that although the computer-related forgery definition has a narrow field of application, it still possesses an increasing importance in the field of digital signatures, especially after the enactment of the Regulation 910/2014.[41] The intentional alteration of the authenticity of electronic identifications set out in the Regulation 910/2014, invokes the offence of computer-related forgery set out in the Budapest Convention.[42]

It is important to note that such an important initiative was taken as long ago as 2001 with no substantial amendments to this day, although technology advances and new methods of cybercrime appear. It is also surprising that a number of Member States have not yet ratified the Convention or the additional protocol to the Convention[43] dealing with acts of racist and xenophobic nature committed through computer systems.

The jurisdictional problem of cybercrime is one of the challenges that the Convention sought to resolve because it manifests itself in the lack of criminal statutes, the lack of procedural powers and the lack of enforceable mutual assistance provisions with foreign states.[44] However, it can be argued that it has failed to do so, as it fails to introduce common elements for the crimes it prescribes, leaving wide discretion to the states that ratify it to implement offences with different objective or subjective requirements. Additionally, the Convention is hampered by the lack of universal participation and also by the fact that the nature of cybercrime is rapidly changing and there is a risk that the amendment process of the treaty will not be equally fast.[45]

Considering that up until today it is the only treaty that has achieved a relative acceptance by a large number of states both within and outside Europe, and given the agreed importance of the Convention despite its defects, there is a pressing need to encourage Member States and relevant third countries to ratify the Convention and even for the European Union itself to become a party to the Convention. However, it should be considered that the drafting of the Convention took place

[40]Iglezakis (2016).

[41]Regulation 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257.

[42]Supra n.41, Iglezakis I (Ed.).

[43]https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f.

[44]Weber (2003).

[45]Supra n. 45.

in 2001, and it is now time to re-draft it or create an entirely new legal instrument that will be updated and more efficient in tackling new forms of crimes. Still, there are doubts over the value of the Convention on Cybercrime in practice, as cybercrime is rapidly changing but the amendment process of treaties is quite time consuming, risking a premature fixation of the law. Furthermore, the Convention does not resolve the extraterritorial jurisdictional issue as it does not set out a common set of crimes.[46]

3.2 European Union: Adoption of Soft Measures and Policies But the Launch of a Regulation or Directive Specifically Targeting Economic Electronic Fraud not Foreseen in the Near Future

The European Union stretched its competence into criminal law matters after the Lisbon Treaty. The Lisbon Treaty provides for a new legal framework for criminal legislation with a strong role for the European and national parliaments, as well as comprehensive judicial control by the European Court of Justice. It is important for the EU to take action in the criminal law policy of its Member States because it can prevent the spread of criminal actions within its borders, and because the more serious crimes, including cyber-crimes, are committed across borders. Such action can help to approximate national laws and create a net from which criminals will not be able to evade liability.

One of the first initiatives adopted by the EU in this regard was their written policy on the fight against cyber crime. In the EU's document 'Towards a general policy on the fight against cyber crime' the term cyber crime is categorised into traditional forms of crime committed over electronic networks, into the publication of illegal content over electronic media and into crimes unique to electronic networks.[47] It recognised that instruments such as identity theft, phishing, spams and malicious codes may be used to commit large scale fraud.

It was also highlighted that the EU has as a goal to fight and prosecute cyber crime in a manner fully respecting fundamental rights, in particular those of freedom of expression, respect for private and family life and the protection of personal data. Most of these rights are inevitably affected in any prosecution of cyber-fraud crime. Therefore, any legislative action taken by Member States should

[46] Supra n. 45.

[47] 'Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a general policy on the fight against cyber crime (COM (2007) 267 final of 22.5.2007) http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l14560&from=EN.

be compatible with such rights, in particular the EU Charter of Fundamental Rights.[48] Consequently, Member States find themselves in a position where they have to balance several tasks, such as safeguarding access and openness,respecting and protecting fundamental rights online and maintaining the reliability and interoperability of the Internet.

The policy set out that all initiatives shall be carried out in full consideration of Articles 12 to 15 of the e-commerce Directive,[49] which apply to online intermediaries and put limitations on whether liability will be imposed for specified activities (mere conduit, caching and hosting). Another Directive that was deemed relevant to the cyber-crime fight was the e-Privacy Directive[50] which also lays down an obligation for providers of publicly available electronic communication services to safeguard the security of their services. Provisions against spam and spyware are also provided there. The Network and Information security policy has since been developed through a number of actions, most recently in Communications on a Strategy for a secure Information society[51] that sets out the revitalised strategy and provides the framework to carry forward and refine a coherent approach to Network and Information security, and on fighting spam, spyware and malicious software,[52] and in the 2004 creation of ENISA.[53]

ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and to raise awareness of NIS, thus contributing to proper functioning of the internal market. It issues recommendations, carries out activities that support policy making and implementation and collaborates directly with operational teams throughout the EU.[54]

[48]Joint Communication to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions ,Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final. Available at https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[49]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).

[50]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201.

[51]Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment",COM(2006) 251.

[52]Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions On Fighting spam, spyware and malicious softwareCOM(2006) 688.

[53]Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (OJ L 77,13.3.2004, p. 1).

[54]https://www.enisa.europa.eu/about-enisa.

The Communication on cyber crime policy titled "Towards a general policy on the fight against cyber crime"[55] consolidated and developed the 2001 Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime[56] that proposed appropriate substantive and procedural legislative provisions to deal with both domestic and trans-national criminal activities. Thereafter, several important proposals followed, in particular the proposal leading to the Framework Decision 2005/222/JHA on attacks against information systems[57] and the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment.[58]

Although there is still no specific EU legislation focusing on online-based fraud, the Framework Decision on Combating Fraud and counterfeiting of non-cash means of payment of 28 May 2001 is an important document that sets out the general policy that should be followed by Member States in this domain. It purports to supplement rules to combat fraud involving non-cash means of payment and to define the types of fraudulent behaviour that should be considered crimes in all EU Member States. It concerns specific conduct that has to do with payment instruments, which are defined as a 'corporeal instrument, other than legal tender (bank notes and coins), enabling by its specific nature, alone or in conjunction with another (payment) instrument, the holder or user to transfer money or monetary value. . .'.[59] Offences which are set out in the Decision include the intentional theft or unlawful appropriation of a payment instrument,[60] the counterfeiting or falsification of a payment instrument for fraudulent uses[61] and the fraudulent use of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument.[62]

Article 3 describes offences related to computers such as introducing, altering, deleting or suppressing computer data, in particular identification data and Article 4 sets out offences related to specifically adapted devices, such as the fraudulent making, receiving, obtaining, sale or transfer to another person of computer programmes the purpose of committing any of the offences described under Article 3.

It has been argued that the most common types of computer fraud are covered by this Framework Decision.[63] Two reports were issued from the Commission based

[55]COM/2007/0267 final, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52007DC0267&from=EN.

[56]COM(2000) 890, 26.1.2001.

[57]OJ L 69, 16.3.2005, p. 67.

[58]OJ L 149, 2.6.2001, p. 1.

[59]Article 1(a) of the Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment [2001] OJ L149/1.

[60]Supra n. 60, Article 2(a).

[61]Supra n. 60, Article 2(b).

[62]Supra n. 60, Article 2(d).

[63]Gercke (2009).

on Article 14 of the Framework Decision,[64] the most recent one indicating that the majority of Member States transposed the provisions of the Framework Decision into their legislation, were in the process of implementing new legislation to transpose them or indicated that their national legislation already covered the offences set out in the Framework Decision.[65]

Another important document containing various initiatives that the EU plans to take is the Communication on cybersecurity strategy of the EU—An open, safe and secure cyberspace, which places the drastic reduction of cybercrimes as one of EU's top priorities.[66] Although, it outlines some very important measures that can be taken to render the online environment safe and open, it highlights that it is predominantly the task of Member States to deal with security challenges in cyberspace.[67] This is ultimately one of the biggest lapses in any supranational strategy regarding cyberspace as Member States have to follow a common pattern to deal effectively with the threats posed online. EU's performance in this regard, can only be achieved if mutual steps are taken by all Member States, so that cyber criminals will not have a choice over residing in EU countries with more lenient online fraud legislation.

EU's strategy acknowledges that right operational tools and capabilities must be adopted as criminals often exploit the anonymity of website domains and stresses that the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross-border approach to respond to this growing threat. For this purpose, strong and effective legislation must be adopted by Member States and it refers to the Council of Europe Convention on Cybercrime, as well as to the Directive on combating the sexual exploitation of children online and child pornography,[68] as indicative examples of effective legislation in this regard.

Another strong point made in the Communication is that all Member States should have updated operational tools to combat cybercrime and to this end, Member States shall strengthen their capability to investigate and combat cybercrime through EU's funding programmes. It recognises as a vital step that contact is made between research, law enforcement agencies and the private sector, similar to the on-going work carried out by the Commission-funded Cybercrime Centres of Excellence already set up in some Member States. To this end, training courses should be desinged to assist law enforcement in acquiring the required

[64]Report from the Commission, 20 April 2004, COM (2004) 346 final, and Report from the Commission, 20 February 2006, COM (2006) 65 final.

[65]Most notably, Latvia, Lithuania, Poland, Czech Republic, Slovakia, Finland, France, Germany, Ireland, Italy, the Netherlands, Spain, Sweden, the United Kingdom, Austria, Greece and Luxembourg.

[66]https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[67]Supra n. 67, p. 4.

[68]Directive 2011/93/EU replacing Council Framework decision 2004/68/JHA.

expertise to tackle cybercrime and therefore address the private sector's and individuals' concern regarding their adequacy in fighting electronic crime.

Directive 2013/40/EUon Attacks Against Information Systems: A Weapon in the Fight of Cyber Attacks That Does Not Specifically Target Hacking for Economic Purposes

The Directive on attacks against information systems replacing Council Framework Decision 2005/222/JHA has been published on 23 July 2011 and one of its objectives is to approximate the criminal law of the Member States in the area of attacks against information systems. As per Recital no.6 "large-scale cyber attacks can cause substantial economic damage".

The Directive has also made sure that criminal penalties will apply in cases of commission of the offences prescribed by the Act and an increased term of imprisonment is provided where three aggravating factors are involved: when the offences are committed within the framework of a criminal organisation, when serious damage is caused or when committed against a critical infrastructure information system. An explanation of what serious damage includes can be derived from the subsequent Directive adopted to ensure cybersecurity, the NIS Directive[69] and Article 6 which provides that when determining the significance of a disruptive effect, a number of factors could be considered, including the impact of incidents on economic and societal activities. Therefore, the economic aspect of cyber-attacks is given legislative recognition as an aggravating factor that will increase prescribed penalties. In addition to that, digital service providers shall notify the specified authorities of any incident that has a substantial effect on the provision of a service, and the extent of the impact on economic activities is one of the parameters that will be considered to determine whether an incident has a substantial impact or not.[70]

Directive 2016/1148/EU Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union

A new development and one of the most important initiatives taken by the EU in the field of cyber-security is the Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.[71] It

[69]Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A194%3ATOC&uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

[70]Supra n. 70, Article 16(4)(e).

[71]http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

was adopted on 6 July 2016 and the date of transposition by all Member States is set to 10 May 2018. It imposes the obligation on Member States to cooperate with each other in relation to network and information security and imposes responsibilities on 'operators of essential services' and 'digital service providers'.

It is the first EU-wide legal instrument which provides for common rules on cybersecurity. It purports to achieve a common level of security of network and information systems whithin the EU by means of improved cybersecurity capabilities at national level, increased EU-level cooperation and risk management and incident reporting obligations for operators of essential services and digital services providers.[72] Consequently, serious incidents of cyber fraud will be treated more readily by Member States and the seriousness of such incidents in essential services will be reduced to a minimum. In its Communication of 5 July 2016, the European Commission encourages Member States to make the most of NIS coordination mechanisms. Building on those, the Commission will propose how to enhance cross-border cooperation in case of a major cyber-incident.[73]

Key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the Directive. These responsibilities include taking appropriate and proportionate technical and organisational measures to manage risks posed to the security of network and information systems they use and taking appropriate measures to prevent and minimise the impact of incidents affecting the security of their network and information systems. Operators of essential services and key digital service providers will both be subject to oversight by designated national authorities that may issue binding insturctions to remedy any deficiencies identified.

It is noteworthy that this Directive is a minimum harmonisation instrument, so Member States may issue or enact further obligations beyond those specified by the Directive. The incidents that will be notifiable by the operators of essential services are not clearly defined by the Directive but three parameters should be considered: Number of users affected, Duration of incident and Geographic spread. For Digital Service Providers, two more additional parameters are set out, the extent of the disruption of the service and the impact on economic and societal activities. These parameters may be further clarified by means of guidelines adopted by the national competent authorities acting together within the Cooperation Group or by the Commission by means of implementing acts.

The Directive sets out that it leaves it to the discretion of the Member States to adopt penalties that are effective, proportionate and dissuasive, without further clarifying the nature of such penalties and whether criminal sanctions may be foreseen as well in the national legislation.

[72] europa.eu/rapid/press-release_MEMO-16-2422_en.pdf.

[73] http://europa.eu/rapid/press-release_IP-16-2321_en.htm.

European Commission Vice-President Andrus Ansip welcomed the adoption of the Directive on Security of Network and Information Systems by stating that: "If we want people and businesses to make the most of digital services, they need to trust them. . . The Directive on Security of Network and Information Systems is the first comprehensive piece of EU legislation on cybersecurity and a fundamental building block for our work in this area."[74]

4 Challenges in Fighting Electronic Fraud and National Measures Adopted: A Lernaean Hydra?

From the beginning of this section it has to be highlighted that challenges in fighting electronic fraud are usually common with challenges encountered by any other form of electronic crime.

4.1 Non-Reporting of Cyber-Crimes by Private Organisations/Lack of Cooperation Between Private Organisations and Law Enforcement Authorities

According to the Global Economic Survey of 2016,[75] cybercrime is the second most reported economic crime affecting organisations and as a consequence, it can be said that organisations are severely concerned by crimes committed electronically and costing them money. The survey distinguishes between two different categories of cyber-crime: Cyber-fraud which includes identity and payment card theft which rarely pose a threat to organisations and transfer of wealth-IP attacks, which involves international cyber espionage and the theft of trade secrets, product information and they are more difficult to detect although they cause severe damage and even destruction of the organisations that have been victims.[76] Among survey respondents, reputational damage is considered the most damaging impact of a cyber breach—followed closely by legal, investment and/or enforcement costs.[77]

One of the biggest challenges an organisation has to face is that their detection and control programmes keep up with the pace of change. Electronic fraud is evolving, and becoming a more complex issue both for organisations and economies. With local law enforcement unable to confront these changes, the onus is left

[74] http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm.

[75] Global Economic Survey of 2016 by WaterHouseCoopers.

[76] Supra n. 76, p. 19.

[77] Supra n. 76, p. 18.

on the businesses to protect themselves and their stakeholders from economic crime committed online. A private step that will assist organisations in better combating cyber incidents is the development of a cyber incidence response plan, and it seems that only 37% of the organisations have developed such a plan.[78] For any Member State to effectively fight cyber-fraud it is a *sine qua non* requirement that even with a private plan in place, organisations should still involve law enforcement agencies in investigating a cyber crime affecting them. In this way, law enforcement agencies will be aware of any novel methods for effecting cyber-crimes and may alert other private organisations and individuals of the dangers of any new form of electronic fraud. Furthermore, the law enforcement agents may better preserve the evidence and may take all necessary actions to prevent it from re-occurring. Moreover, they could also use their specialised personnel and enforce cooperation agreements with other bodies to fight any type of cyber crime.

To this end, the U.K. has recently expressed its intention to incriminate the non-reporting of economic crimes even if such an omission is made by a legal person. Firms will face huge fines for failure to report economic crime.[79] This measure will enable the prosecution of economic crime, with a particular focus on economic crime committed electronically, since the effect of this measure will be to expose any new type of cyber-attack on organisations, as it has been reported that such crimes are not usually reported by organisations because of their concerns for harm to their reputation and because they do not trust the efficiency of the government system in dealing with electronic crimes.[80] More recently, the U.K. government has announced that it "will soon consult on plans to extend the scope of the criminal offence of a corporation 'failing to prevent' offending beyond bribery to other economic crimes, such as money laundering, false accounting and fraud."[81]

A recent incidence that was reported and showed the vulnerability of private organisations to fraud despite some protections that were in place, concerned the acts of a pair for a decade-long insider fraud scheme. The main actor lead a sophisticated fraud scheme that involved the identity theft of a business contact

[78]Supra n. 76.

[79]Reported by Jeremy Wright QC MP, at the Cambridge International Symposium on Economic Crime. The model for such provision will be as per section 7 of the Bribery Act, which was viewed with widespread alarm in the business community and it was argued that it was unfair, heavy and put the onus of proof on the firms , cited in www.ubdeoebdebt.co.uk/news/business/news/companies-face-prosecution-if-they-fail-to-stop-economic-crime-9706296.html, http://www.independent.co.uk/news/business/news/companies-face-prosecution-if-they-fail-to-stop-economic-crime-9706296.html.

[80]Supra n.76. In the report, it was estimated that close to half of the organisations surveyed believe that local law enforcement is not adequately resourced to investigate economic crime, leaving the responsibility for fighting economic crime on organisations.

[81]On 5 September 2016, in the Cambridge Symposium on Economic crime, available at https://www.gov.uk/government/speeches/attorney-general-jeremy-wright-speech-to-the-cambridge-symposium-on-economic-crime.

to receive commission payments into his bank account and adjusted his tactics in response to any new measure adopted by the company.[82]

Another issue that arises in many member states concerns the apparent lack of exchange of information, expertise and best practices between the public and the private sector. Private sector organisations or companies are keen to protect their secrets and other models developed in business and for this reason they are reluctant to report fraud incidences to the law enforcement authorities. In addition, they do not usually have any legal obligation to report such incidences, unless there is a personal data breach.[83] Consequently, there is no cross-reference between private and public sectors of relevant information on electronic fraud incidences, therefore weakening the position of the law enforcement authorities to create efficient policies.

Given that in such circumstances the personal data protection rules are insufficient, it is pertinent that the legislation provides a shield for private companies that communicate issues and incidences of electronic fraud to the law enforcement agencies so that they will be covered in case an incriminating issue comes to light. In addition to the above, the law shall clearly protect their business secrets[84] and other information that may be disclosed in case an investigation is carried out. Private and public sectors are equally concerned about the commission of cyber-fraud and both wish to develop methods to identify and prevent any form of cyber-fraud that will result to economic harm of organisations, individuals and governments, without any adverse consequences on any of them.

While national judicial and law enforcement authorities in Europe cooperate closely via Europol, Eurojust and other structures, there remains an obvious need to strengthen and clarify responsibilities. Because of the global nature of information networks, no policy on cyber crime can be effective if efforts are confined within the EU. Criminals can not only attack information systems or commit crimes from one Member State to another, but can easily do so from outside the EU's jurisdiction. The problem becomes more acute because there are different systems within the EU (common law system and civil law system) that prescribe different procedures when cases of electronic fraud are investigated or prosecuted.

[82]http://www.cps.gov.uk/news/latest_news/pair_sentenced_for_decade_long_insider_fraud_scheme/, http://www.cityoflondon.gov.uk/.

[83]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive95/46/EC (General Data Protection Regulation). The Regulation entered into force on 5 May 2016 and shall apply from May 2018.

[84]A recent Directive with direct relevance to the protection of business secrets is Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

4.2 Harmonisation of Laws/Measures to Confiscate and Forfeit Illicit Profits

Another challenge posed in the fight against cyber-fraud is tracing offenders and victims, who may be located anywhere in the world. The nature of computer related fraud is also increasingly transnational requiring increasing efforts for harmonisation of laws and effective cooperation between law enforcement agencies.[85] National laws, as well as international binding and non-binding instruments, may be the starting point from which the countries establish a solid framework to exchange information in relation to electronic economic crimes, cooperate and seek remedies in other jurisdictions.

Issues that need to be clarified to effectively fight electronic fraud crime are the regulation of tracing proceeds of economic crime on the internet and the matter of transnational confiscation and forfeiture. A number of international conventions place a positive duty on state parties to enact or amend their legislation to provide for confiscation of the proceeds of crime.[86] The Directive of the EU on Confiscation[87] is regarded as a very positive step on the fight against organised crime putting on onus on all Member States to incorporate special provisions in their legislation regarding tracking and confiscating illicit money. The Directive only concerns certain types of crimes, the more serious ones, including fraud and counterfeiting on non-cash means of payment[88] and organised crime.[89] However the means to trace, freeze, manage and confiscate the proceeds of crime, especially in cases where a transnational element is present, are often very lengthy and costly and require a lot of resources whereas the outcome is not always predictable.

The complexity of this matter is evident in the guidelines provided by the English Courts for applications to enforce a worldwide freezing order.[90] These guidelines try to balance the conflicting rights at stake, the interests of the parties and other potentially third parties and the efficiency of such freezing orders. In practice, these guidelines also require the parties to provide evidence as to the applicable law and practice in the foreign court and the assets believed to be located in the jurisdiction of the foreign court, having as a consequence an increase to the costs of such applications and results in undue delay and sometimes with the effect of alerting the persons concerned. It has to be considered that criminals often move

[85] Russell (2014).

[86] Inter alia, United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, United Nations Convention against Transnational Organised Crime, 2008 Convention of the Council of Europe on laundering, search, seizure and confiscation of the proceeds of crime and on the financing of terrorism.

[87] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042.

[88] Supra n. 88, Art.3(c).

[89] Supra n. 88, Art.3(h).

[90] Dadourian guidelines, in the case of Dadourian Group Int. Inc v Simmes & Others [2006] EWCA Civ 399.

the proceeds of illegal activity in different countries, interchanging between common law and civil law jurisdictions so as to make it more difficult for the authorities to acquire freezing orders from the courts on time to hamper the transfer and legalisation of proceeds.

In any kind of scenario, freezing and confiscation orders are complicated and require a lot of time, resources and specialised personnel to effect them and this renders their use quite limited in practice.

4.3 Dilemma of Enacting New Criminal Laws or Using Existing Legal Provisions

According to Jonathan Clough, there are traditional fraud offences, which although assuming new forms, may be prosecuted under general fraud offences but this presents challenges such as the application of traditional provisions to new forms of property, terms such as 'obtaining', 'belonging to another' and the issue of consent.[91] Therefore, terms that have appeared recently or have a different meaning within an online environment need to be defined clearly and precisely to clarify any ambiguity or doubt over their true meaning.

In addition to the aforementioned, there is lack of legislation that would apply in all European Member States that would set out the required elements of computer related fraud and would lead to the same application of the offence in all countries of the European Union. Another issue of concern is whether the traditional criminal system is adequately equipped to prosecute computer-related fraud especially when perpetrated in a number of different countries and jurisdictions. This issue grows when Member States have to confront and manage complex fraud cases.

Turning into identity-related crimes, it seems that countries attempted to address them in different ways and only a minority of them has enacted specific legislation to address this matter.[92] Most of the countries use existing fraud or forgery legislation. The most pertinent issue that needs to be determined before introducing an international instrument specifically for identity-related crimes is the definition of identity theft which has not been agreed on.

With regards to criminalising identity-related conduct, a notable challenge is the difficulty of establishing possession of data in digital form,[93] as well as the danger of criminalising simple possession of identity information without the requirement of further evidence concerning the possessor's mental state in respect of that information. Additional safeguards should be put in place for defendants in this

[91]Clough (2015).

[92]Most notably, the United States.

[93]Clough (2010).

regard and any new law should also provide for defences such as 'reasonable excuse'.[94]

It has been agreed that already some soft measures have been taken to combat cybercrime which can be applied to cases of electronic identity theft such as cooperation between national investigative bodies.[95] An issue that has been recognised in this regard, is that of prioritisation because in cases with an internet component, investigations can be complex and expensive. It was shown that some cases were not followed up on, simply because of a real or perceived disproportion between the harm suffered by the victim and the resources required to take action.[96] It was also shown in the same report that a common criminalisation framework does not pose a significant barrier to combat identity-related theft as other existing criminal provisions can be used, but cooperation between countries in the investigation stage and actual follow-up of reported cases continues to be an issue.

The motive for committing this sort of crime is partly economic,[97] and as a result of this or related crimes, businesses and people lose an estimated $16 billion to $50 billion per year.[98] It has been said that legal responses in relation to identity theft usually take the form of a civil action, which is inadequate especially given the development of new behaviours and the misuse of internet access.[99]

In France, a new offence was added in the French Penal Code, stipulating that the act of usurpation of the identity of a third person or of using one or more data which identify him to disturb his or others tranquility, to detract his honour or reputation is an offence. It also specifies that it can be committed in an online network of communication. Problems with this definition focus mainly with the proof of mens rea.

In relation to evidence that links people to a certain identity crime there are many gaps and it is difficult to use traditional rules of evidence and apply them to the digital environment. In this regard, and to safely ascertain the theft of an identity on the internet, it has been suggested that the generalisation of smart cards, which use strong cryptographic algorithms and universal modules of connection to create a certified electronic identity would help to secure the online transactions.[100] In addition to that, concerns have been raised about the importance placed on IP addresses and the link to the owner of a computer.

In the U.K., the new Fraud Act of 2006 creates a general offence of fraud that covers phishing and other types of fraud committed online as the actus reus of the offence is proven if a person dishonestly makes a false representation and this

[94]Supra n. 94, p. 376.

[95]Council Framework Decision 2005/222/JHA.

[96]Robinson et al. (2011).

[97]2007 Study for the Centre for Identity Management and Information Protection (CIMIP), in http://www.utica.edu/academic/institutes/cimip.

[98]Vieraitis et al. (2014).

[99]Jougleux (2012).

[100]Supra n. 100.

representation may be express or implied. The mensrea requirement is satisfied by the element of dishonesty[101] and furthermore with the intention of the offender to make a gain for himself or another or to cause loss to another or expose another to a risk of loss.[102] Another element that must be proved is that the offender knows that the representation is or might be untrue or misleading.[103]

The new Fraud Act of 2006 has been characterised as removing the deficiencies on fraud and incorporating principles which conform to the concept of technological neutrality, as well as removing procedural and technical obstacles from the prosecution of online fraudsters, but it is still considered as insufficient to manage the complexity which is inherent in the interaction of users with data, devices and networks.[104] It repealed the 'old' traditional offences that were constructed narrowly over the years, such as obtaining property by deception and obtaining pecuniary advantage by deception, to include the new concepts of fraud and the evolving use of the internet to commit crimes.

As with other European countries, there is overlap with theft and other offences, which leads to prosecutorial dilemmas as it is left to the prosecutor to choose which charges to include in the indictment. However, if the prosecutor decides to include all possible offences, more resources will be needed to collect sufficient evidence and to gather testimony on all available charges. This choice to include all offences that may be invoked for a certain conduct can create uncertainty for the Defendant who can more easily invoke a breach of article 6 of the ECHR if he is not able to efficiently prepare his defence. In addition to the above, different charges might require a different mental element. Therefore, prosecutors should be very careful when deciding which offence properly reflects the criminal behaviour concerned. The ultimate choice is left in many cases to the prosecutors, who shall be very well informed and experienced in this kind of cases and certainly, in the online environment. Therefore, it would be crucial for prosecutors to have IT knowledge and train to familiarise themselves with technical terms and the operation of computer systems.

A recent paper aimed to demonstrate the causes of failure of some fraud prosecutions.[105] Amongst the factors discussed that lead to failure of many fraud prosecutions, are the mass of documentary evidence, lack of effective management of the trial process and the length of these cases due to presentation of complex facts and vast amounts of documentation to a lay jury. Therefore, a proposition was made that such cases could be decided by tribunals without juries.[106]

In addition to the above, the effective deterrence of economic e-criminals is hampered by the hesitation of courts to impose heavy sentences on offenders of

[101] Section 2(1)(a) of Fraud Act 2006.

[102] Section 2(1)(b) of Fraud Act 2006.

[103] Section 2(2)(b) of Fraud Act 2006.

[104] Savirimuthu (2008), p. 188.

[105] Wright (2006).

[106] Supra n. 106.

electronic fraud when they have not proceeded to cause actual harm or losses on the victims or when their behavior does not extend to a long period.

In the U.K. case ***R v. Brown***[107] a conviction for offences relating to possession on a computer of stolen bank and credit card details was concluded. What was initially considered when determining the sentence was the potential loss from the accessed accounts although no actual loss was suffered. However, this rationale was overturned by the Court of Appeal which reduced the sentence imposed solely on the lack of actual loss. In R v Crosskey (Gareth),[108] the Defendant had accessed the Facebook account of an actress's manager, accessed and copied the actress's private emails and contacted magazines offering to reveal information about her. The appellate court referred to a number of aggravating factors including the element of deceit involved, the boasting to others and the harm to the actress. However, it reduced the sentence imposed, considering his previous good character and the short period of the occurrence of the events.

In ***R v Mangham (Glen Steven),***[109] the defendant pleaded guilty to unauthorised access on Facebook's computers and modifying the functionality of various programs, costing approx. 200,000 USD for Facebook to respond to the incident. On appeal, the court identified a number of aggravating factors which would be 'bear on sentences in this type of case'. Among those mentioned by the court were whether the offence is planned and persistent, the nature of the damage to the system, the cost of the remediation, motive and benefit and whether there was any attempt to reap financial benefit by the sale of information accessed.

However, another view taken was that the legislature should not keep passing new laws to ensure that the new crimes are covered, but the existing criminal law may equally apply to 'new' types of crime because they are usually a different version of an existing crime. Arguments advanced in favour of the above proposition include the unnecessary expansion and complication of the criminal code, the introduction of ambiguous laws and the lack of technical expertise by legislatures to frequently update technology-based legislation.[110] In the U.S., the Computer Fraud and Abuse Act ("CFAA")[111] was passed to outlaw conduct that victimises computer systems and in response to the growing abuse of computers. There are also other laws that treat computers as arenas for crime, such as identity theft, obscenity and pornography.[112] This special law has been criticised for unnecessary duplicating existing crimes and for lack of proper definition of new terms such as

[107][2014] EWCA Crim 695.It has been brought under the Computer Misuse Act 1990 together with the Fraud Act 2006.

[108][2012] EWCA Crim 1645; [2013] 1 Cr. App. R. (S) 76.

[109][2012] EWCA Crim 973; [2013] 1 Cr. App. R (S.) 11.

[110]Simmons (2016), also citing Sun Beale S., The Many Faces of Overcriminalization: From Morals and Mattress Tags to Overfederalization, 54 Am U.L. Rev., 747 (2005), Struntz W., The Pathological Politics of Criminal Law, 100 Mich. L. Rev. 505 (2001).

[111]18 U.S. Code § 1030.

[112]https://www.fas.org/sgp/crs/misc/97-1025.pdf.

"unauthorised access" and "damages", which lead to confusion in the courts and abuse by prosecutors.[113]

An example of this ambiguity of the term "unauthorised access" is given in the case of ***United States v Lowson,***[114] in which it was alleged that the defendants gained "unauthorised" access to the Ticketmaster site to purchase a number of tickets and resell them at a profit. The different kind of actions set out in the indictment were not clearly falling into the term "unauthorised access" and raised complicated questions such as whether the level of sophistication of a software could affect "unauthorised access" and whether employing a hundred people to buy tickets in the usual method without using software could count as unauthorised access.

Problems also arise when a fraudster employs new methods that have not been foreseen by the legislature when drafting a new law. A solution can be the enactment of legislation with a general scope and application that uses open terms, leaving the specific definition of electronic crimes and the methods that can be employed in the commission of the said crimes, to the discretion of the courts to include all new behavior that might arise in the future. Indeed, this approach will be heavily criticised, as the interpretation of the courts can vary and the offenders might argue that they had no previous knowledge that a specific behaviour was illegal and prohibited.

The protection of anonymity and the protection of the identity of internet and IP users is also an issue in investigating and uncovering cases of electronic fraud. In most cases, the need to connect a user with an IP address and to acquire other personal information stored using the internet or the technology might be an issue. For instance, in Cyprus, article 17 of the Constitution protects the secrecy of correspondence and other communications and used to be a complete barrier to criminal investigations of offences committed using a computer and/or the internet. Therefore, the Cypriot legislature was forced to amend the Constitution in 2010 to enable interference with the right, in specified situations and most notably, in the detection and prosecution of serious crimes and crimes carrying out a sentence of 5 years imprisonment or more and when such an interference relates to the traffic data and location data and relevant data required to identify the subscriber or the user. A necessary requirement for such interference with the right is the issue of a Court Order, therefore the court acts as an additional safeguard to protect the rights

[113] Supra n. 111.

[114] 2010 WL 9552416 (D.NJ.2010), as referred to in Simmons R., The Failure of the Computer Fraud and Abuse Act: Time to Take a New Approach to Regulating Computer Crime, George Washington Law Review No. 329, 2 February 2016.

of citizens and check whether the request by the authorities is justified and proportionate.[115]

5 Conclusion

The danger today remains the existence of possibilities for computer criminals to relocate to countries that do not regulate sufficiently this type of conduct, therefore the thorn on an effort to regulate electronic fraud and other computer-related economic crimes is the lack of universal application of rules against this type of crimes. An example of this lack of coordination that left a computer fraudster on the loose was the perpetrator of the 'I love you' virus that infected millions of computers around the world in May 2000 and although he was tracked in the Philippines, he remained unpunished because there were no legislative provisions in place criminalising his behavior in the Philippines.

The idea remains that criminal law can be used in the online environment to maintain order and to compel individuals to share common acceptable norms and values. However, it is evident that steps taken by different Member States and the EU to this direction are still embryonic and have not been efficient. A more coherent plan needs to be designed so that the next steps will be more structured in order to address increasing concerns over the security of using the internet both commercially and socially. Criminals have found new ways to act and fraud has taken new dimensions and it is predicted that the concept will evolve even further in the next few years. We will be witnesses of new types of electronic economic crime and we should not only hope for the best, but also take measures and ensure that strategies and 'weapons' are in place to annihilate the danger.

[115] A recent preliminary ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber) of 21 December 2016 concerned the retention of data and distinguished the cases where such retention is legal and the cases where it breaches rights. "Article15(1) of Directive 2002/58, read in the light of Articles7, 8 and 11 and Article52(1) of the Charter, must be interpreted as precluding national legislation which, for fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication" (paragraph 112) and concluded that Article 15 and the EUCFR "must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union." (paragraph 125).

References

Anti-Phishing Working Group (2014) Phishing activity trends report 1st quarter 2014. http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf. Accessed 11 Jan 2017

Borzykowski B (2016) "The chilling truth about cybercriminals – from a paid hacker", at http://www.cnbc.com/2016/07/26/microsoft-google-hacker-reveals-truths-about-data-thieves.html

Clough J (2010) 'Now you see it, Now you dont' digital images and the meaning of possession. Crim Law Forum 19:205

Clough J (2015) Computer related fraud. In: Rider B (ed) Research handbook on international financial crime. Elgar, Chapter 30

Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a general policy on the fight against cyber crime (COM(2007) 267 finalof 22.5.2007), Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14560. Accessed 11 Jan 2017

Constantin L (2016) Rent-a-botnet services making massive DDoS attacks more common than ever before. Available at http://www.pcworld.com/article/3079990/security/massive-ddos-attacks-reach-record-levels-as-botnets-make-them-cheaper-to-launch.html. Accessed 11 Jan 2017

Cybercrime Unit of the Greek Police (2016a) Press release, solved case of extortion and violation of personal data legislation against a 21-year old person, Athens, 21 September 2016, available in Greek. http://www.astynomia.gr/index.php?option=ozo_content&lang&perform=view&id=65601&Itemid=1757

Cybercrime Unit of the Greek Police (2016b) Press release, solved case of systematic electronic frauds by a 40-year-old member of a criminal organisation, Athens, 9 July 2016, available in Greek. http://www.astynomia.gr/index.php?option=ozo_content&lang&perform=view&id=63854&Itemid=1725

Doyle C (2014) Cybercrime: an overview of the federal computer fraud and abuse statute and related federal criminal laws. https://www.fas.org/sgp/crs/misc/97-1025.pdf

European Commission (2013) Cybersecurity strategy of the European Union: an open, safe and secure cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7 February 2013, JOIN(2013) 1 final. https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission (2016a) Press release, commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats Brussels, 5 July 2016. http://europa.eu/rapid/press-release_IP-16-2321_en.htm

European Commission (2016b) Fact sheet, directive on security of network and information systems, Brussels, 6 July 2016. http://europa.eu/rapid/press-release_MEMO-16-2422_en.pdf

Evans M (2015) Hackers steal £650 million in world's biggest bank raid. http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html. Accessed 11 Jan 2017

FBI Press Release (2016) FBI warns of online dating scams, 11 February 2016. https://www.fbi.gov/contact-us/fieldoffices/sandiego/news/press-releases/fbi-warns-of-online-dating-scams. Accessed 5 Aug 2017

Gercke M (2009) Europe's legal approaches to cybercrime. ERA Forum 10:409

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

http://fraud.laws.com/fraud-news/scam-targeting-women-on-dating-websites-35975.html

Iglezakis I (ed) (2016) The legal regulation of cyber attacks. Wolters Kluwer

Internet Crime Compaint Centre (2015) Internet crime report. https://pdf.ic3.gov/2015_IC3Report.pdf. Accessed 11 Jan 2017

Jougleux P (2012) Identity theft and internet. Int J Liabil Sci Enq 5(1):37–45

McNally M, Newman G (2008) Perspectives on identity theft. Crime prevention studies, Vol 23. Willan Publishing, Cullompton, Devon UK

Microsoft Malware Protection Centre Ransomware. https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx. Accessed 5 Aug 2017

National Fraud Intelligence Bureau, Identity Fraud and Identity Theft. http://www.actionfraud.police.uk/fraud_protection/identity_fraud. Accessed 5 Aug 2017

O'Gorman G, McDonald G (2012) Ransomware: a growing menace. Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf. Accessed 5 Aug 2017

Results of the Second Meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Crime Misuse and Falsification of Identity' (E/CN.15/2007/8) (2007) Available via https://pdf.ic3.gov/2015_IC3Report.pdf. Accessed 11 Jan 2017

Roberson C (2008) Identity theft investigations. Kaplan Publishing, p 3

Robinson N, Graux H, Parrilli M et al (2011) Comparative study on legislative and non legislative measures to combat identity theft and identity related crime: final report TR-982-EC. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf. Accessed 11 Jan 2017

Russell S (2014) In: Reichel P, Albanese J (eds) Handbook of transnational crime and justice, 2nd edn. Sage Publishing, Oaks, Ch. 7

Savirimuthu J (2008) Identity theft and the gullible computer user: what Sun Tzu in the art of war might teach. J Int Commer Law Technol. Available at http://www.jiclt.com/index.php/jiclt/article/viewArticle/49

Scamwatch (2016) $22.7 million lost to dating scams in 2015, 12 February 2016. http://www.scamwatch.gov.au/news/227-million-lost-to-dating-scams-in-2015

Simmons R (2016) The Failure of the Computer Fraud and Abuse Act: Time to Take a New Approach to Regulating Computer Crime, George Wahington Law Review No. 329, 2 February 2016, also citing Sun Beale S (2005) The many faces of overcriminalization: from morals and mattress tags to overfederalization. Am Univ Law Rev 54:747, Struntz W (2001) The pathological politics of criminal law. Mich Law Rev 100:505

Smith R (2014) Transnaional cybercrime and Fraud. In: Reichel P, Albanese J (eds) Handbook of transnational crime and justice, 2nd edn. Sage, ch. 7

Smith RG (2010) Identity theft and fraud. In: Jawkes Y, Yar M (eds) Handbook of internet crime, 1st edn. Willan Publishing, pp 273–301

Sproule S, Archer N (2006) Defining Identity Theft – A Discussion. Paper Prepared for the Ontario Research Network in Electronic Commerce (ORNEC) Identity Theft Research Program, pp 1–37

Squarcialupi V, Report in the Committee of Economic Affairs and Development at the Parliamentary Assembly (2001) "Europe's fight against economic and transnational organised crime: progress or retreat?" Available at http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewHTML.asp?FileID=9242&lang=en. Accessed 11 Jan 2017

Study for the Centre for Identity Management and Information Protection (CIMIP) (2007). http://www.utica.edu/academic/institutes/cimip

Summers S, Schwarzenegger C, Ege G et al (2014) The emergence of EU criminal Law. Hart

The Crown Prosection Service Press Office (2016) Pair sentences for decade-long insider fraud scheme, 19 August 2016. http://www.cps.gov.uk/news/latest_news/pair_sentenced_for_decade_long_insider_fraud_scheme/

The United States Department of Justice (2017) Identity theft. https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Vieraitis L et al (2014) Identity theft. In: Bruinsma G et al (eds) Encyclopedia of criminology and criminal justice. Springer, pp 2419–2429

Weber MA (2003) The Council of Europe's Convention on Cybercrime. Berkeley Technol Law J 425. Available at http://scholarship.law.berkeley.edu/btlj/vol18/iss1/28

Wright R (2006) Why (some) fraud prosecutions fail. J Financ Crime 13(2):177–182

Zetter K (2016). That Insane, $81M Bangladesh Bank Heist? Here's What We Know. https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/