

# 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 new 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 inquires 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 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 Jougoux 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’.

EU Internet Law

Regulation and Enforcement

Synodinou, T.; Jougleux, P.; Markou, C.; Prastitou-Merdi,  
T. (Eds.)

2017, XX, 433 p., Hardcover

ISBN: 978-3-319-64954-2