ADRIENN LUKÁCS *

Recent Challenges of Data Protection Law in the European Union, with Special Regard to the Internet

I. Introduction

The topicality of the subject is given by the increasing role of data protection in modern societies today. The reason behind this phenomenon is that due to the development of science and technology, the possibility to intrude into someone's privacy has increased. The pace of this development is so fast that *Orwell's* vision of the Big Brother has already become technologically possible.[1] According to *Scott McNealy*, former CEO of Sun Microsystems: "[y]ou have zero privacy. Get over it."[2] The importance of data protection is increasing, as nowadays these technological developments have made the possible intrusion into one's privacy more severe and easier. With the Internet gaining more and more space in our lives, it is easy to see that crucial privacy challenges appeared.

My aim is to present in this study the most important questions of data protection with special regard to the Internet. In the first part of my study I will briefly present the history of data protection and the new challenges shaping the form of protection, especially the Internet. Then I will present the most important legal norms of the European Union which cover data protection law and the Internet. In the third part of my study I will examine the new technologies and challenges posing problems while using the Internet and the legal responses given to them, with special regard to the upcoming data protection regulation. In the final part of my study I will draw attention to the deficiencies of the legal regulation and recommend some complementary solutions in order to ensure the effective privacy protection on the Internet.

* PhD student, University of Szeged

[1] STANLEY, JAY – STEINHARDT, BARRY: *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society.* American Civil Liberties Union, January 2003. https://www.aclu.org/sites/default/files/field_document/aclu_report_bigger_monster_weaker_chains.pdf p. 1. (Accessed: 15 September 2015)

[2] SMITH-BUTLER, LISA: *Workplace Privacy: We'll Be Watching You.* Ohio Northern University Law Review 2009/35. p. 55.

II. History

The right to data protection aims to ensure the protection of the individual's privacy.[3] At present there exists no exhaustive definition of privacy. Despite the fact that (the right to) privacy appeared in every country,[4] its concrete form differs according to the given society and culture.[5] It means that privacy must be reinterpreted in the light of the current era and be examined in the actual context. There are numerous legal scholars who made an attempt to define privacy: *Samuel Warren* and *Louis Brandeis* defined privacy as "the right to be let alone".[6] *Richard Posner* states that "one aspect of privacy is the withholding or concealment of information."[7] *Alan Westin* defined privacy as "the claim of an individual to determine what information about himself or herself should be known to others"[8] while *Charles Fried* stated that "privacy [...] is the control we have over information about ourselves."[9] *Máté Dániel Szabó* argued that "privacy is the right of the individual to decide about himself/herself."[10] In spite of these changing concepts of privacy, legal regulations defined an obligatory minimum level of protection, which protects the private sphere of the individual.[11]

In the 1960s there was a fundamental technological change that has reformed the paradigm of privacy protection: the computers appeared. This technological change also needed an equivalent legal change in order to ensure the protection of privacy, and this need gave birth to the right to data protection. Although a lot of attention has been paid to data protection, to date, there is still no agreement on the relation between the right to data protection and the right to privacy.[12] It is not this present study's aim to distinguish these two rights in detail. The right to data protection is a named and recognized right in the European Union,[13] formally separated from the right to privacy.[14] The significance of data

[3] 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, 23.11.1995, pp. 31–50. Recital 10 and Article 1. 1

[4] SOLOVE, DANIEL J.: *Nothing to hide: the false tradeoff between privacy and security*. Yale University Press, New Haven & London, 2011. p. 4.

[5] FRIED, CHARLES: *Privacy*. The Yale Law Journal Vol. 77. No. 3. (1968). p. 486.

[6] WARREN, SAMUEL D. – BRANDEIS LOUIS D.: *The right to privacy*. Harvard Law Review Vol. 4. No. 5. (1890). p. 193. They were the first to recognize the threats to privacy caused by the technological development (instantaneous photographs) and societal developments (gossip, which became a trade in newspapers). WARREN – BRANDEIS 1890. pp. 195–196.

[7] POSNER, RICHARD A.: *The right of privacy*. Georgia Law Review Vol. 12. No. 3. (1978). p. 393.

[8] WESTIN, ALAN. F.: *Social and political dimensions of privacy*. Journal of Social Issues Vol. 59. No. 2. (2003). p. 431.

[9] FRIED 1968, p. 482.

[10] SZABÓ MÁTÉ DÁNIEL: *Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival*. Információs Társadalom 2005-2. p. 46.

[11] E.g.: Article 12 of the Universal Declaration of Human Rights; Article 17 of the International Covenant on Civil and Political Rights; Article 8 of the European Convention of Human Rights and Article 7 of the Charter of Fundamental Rights of the European Union

[12] PURTOVA, NADEZHDA: *Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights*. Netherlands Quarterly of Human Rights, Vol. 28, No. 2. (2010) Available at: http://ssrn.com/abstract=1555875 p. 3. (Accessed: 23 February 2016)

[13] Article 8 of the Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407

[14] GELLERT, RAPHAËL – GUTWIRTH, SERGE: *The legal construction of privacy and data protection*. Computer Law and Security Review Vol. 29. Iss. 5. (2013). pp. 522–523.

protection is high. Data protection does not only consist of a set of rights concerning the processing of personal data, it is also the result of the process of protecting individual freedoms in the information society.[15] While the right to privacy is a "redress" right, which ensures the protection from interference by public powers, the right to data protection is a "control" right, which aims to give the right to control the processing of personal data relating to the individual.[16] In the famous population census judgement the German Federal Constitutional Court interpreted the right to data protection as the right to informational self-determination. The court stated that this right enables the individual to decide about the disclosure and use of his/her personal data, and this self-determination needs an increased level of protection in the era of technological developments.[17] It stated that if an individual is uncertain about the registered data, his/her behaviour will be governed by an external force; instead of following his/her own motivations, he/she will aim to conduct himself/herself in such a way that he/she will not stand out from the others.[18]

Nowadays we live in the era of the information society, which extremely influences our everyday lives. According to *Máté Dániel Szabó*, this phenomenon has several impacts on privacy, too. On the one hand, the private sphere of the individual becomes more open, as the new developments make more intrusions into it, more and more aspects of private life can be reached or touched through technologies.[19] On the other hand, the individual becomes more closed in the offline world as people tend to withdraw, their relationships become less personal, as more areas of life are conducted online. Due to the technological development and the new possibilities brought by it, it is even possible to have a complete life online. As a consequence, in the society the individual is determined not by himself/herself, but by the information obtained about him/her. The individual becomes virtual, as he/she does not exist in his/her real physical integrity to a lot of his/her relations, but he/she is identified as a group of data, from which the recipient identifies the individual. In spite of this virtualization the individual still stays a real being, however, the outside world might find it difficult to accept that this online person (or set of data) they interact with is a real individual in the offline world.[20]

It is clear that the Internet has completely transformed the way how we live and work today and these changes bring new challenges for data protection.[21] More and more activities of our everyday lives are conducted online, and whenever we visit a page on the Internet, we leave digital traces, from which a complete profile could be drawn up.[22] Internet has a central role in our lives: we work there, study there, handle our bank account, communicate with others either in e-mail or on social networking sites, or just

---

[15] COSTA, LUIZ – POULLET, YVES: *Privacy and the regulation of 2012*. Computer Law and Security Review Vol. 28. Iss. (2012). p. 262.

[16] KNIGHT, ALISON – SAXBY, STEVE: *Global challenges of identity protection in a networked world.* Computer Law and Security Review Vol. 30. Iss. 6. (2014). p. 625–626.

[17] JÓRI ANDRÁS: *Adatvédelmi kézikönyv*. Osiris Kiadó, Budapest, 2005. pp. 25–26.

[18] HALMAI GÁBOR –TÓTH GÁBOR ATTILA: *Emberi jogok.* Osiris Kiadó, Budapest, 2008. p. 584.

[19] It is enough to think of smartphones, smartwatches, laptops, tablets, etc.

[20] SZABÓ 2005, p. 47.

[21] Working Party on the Protection of Individuals with regard to the Processing of Personal Data: *Recommendation 3/97: Anonymity on the Internet.* 3 December 1997. (XV D /5022/97 final WP 6.) p. 3. (hereinafter this Working Party is referred to as WP)

[22] WP: *Anonymity on the Internet.* 1997. p. 4.

surf it in our free time. Time and space are not an obstacle any more to publishing information or to engaging in a real time conversation with anyone in the world.[23] During all of these activities enormous amounts of data are collected, however, many users are not aware of this phenomenon.[24] So it is crucial to ensure that the fundamental rights of the users (the right to privacy and the right to data protection) are respected on the Internet, too.[25]

III. Legal regulation of the right to data protection

The right to data protection has a detailed regulation at the level of the European Union. Data protection and the Internet are covered by two main legal norms of the European Union: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as: the Directive) and 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 (hereinafter referred to as: the ePrivacy Directive).[26] The General Data Protection Regulation will completely transform the existing legal environment, which I will detail later in my paper. This paper is not destined to exhaustively present these regulations, I will highlight the most important dispositions and the dispositions that have relevance to the Internet only briefly.

1. Data Protection Directive

From among the European Union's data protection instruments, the most significant one is the *Directive*, which defines basic requirements that the Member States have to transpose into their national legal systems. The *object* of the Directive is to find a balance between the natural person's right to privacy and to data protection and the free flow of personal data. (Article 1) Among the most important definitions we have to mention the definition of *personal data*. Personal data mean any information relating to an identified or identifiable natural person (data subject). An *identifiable person* is a person "[...] who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural

[23] International Working Group on Data Protection in Telecommunications: *Report and Guidance on Privacy in Social Network Services – "Rome Memorandum"*. 3-4 March 2008. (675.36.5.) p. 1.

[24] Article 29 Data Protection Working Party: *Working Document: Privacy on the Internet - An integrated EU Approach to On-line Data Protection.* 21 November 2000. (5063/00/EN/FINAL WP 37.) p. 19.

[25] The United Nations adopted in 2012 a resolution in which they stated that "[...] the same rights that people have offline must be also protected online[.]" See: United Nations General Assembly: *The promotion, protection and enjoyment of human rights on the Internet.* 2012. (A/HRC/20/L.13)

[26] 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, 31.7.2002, pp. 37–47.

or social identity[.]" [Article 2 (a)] At first glance it might not be obvious, but the IP address is also considered to be personal data.[27]

The Directive applies "[...] to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system." (Article 3. 1) It means that the Directive applies to any data processing regardless of the technology used, so it applies to the Internet too. That means that the processing of personal data on the Internet has to respect the same data protection rules as the offline world.[28] The Directive shall not apply in two cases: when the activity falls outside the scope of Community law and when the processing of personal data is performed by a natural person in the course of a purely personal or household activity. (Article 3. 2) The application of the latter disposition can be dubious when we consider the use of social networks. In most cases social networks are used for purely personal purposes, however, the application of the exemption to their case might be against the original purpose of the legislator.[29] There are different opinions on that question: the Court of Justice of the European Union stated in the Lindquist case that the exemption cannot apply to cases where the data is made available for an indefinite number of users on the Internet,[30] while the Article 29 Data Protection Working Party states in its opinion that the exception might *not* apply in *some* cases to social network users.[31]

The Directive defines when the processing of personal data is lawful. Data processing is lawful when (1) the data subject has unambiguously given his consent; or (2) the processing is necessary for the performance of a contract to which the data subject is party; or (3) for compliance with a legal obligation to which the controller is subject; or (4) to protect the vital interests of the data subject; or (5) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or (6) for the purposes of the legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection. (Article 7) Interpretation problems might arise among different Member States when we discuss the interpretation of *consent*.[32] According to the Directive, consent is a freely given, specific and informed decision to agree to the processing of personal data. [Article 2 (h)] However, meeting these requirements might be problematic, as privacy policies on the Internet are usually too extensive and have a wording not easily understandable by the

[27] WP: *Privacy on the Internet*, 2000. p. 21.; C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] ECR I-11959 par. 51.

[28] Working Party on the Protection of Individuals with regard to the Processing of Personal Data: *Working Document: Processing of Personal Data on the Internet.* 23 February 1999. (5013/99/EN/final WP 16.) p. 3.

[29] VAN EECKE, PATRICK – TRUYENS, MARTIN: *Privacy and social networks*. Computer Law and Security Review Vol. 26. Iss. 5. (2010). p. 539.

[30] C-101/01 Bodil Lindqvist [2003] ECR I-12971 par. 46-48.

[31] Article 29 Data Protection Working Party: *Opinion 5/2009 on online social networking.* 12 June 2009. (01189/09/EN WP 163.) pp. 5-7.

[32] See more: Article 29 Data Protection Working Party: *Opinion 15/2011 on the definition of consent.* 13 July 2011. (01197/11/EN WP187)

user.[33] More severe rules apply to *special categories of data,* also called sensitive data. This category contains personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life. (Article 8. 1) In the age of the widespread use of social networks, blogs, newsrooms and other forums with the possibility to self-expression online, the publication of sensitive information can be considered as a growing issue.

There are several principles related to *data quality* that shall be respected during the processing. Personal data must be processed *fairly* and *lawfully*; must be collected for *specified, explicit* and *legitimate purposes* and *not further processed* in a way incompatible with those purposes. Personal data must be *adequate, relevant* and *not excessive* in relation to the purposes for which they are collected and/or further processed; *accurate* and, where necessary, *kept up to date.* (Article 6) It is not a data quality principle but the controller must also ensure the security of processing. (Article 17)

The data subject can exercise *rights*, namely he/she has the right to obtain information, the right to access data (to know whether data relating to him/her are being processed, what data; the right to erase or block the data and the right to notification) and the right to object to the processing of personal data. (Article 10, 12, 14) The right to erasure is a very topical question nowadays, as it is impossible to delete something that was once published on the Internet. If the data subject's rights are breached, he/she can exercise the right to *judicial remedy.* (Article 22)

The *transfer of personal data to third countries* is only possible when the third country where the data is transferred ensures an adequate level of protection. (Article 25. 1) This requirement is extremely important when it comes to the Internet as in the online world national borders do not exist.[34] The Directive has to be transposed into national legislation, and each Member State shall provide a public authority that would be responsible for monitoring the application of the Directive in the given Member State. (Article 28) The Directive also created the Article 29 Working Party (Article 29), which adopted several important documents in certain special fields of data protection, also in the field of data protection and the Internet.[35]

2. Privacy Directive

Although the general data protection rules have to be respected, the Internet requires specific rules and safeguards concerning data protection which particularizes and complements the Data Protection Directive. (Article 1. 2) In order to ensure this

[33] DE HERT, PAUL – PAPAKONSTANTINOU, VAGELIS: *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals.* Computer Law and Security Review Vol. 28. Iss. 2. (2012). p. 136.

[34] It is enough to think of the NSA's mass surveillance scandal leaked by Edward Snowden in 2013. See: The Guardian: *NSA spying scandal: what we have learned* 10 June 2013. http://www.theguardian.com/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned (Accessed: 23 February 2016); PINTÉR RÓBERT: *Yes, we (s)can!* Információs Társadalom 2013/3-4. pp. 28–42.

[35] See for example: WP: *Processing of Personal Data on the Internet.* 1999; WP: *Anonymity on the Internet.* 1997; WP: *Privacy on the Internet.* 2000.

protection, the European Union adopted the ePrivacy Directive. The ePrivacy Directive regulates the question how providers of electronic communication services (e.g. telecoms companies and Internet service providers) should process the service users' data. The ePrivacy Directive also regulates the main rights of the users.[36]

The ePrivacy Directive applies "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices." (Article 3)

According to the main requirements of the ePrivacy Directive, the service provider shall ensure the *security* of networks and services. It means that the service provider has to (1) ensure that personal data are accessed only by authorized persons, (2) protect the data from being destroyed, lost, processed without authorization, etc., and (3) ensure the implementation of a security policy. (Article 4. 1-1a) The ePrivacy Directive regulates in detail the notification of data breach, defining in which cases the service provider must inform the national authority and / or the users. (Article 4. 3) Member States must respect the *confidentiality of the communications* on public communication networks. The listening, tapping, storage and any type of surveillance or interception of communication or traffic data must be prohibited without the consent of the user and unless certain specific requirements are met. (Article 5) *Traffic and location data* must be erased or made anonymous when they are no longer required for communication or billing purposes, except if the user has given consent for another use. (Article 6. 1, 6. 3) The user has to give his/her prior consent (1) in order to send him/her unsolicited communications (SPAM), which applies to SMS and other electronic messaging systems, (2) so that information (cookies) can be stored on their devices, and (3) to make their telephone numbers, e-mail or postal addresses appear in public directories.[37]

IV. Privacy challenges in the era of the information society

I will address two main categories of privacy related problems in the information society. The first category is a general one; it is connected to the users of the Internet, their comportment/behaviour on the Internet and the new trends and services that affect privacy. So these are risks which result either from the user conducts or from the mere characteristics of the different services. The second category is composed of the legal problems, which can be considered as data protection problems related to the appearance of Internet, especially the challenges of the application and interpretation of the already existing regulation in the case of this new phenomenon.

---

[36] European Commission: *The ePrivacy Directive.* 12 July 2002. https://ec.europa.eu/digital-agenda/en/news/eprivacy-directive (Accessed: 5 December 2015)

[37] Eur-lex: *Data protection in the electronic communications sector.* 27 May 2014. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24120 (Accessed: 5 December 2015)

1. New developments challenging privacy protection on the Internet

In spite of the fact that the Directive was a great step ahead in protecting privacy, since its creation the rapid pace of technological development and globalisation has raised new challenges for the protection of personal data, which even raise the question whether the Directive is still capable of facing these challenges effectively.[38] I have already presented how the Internet has changed our lives in general, and that it records every move we make in the online world. Now I will discuss some concrete examples of privacy threats within the Internet. The use of *search engines* raises serious privacy issues. On the one hand, the privacy of the search object can be injured,[39] as search engines contribute to making information easily accessible to users from the whole world, which may pose certain risks to the privacy of the individual.[40] On the other hand, the privacy of the user who does the search can be infringed.[41] During browsing on the Internet (or monitoring the activities of users on different websites) every aspect of the behaviour of the user is recorded, potentially the complete history of the Internet usage could be known.[42] Different actors (e.g. businesses or the state) are interested in obtaining that information and analysing it for different purposes.[43] These bits of information present on the Internet can be composed and be used to create profiles from which predictions for the future are made. Profiling represents a serious privacy threat as different decisions can be made from the obtained information without the knowledge or the participation of the data subject.[44]

A very serious threat to privacy is posed by *social network services*. Social networks are relatively new phenomena, and are extremely popular. On social networking sites, people share (on their own initiative) personal data and information concerning their lives that are traditionally considered to be private, in a way and quantity never experienced before.[45] The problem occurring with this phenomenon is that the concept of community has changed: the online community is much bigger than the offline community. So it is crucial for users to know how to use the privacy settings and to be properly informed about the sharing/the privacy settings of their profile information.[46] So raising their

[38] European Commission: *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.* Brussels, 4 November 2010. COM(2010) 609 final. pp. 1-2.

[39] TENE, OMAR: *Privacy: The new generations.* International Data Privacy Law Vol. 1. No. 1 (2011). pp. 21-22.

[40] Article 29 Data Protection Working Party: *Opinion 1/2008 on data protection issues related to search engines.* 4 April 2008. (00737/EN WP 148) p. 5.

[41] TENE 2011, p. 22.

[42] International Working Group on Data Protection in Telecommunications: *Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential.* 15-16 April 2013. (675.46.13) par. 6

[43] KNIGHT – SAXBY 2014, p. 620., pp. 623–624.

[44] KNIGHT – SAXBY 2014, pp. 621-622.

[45] *Rome Memorandum* 2008. p. 1. This phenomenon raises the question whether a "new" data protection has appeared. The first generation of data protection laws were created in order to protect citizens from the excessive power of the state and its institutions ("the big brother") or big companies ("little brothers"), but in the case of social networks most of the privacy risks are caused by the user himself/herself. So while the "traditional" data protection regulation was about defending citizens against the public administration and businesses, the "new" data protection regulation should focus on the publication of personal data on the initiative of private individuals. (*Rome Memorandum* 2008. p. 1.)

[46] *Rome Memorandum* 2008. p. 2.

awareness would be crucial, it could mean an important leap in the (self)-protection of personal data on the Internet. As concerns the information shared on social networks: usually users share data on their profile, but they also have the possibility to post instantly and at any time their own content: photos, videos, personal entries, location data, etc. This leads to numerous users sharing the most intimate moments of their lives.[47] There are serious risks that occur from the wide share of personal information without control: the possible misuse of personal data and identity theft,[48] misinterpretation of information or even the share of personal data without the knowledge of the data subject.[49]

The access to Internet from mobile devices (e.g. smartphones, laptops) is also a growing phenomenon worldwide, especially when we consider the gathering of location data.[50] While the privacy risks of the Internet are commonly known to society at a basic level, people tend to forget about the same risks posed by *smartphones*.[51] However, smartphones are usually linked to one person, while computers can be used by several people, so there is a stronger connection between the user and the device. From mobile devices important geo-location data can also be made accessible.[52] The use of *cloud computing* might have its risks too, as it basically means computers without borders. Cloud computing can be considered as "the ultimate form of globalisation"[53], which can pose risks concerning the applicable regulation to the processing of personal data as services can be found in a variety of places, which can even lead to the application of a different (less severe) regulation.[54]

2. Legal challenges and the solutions

As the Directive was adopted more than 20 years ago, in a technologically completely different era, the technological and legal changes (data protection has become a fundamental right in the EU) lead to the fact that the different Member State legislations did not provide the desired level of harmonization.[55] In 2012 the Commission proposed a new data protection reform in the form of the General Data Protection Regulation (hereinafter referred to as GDPR)[56] in order to modernize data protection rules. The final

---

[47] QI, MAN – EDGAR-NEVILL, DENIS: *Social networking searching and privacy issues.* Information Security Technical Report Vol. 16. Iss. 2. (2011). p. 75.

[48] On the importance of the digital identity and its threats see: KNIGHT – SAXBY 2014

[49] SMITH, WILLIAM P. – KIDDER, DEBORAH L.: *You've been tagged! (Then again, maybe not): Employers and Facebook.* Business Horizons Vol. 53. Iss. 5. (2010). p. 495., p. 496.

[50] See: TENE 2011, p. 18.

[51] WEBER, ROLF H.: *The digital future – A challenge for privacy?* Computer Law and Security Review Vol. 31. Iss. 2. (2015). p. 239.

[52] International Working Group on Data Protection in Telecommunications: *Web Tracking and Privacy.* 2013. par. 18

[53] The Economist: *Let it rise. A special report on corporate IT.* 25 October 2008. http://www.swpartners.com/wp-content/uploads/EconomistITSurvey20081025.pdf p. 13. (Accessed: 23 February 2016)

[54] The Economist 2008, pp. 13–14.

[55] DE HERT – PAPAKONSTANTINOU 2012, p. 131.

[56] *Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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).* 2012/0011 (COD) Brussels, 6 April 2016, 5419/16.

text of the GDPR was adopted by the European Parliament on 14 April 2016 and will be applicable from 2018.[57] The GDPR addresses a part of the new challenges of the digital world that I will present in the next part of my study, either by regulating them or clearing the interpretation of the already existing dispositions. The GDPR constitutes a big step ahead in privacy protection in the EU as it creates a uniform data protection legislation within the EU, still, some problems remain unsolved, so further solutions are needed.

2. 1. General Data Protection Regulation

As a response to the technological development, the GDPR gives clear guidance on what can be considered *personal data*. Although the definition itself has not changed ["'personal data' means any information relating to an identified or identifiable natural person ('data subject')" and 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"],[58] it is a significant change that the recital gives clear guidance (Recital 30) that IP addresses can identify the individual.[59] The importance of this disposition is that it pointed out that with the development of certain technologies (IP addresses) it is possible to make profiling, and to be able to identify the person even without knowing his/her nominative identity.[60]

The GDPR keeps *consent* as one of the legal bases of data processing and gives further guidance and conditions on the requirements of the consent. It is the controller's responsibility to prove that the data subject has given his/her consent. (Recital 42) In order to ensure the freely given nature of the consent, it should not be the legal basis for processing when there is a significant imbalance between the parties. (Recital 43) The GDPR also makes it clear that pre-ticked boxes on different websites are not accepted as consent. (Recital 32) The request for consent must be presented in an understandable form for the data subject, using clear and simple expressions. (Article 7. 2) It is also stated that the consent can be withdrawn any time. (Article 7. 3)

As people have very limited control over their personal data, the GDPR aims to strengthen to data subject's rights, by clarifying the right to be forgotten and introducing the right to data portability.[61] The *right to be forgotten* is not completely new as it existed already in the Directive.[62] It means "the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes."[63] This

[57] European Commission - Statement: *Joint Statement of the final adoption of the new EU rules for personal data protection*. Brussels, 14 April 2016. Source: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm (Accessed: 23 April 2016) The study was finished on 23 April 2016 when the GDPR was not yet published in the Official Journal of the European Union.

[58] General Data Protection Regulation Article 4 (1)

[59] DE HERT – PAPAKONSTANTINOU 2012, p. 133.

[60] COSTA – POULLET 2012, p. 255.

[61] COSTA – POULLET 2012, p. 256.

[62] See more on this subject: BUNN, ANNA: *The curious case of the right to be forgotten*. Computer Law and Security Review Vol. 31. Iss. 3. (2015). pp. 336–350.

[63] European Commission: *Communication from the Commission*. 2010. p. 8.

right has two aspects.[64] The first one is the "traditional" right to erasure, which means that "[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay [...]" if other conditions are met. (Article 17. 1) It is completed by a second disposition in order to strengthen the data subjects' rights in the online world: with the obligation of the data controller to take all the reasonable steps to inform other controllers processing that data that the data subject wants these controllers to erase the data, any links to it, any copies or replication if the controller has made data – subject to the right to erasure – public. (Recital 66, Article 17. 2) The reason for the acceptance of the right to be forgotten is while the human mind has its limits in remembering, the Internet does not have any limits.[65] However, the concrete way of the implementation of this right is still a question, as right now the Internet is not capable of forgetting, as it is not possible to permanently remove content.[66] This right is still a big step in protecting personal data, however, it might be more accurate to interpret it as the right to not to be found, as the complete erasure from the Internet is technically not possible.[67] The importance of this right is significant, as it gives people the possibility to escape from their past. Everyone can imagine a moment in their online life that they might like to erase in the future.[68] *Luiz Costa* and *Yves Poullet* interpreted this right as the avoidance of a special type of Miranda warning: not to live in the constant threat that everything I do can be used against me in the future.[69] Of course, the right to be forgotten is not an absolute right; there exist some interests that justify that the right to be forgotten does not prevail in some cases: e.g. freedom of expression, or historical, scientific research. (Article 17. 3)

The other Internet specific right is *the right to data portability*, which has two parts: the first part is the right to obtain a copy of the personal data processed by the controller in a structured way, and the second one is the right to transmit this personal data to another service provider.[70] An example is the possibility to change a social network service by taking all the information submitted and then to choose another social network provider.[71] So basically this right enables the interoperability between different service providers. (Recital 68)

The GDPR introduces new ways beyond the traditional legal protection, by regulating the technology itself, by making it more privacy friendly. Three principles make this possible: data protection by design, data protection by default and data protection impact assessment.[72] *Data protection by design* means that already when planning the data

[64] European Digital Rights: *Key aspects of the proposed General Data Protection Regulation explained.* https://edri.org/files/GDPR-key-issues-explained.pdf p. 6. (Accessed: 5 December 2015)

[65] KINDT, ELS: *Privacy and Data Protection Law: An Introduction.* (Conference presentation at the IC1206 Training School: De-identification for privacy protection in multimedia content 07-11 October 2015, Limassol, Cyprus, 11 October 2015)

[66] BOLTON, ROBERT LEE: *The Right to Be Forgotten: Forced Amnesia in a Technological Age.* The John Marshall Journal of Information Technology & Privacy Law Vol. 31. Iss. 2. (2014). p. 133.

[67] International Working Group on Data Protection in Telecommunications: *Working Paper and Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy.* 15-16 April 2013. (675.46.32.) pp. 1–2.

[68] BOLTON 2014, p. 40.

[69] COSTA – POULLET 2012, p. 257.

[70] COSTA – POULLET 2012, p. 257.

[71] DE HERT – PAPAKONSTANTINOU 2012, p. 138.

[72] COSTA – POULLET 2012, p. 259.

processing "[...] the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." (Article 25. 1) So it basically means – after the analogy of privacy by design – the use of built-in data protection friendly solutions into the whole designing of the processing.[73]

Data protection by default means that "[t]he controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility." (Article 25. 2) A very simple example to illustrate this principle is the case of social networks, where the privacy settings of profiles should be private by default, and those who would like to share it with the public should change the privacy settings to public and not from public to private.

Data protection impact assessment means the evaluation of the possible risks related to the protection of personal data, prior to the processing. In cases when data processing comes with higher risks for the rights of the individual, the controller should evaluate these risks in a data protection impact assessment, by taking into consideration the characteristics of the processing. (Recital 83, Article 35) The aim of the assessment is to ensure the security and confidentiality of the processing. When there is a high risk which might cause difficulties to the controller to ensure the appropriate measures, a consultation of the supervisory authority shall take place. (Recital 84) It is considered to be easier to ensure the protection of privacy and personal data if the risks endangering them are taken into account in the early stages of the planning of the processing.[74]

So it can be seen that the GDPR constitutes a huge step ahead in ensuring data protection on the Internet, as the new regulation tries to comply with the recent technological inventions. Amending the existing basic definitions and introducing new Internet specific dispositions are further steps towards the solution. However, in my opinion, there are still some legal issues, mostly in practice. It is still questionable whether the user – who is in weaker position against the service/application providers – can effectively enforce his/her rights, as in practice the transparency principle and the right to information do not always work. The GDPR introduces fines and penalties[75] which will hopefully contribute to ensuring the law-abiding conduct of data controllers in practice.

[73] DE HERT – PAPAKONSTANTINOU 2012, p. 260.

[74] European Commission: *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments.* 20 January 2010 JLS/2008/C4/011 – 30'CE'0219363/00'28 http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf par. 131. (Accessed: 5 December 2015)

[75] General Data Protection Regulation Article 83, Article 84.

2. 2. Other solutions

The GDPR brings some very important changes; however, they are not enough to ensure the effective protection of privacy in the age of rapid technological development. Besides the legal regulation, some other solutions are also needed.

The development of *technological solutions* is a key issue. The data protection by design principle contains dispositions concerning the technology by placing obligation on the controller, but in my opinion it is also crucial that not only data controllers but also technology designers take privacy into account during the invention of the technology.[76] It is also very important that legislators understand the technology before regulating it in order to be able to adopt an effective and enforceable regulation.[77] Naturally, in the age when different devices appear and evolve all the time, it is crucial to have a technology neutral regulation – like the Directive or the GDPR – in order to protect data protection issues regardless of the technology. However, for inventions which become extremely popular and pose special or different data protection risks, the role of the *lex specialis* must not be forgotten, either in the form of a directive or a soft law document.

The role of *international cooperation* is also very important as on the Internet borders do not exist, so the same processing can be subject to different privacy and data protection acts (with may represent a lower level of protection). In spite of the fact that the time might not be ready for the creation of an international data protection regulation, it is still needed to react to the global flow of personal data and to ensure the effective protection of the processing of personal data wherever it is processed.[78] One example is the Safe Harbour agreement (which was the central document for regulating the transfer of personal data between the EU and the United States for the last 10 years), which was declared invalid by the Court of Justice of the European Union in October 2015 as the United States did not provide the adequate level of protection needed.[79] Since this decision, in February 2016 they agreed on a new framework for the transfer of personal data between them, which is called the EU-US Privacy Shield.[80] When someone's data might be processed anywhere in the world, it is crucial to have efficient safeguards to ensure an adequate level of protection regardless of the geographical location of the processing.

Raising awareness is also a key issue, as users are not always aware of the privacy risks occurring during the use of the Internet and its services. So the first step would be that the users themselves recognize the threats to privacy and then they could use the technology knowing the possible risks. *David Flaherty* emphasizes the responsibility of the individual in this technologically advanced world, stating that "[y]ou have to be your own privacy commissioner. And you have to decide, in your own life, to the extent that you can do it, where you want to draw the line between openness and candour; or, to what

---

[76] For example see: WEBER 2015, pp. 239–242.

[77] KNIGHT – SAXBY 2014, p. 629.

[78] KUNER, CHRISTOPHER: *An international legal framework for data protection: Issues and prospects.* Computer Law and Security Review Vol. 25. Iss. 4. (2009). p. 308. On the possible adoption of an international regulation see more in the same article.

[79] C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] par. 106.

[80] For more information see: European Commission Press release: *Restoring trust in transatlantic data flows though strong safeguards: European Commission presents EU-U.S. Privacy Shield.* Brussels, 29 February 2016. http://europa.eu/rapid/press-release_IP-16-433_en.htm (Accessed: 23 April 2016)

extent you want to control your personal privacy. You reflect on it: all of us protect our personal privacy day in and day out by various strategies that we have developed."[81] Then, the enforcement of the transparency principle is also needed. This principle is accepted by the GDPR, too, but in my opinion in order to ensure that individuals understand what happens to their personal data it is not enough if the GDPR's transparency principle is implemented, it is also needed to actively inform people in general about the structure of the Internet and the collected data (so they should be informed already before the use of the service). Then, as a next step, users should be educated on how IT technology works, and what they could do in order to protect their own privacy and control their data on the Internet. This is especially important in the case of social networks where users choose to share personal data. With this, the self-responsibility of the individual can be enforced.

V. Conclusion

In conclusion it can be stated that we live in the era of the information society and the Internet has an increasing role in everyday life. The joint examination of the Internet and the right to the protection of personal data is an extremely important subject as data protection issues arise all the time, threatening the right to privacy and the right to the protection of personal data. At the same time we can also experience the replacing of the Directive by the GDPR, which gives a solution to certain Internet specific problems. However, the rapid technological development, the characteristics of the online world and the transforming user conducts cause that this legal change in itself might not be enough to ensure the effective privacy protection of Internet users. It is also needed to complement this legal protection with other methods in order to solve the existing and arising problems. First, in spite of the fact that some definitions in the GDPR were changed in order to comply with the online world, there are still a lot of questions to be answered. There exist remaining interpretation problems and uncertainties concerning the basic definitions, like consent, data controller or household exemption in the light of the new technologies and devices. Second, the contents posted to the Internet cannot be perfectly controlled, which leads to the fact that user conduct acquired a new significance. On the one hand, raising users' awareness is crucial, as it is the first step to take in the course of (self) privacy protection. On the other hand, the education of users is also very important as nowadays a growing number of privacy issues are self-generated, so users shall be able to "defend" themselves against these risks. Finally, the creation of a regional protection is not enough, regarding that one of the most important features of the Internet is its global nature. Some kind of international cooperation is needed in order to effectively ensure the right to privacy on the Internet.

[81] FLAHERTY, DAVID H.: *Some reflections on privacy and technology*. Manitoba Law Journal Vol. 26. No. 2. (1999). p. 233.

LUKÁCS ADRIENN

AZ ADATVÉDELMI JOG AKTUÁLIS KIHÍVÁSAI AZ EURÓPAI UNIÓBAN, KÜLÖNÖS TEKINTETTEL AZ INTERNETRE

(Összefoglaló)

Napjainkban az adatvédelem szerepe egyre inkább felértékelődik a modern társadalmakban. Ennek oka, hogy a tudomány és a technológia fejlődése következtében a magánszférába történő beavatkozás egyre könnyebben és egyre mélyebben valósítható meg. Az internet térnyerése a mindennapi életben vitathatatlan, ugyanakkor használata során számos adatvédelmi szempontból igen érzékeny problémával találkozunk. A tanulmány célja ezen kihívások és a rájuk adott lehetséges megoldások bemutatása.

A tanulmány első része röviden bemutatja a magánszférához és a személyes adatok védelméhez való jog történetét és jelentőségét, valamint az információs társadalom által okozott megváltozott viszonyokat. A második rész az adatvédelemre vonatkozó jelenleg hatályos európai uniós szabályozást mutatja be: a 95/46/EK adatvédelmi irányelv és a 2002/58/EK ePrivacy irányelv vonatkozó rendelkezéseit. A harmadik rész tartalmazza az internet és a hozzá kapcsolódó szolgáltatások által okozott speciális adatvédelmi kihívásokat, többek között az internetes keresőmotorok, a közösségi oldalak, az okostelefonok vagy a felhőszolgáltatás által generált adatvédelmi problémákat. Ezt követően, mint már létező megoldásként, ismertetésre kerülnek az Európai Adatvédelmi Rendelet internet specifikus rendelkezései. A tanulmány befejező része az egyéb megoldási javaslatokat rögzíti.

A tanulmány eredményeképp megállapítható, hogy az internet és a hozzá kapcsolódó technológiai fejlesztések igen nagymértékben veszélyeztetik a felhasználók magánszféráját. Habár az Európai Unió szintjén már létezik adatvédelmi szabályozás, kérdéses, hogy a több évtizeddel ezelőtt alkotott rendelkezések képesek-e megfelelő védelmet biztosítani napjainkban is. Részben ezen változásokra reagálva került elfogadásra az Európai Adatvédelmi Rendelet, amely jelentős előrelépést jelent-e téren, hiszen számos olyan rendelkezést tartalmaz, mely hatékony védelmet biztosít az információs társadalom korában is. Ugyanakkor további megoldások is szükségesek, többek között a nemzetközi adattovábbításokra vonatkozó szabályozás szigorítása, magának a technológiának a szabályozása vagy a felhasználók magatartásának és felelősségének a felértékelődése.