Marta KOŁODZIEJCZYK*

LIABILITY OF INTERNET USERS AND INTERNET DATA PROVIDERS IN THE CONTEXT OF THE REFORM OF THE EU DATA PROTECTION LAW

Summary
On 25 January 2012 the European Commission proposed a comprehensive reform of the EC 1995 data protection rules. The need for this reform can be explained by rising impact of IT technologies on our lives; astounding capabilities of modern technologies; increased globalization of data flows and access to personal data by law enforcement authorities by means of electronic data basis. What is more, at the time when the old directive was adopted, the Internet barely existed. Nowadays, however, reality data processing is taking place on websites, search engines and social networks. That is why the aim of the new legislative acts proposed by the Commission is to, broadly speaking, dealiniate the liability of - on one hand - internet users and - on the other - internet providers. This paper discusses data protection tools introduced by the European Commission; firstly, the European legal framework for data protection; secondly, the possible ways aimed at reinforcement of rights of data subjects, e.g. the definition of consent; thirdly, enhancement of responsibility of controllers and processors as well as liability of internet users and internet data providers in the context of the right to be forgotten; and finally the European case law concerning liability of Internet users and Internet providers.

Key words: *internet data providers, data subjects, data controllers/processors, definition of consent*

1. Privacy and data protection - history and current state of law

Privacy and data protection as a specific field of law have been elaborated over the last four decades, notably in the context of the Council of Europe and the European Union, stimulated by the growing impact of information and communication technology. The concept of the 'right to privacy' emerged in international law after the second World War. This was illustrated in the Article 12 of the Universal Declaration of

* dr Marta Kołodziejczyk, wykładowca Wyższej Szkoły Finansów i Prawa w Bielsku-Białej

Human Rights (UN General Assembly, Paris 1948) according to which no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. This declaratory level of protection became later lawful in Article 8 of the European Convention on Human Rights (Council of Europe, Rome, 1950), according to which everyone has the right to respect for his private and family life, his home and his correspondence, and no interference by a public authority with the exercise of this right is allowed except in accordance with the law and where necessary in a democratic society for certain important and legitimate interests. The above definition has been reflected in the series of judgments, e.g.: Leander v. Sweden (26.03.1987); Kopp v. Switzerland (25.03.1998); Amann v. Switzerland (16.02.2000), issued by the European Court of Human Rights in Strasbourg. However, in about 1970 the Council of Europe came to conclusion that Article 8 ECHR had a number of shortcomings, e.g. the uncertain scope of 'private life', the emphasis on interference by public authorities, as well as lack of a more proactive approach against the possible misuse of personal information by companies or other organizations in the private sector. As a result the Data Protection Convention, also known as Convention 108 (Strasbourg 1981) had been adopted and has been ratified by 44 Member states of the Council of Europe, including all EU Member States. Parties to this convention guarantee every individual, whatever his nationality or residence, respect for his/her rights and fundamental freedoms; in particular right to privacy, with regard to automatic processing of personal data relating to him/her ('data protection'). In addition, the concept of 'personal data' is defined as any information relating to an identified or identifiable data subject. Hence, 'data protection' is broader than 'privacy protection' because it also concerns other fundamental rights and freedoms, and all kinds of data regardless of their relationship with privacy.

Let us now consider some of the key provisions of the above mentioned Convention; personal data are to be "obtained and processed fairly and lawfully" and "stored for specified and legitimate purposes and not used in a way incompatible with those purposes". Personal data should also be "adequate, relevant and not excessive in relation to the purposes for which they are stored", "accurate and, where necessary, kept up to date". Other crucial principles expressed in the text of the Convention are: " appropriate security measures", "additional safeguards for the data subject such as the right to have access to his or her own

personal data, the right to obtain rectification or erasure of such data, and the right to remedy if such rights are not respected". To conclude, the Convention's philosophy is not that processing of personal data should always be considered as a breach of privacy, however, in its interests as well as other fundamental freedoms, any processing must always observe certain legal conditions. In this context, the core elements of Article 8 ECHR, such as interference with the right to privacy only on adequate legal basis, and where necessary for a legitimate purpose, have been transferred into a broader context. Furthermore, since 1997 the European Court of Human Rights has ruled in a number of cases that the protection of personal data is of "fundamental importance" for the right to respect of private life under Article 8 ECHR.

Although the Data Protection was put on the agenda of the Council of Europe and, as a result, exposed in the binding Conventions, this intergovernmental organization was less successful in terms of ensuring greater consistency across the EU. Some Member States were late in implementing the Convention, and those who did so arrived at different outcomes, in some cases even imposing restrictions on data flows with other Member States. Concerned that this lack of consistency could hamper the development of internal market involving a circulation of peoples and services, where the processing of personal data was to play an increasingly important role, the European Commission submitted a proposal for a Directive to harmonize the national laws on data protection in the private and most of the public sector. After four years of negotiations the 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 (DPD) has been adopted. It specified the basic principles of data protection already included in the Convention 108 of the Council of Europe. In the first place, it required all Member States to protect the fundamental rights and freedoms of natural persons, and in particular the right to privacy with the respect to processing of personal data, in accordance with the Directive. In this context, the data could be processed only if the data subject has unambiguously given his consent, if processing was necessary for the performance of a contract to which the data subject was party, or for compliance with a legal obligation, for the performance of a government task, in order to protect the vital interests of the data subject, or to protect the legitimate interests pursued by the controller, except where such interests are overridden by the interests of the data subject. Furthermore, the Directive committed the

controller to always inform the data subject about the purposes of the processing and other relevant matters in order to guarantee fair processing in respect of the data subject. In case of not fulfilling this condition, the data controller might become liable for committing an offence. Responsibility for compliance with national legislation on data protection belongs to supervisory authorities. Secondly, the Directive applies to the processing of personal data carried out "in the context of the activities of an establishment" of the controller on the territory of an EU Member State. In other words, where the controller is not established in the EU, the applicable law is that of the Member State in which the equipment used for processing is located. Thirdly, according to the Directive personal data may only be transferred to third countries that ensure adequate level of protection.

However, the Directive 95/46/EC (DPD) on the protection of individuals with regard to the processing of personal data and on the free movement of such data offers some important limitations[1]. First of all, Recital 17 of the DPD states that 'as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned . . . the principles of the Directive are to apply in a restricted manner.' Recital 37 goes in the same direction, by recognizing that 'the processing of personal data for purposes of journalism or for purposes of literary or artistic expression should qualify for exemption from the requirements of certain provisions of this Directive.' Moreover, Article 9 of the DPD creates an obligation for member states to adopt, in their national laws, exemptions or derogations from the provisions of chapters II, IV, and VI for the processing of personal data carried out solely for journalistic purposes or for the 'purpose of artistic or literary expression'. Such exemptions must, however, be necessary to reconcile the right to privacy with the rules governing freedom of expression'. Furthermore, the e-Commerce Directive recognizes that 'The free movement of information society services can in many cases be a specific reflection in Community law of

[1]Mario Viola de Azevedo Cunha, Luisa Marin Giovanni Sartor, Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web, in: International Data Privacy Law, 2012, p. 1-18;Giovanni Sartor and Mario Viola de Azevedo Cunha,*The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents,* in: „International Journal of Law and Information Technology", Vol. 0 No. 0 © Oxford University Press 2010; all rights reserved doi:10.1093/ijlit/eaq010

a more general principle, namely freedom of expression' (recital 9). Furthermore, with regard to liabilities for the illegal processing of personal data, the provisions of the DPD need to be coordinated with those of the e-Commerce Directive, which establishes, as we shall see, some exemptions for Internet Services Providers when they transmit, host, or cache user-generated content. The most recent European legislation seems to confirm the need to limit the liability of the provider. Indeed, Directive 2009/136/EC, amending the Universal Service Directive2[3], the Directive on privacy and electronic communications[4], and the Regulation on consumer protection cooperation[5] reaffirm that the provider cannot be liable for merely transmitting user-generated information (the 'mere conduit' rule) and that it is not a provider's task to define what is lawful or harmful as to content, applications, and services[6].

To conclude, the Directive 95/46/EC required the Member States neither to restrict nor prohibit the free flow of personal data between

---

[2]Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.

[3]Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and
services [2002] OJ L108/51.

[4]Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337/11.

[5]Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement
of consumer protection laws [2004] OJ L364/1.

[6] Recital 31 of Directive 2009/136/EC: 'In the absence of relevant rules of Community law, content, applications and services are deemed lawful or harmful in accordance with national substantive and procedural law. It is a task for the Member States, not for providers of electronic communications networks or services, to decide, in accordance with due process, whether content, applications or services are lawful or harmful. The Framework Directive and the Specific Directives are without prejudice to Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), which, inter alia, contains a "mere conduit" rule for intermediary service providers, as defined therein.'

them for reasons connected with such protection. This provision aimed at achieving an equivalent high level of protection in all Member States and as a result assure a balanced development of the internal market. However, this goal has not been entirely fulfilled due to the fact that the distinctive features of this particular legal act - Directive - allowed Member States fairly broad discretion on its transposition. In this context, it is worth to refer to the Treaties; Article 16 (2) TFUE mandates the European legislators to adopt 'the rules relating to the protection of individuals with regard to processing of personal data', without, however, specifying the type of legislative act to be chosen. As a consequence, in line with Article 289 (1) TFEU on the ordinary legislative procedure, the rules can be laid down in a regulation, a directive, or a decision. Let us note that a regulation has general application being at the same time directly applicable (it does not require implementation by EU member states), whereas a directive sets forth the results to be achieved, but leaves the means for achieving them largely up to implementation into national law by the members states. As a consequence, by now the Commission has launched several legal actions for improper implementation of the Directive; in March 2009, the Court of Justice in Luxembourg ruled (case against Germany) that the requirement of 'complete independence' for a supervisory authority means that it should be free from any external influence. This has been also recently confirmed and elaborated in a case against Austria. That is why the choice of regulation will according to the European Commission reduce legal fragmentation among member states in respect to different national data protection laws. This will lead e.g. to a net savings for companies of about €2.3 billion a year in terms of administrative burden alone. But even the regulation cannot result in complete harmonization of all legal provisions affecting data protection or totally eliminate the need to amend national laws. This fact may confirm that the type of legal instrument used is not determinative with regard to harmonization; for example it is also possible for a directive to leave little margin for member state implementation (e.g. EU Consumer Rights Directive 2011/83/EU). To conclude, the final proposal contains two legislative instruments that form the core of the data protection reform package: in the first place, the Regulation, setting out the general EU framework for data protection; secondly, the Directive for the police and criminal justice sector which is due to replace Framework Decision 2008/977/JHA which covers the protection of personal data processed by police and

judicial authorities in criminal matters.

Another crucial reason for the review of the Directive 95/46/EC has to do with the new institutional framework of the EU. The Lisbon Treaty (December 2009) emphasizes fundamental rights; Article 16 provides for comprehensive data protection in all policy areas, regardless of whether it relates to the internal market, law enforcement, or almost any other part of the public sector. Not to mention about the separate right to the protection of personal data laid down in Article 8 of the Charter of Fundamental Rights that became legally binding on the EU institutions and national governments with the entry into force of the Treaty of Lisbon.

2. Reinforcement of the rights of data subjects

The need for reform of current EU data protection legislation can be explained by the rising impact of IT technologies on our lives. Specifically, at the time when the Directive was adopted the Internet barely existed. However, in nowadays reality the data processing is taking place on the web sites, by search engines or social networks. What is more, in 2000, when 40 the EU e-Commerce Directive was passed, web hosting consisted mainly in websites (html pages and related documents) completely developed by the recipient of the hosting service, including the way the content was posted, the structure of the websites and so on. The host provider only made available the server (disk-space and processor) for storing the website, the connection from that server to the Internet, and the software (the web-server) that would provide access to the website (by typing a domain name or using a search engine). While the recipient of the service had the greatest freedom in developing the website according to his or her tastes and preferences, editing web pages was relatively difficult and complicated, and thus the web could not be a creative space for the majority of people. However, Web hosting has dramatically changed in the last years. Now platforms are available that facilitate the creation and distribution of online contents, thus enabling everyone to participate in these activities. Among the most popular platforms used worldwide we can name iTunes and YouTube for videos, Facebook for personal information, Wordpress for blogs, Twitter for short messages, e-Bay for auctions; the list is far from being exhaustive. Such platforms, to a different degree, support the creative activity of the users: first, they provide facilities (and constraints) for creating content, such as

page templates, ways to organize the information and link it, apps for an infinite variety of functions; secondly, they facilitate the retrieval of the user- generated materials, by indexing, classifying, ranking them (usually by aggregating users' preferences and choices). Such platforms are mostly run by commercial companies that usually make a profit by associating advertisements to the user-generated materials, often by selecting the ads on the basis of the content of such materials. Google, whose mission is 'to organize the world's information and make it universally accessible and useful', exemplifies this business model[7]. However, in this virtual reality where internet users have been transformed from passive content receivers to active content providers, more than two-thirds of Europeans -72 per cent (according to the survey) - expressed their concerns connected to uncontrolled usage of their data personal data by companies on the Internet[8]. The official comment of the European Commission seems to mirror these feelings; the document is focused on such challenges for the protection of personal data in the future as: the astounding capabilities of modern technologies; the increased globalization of data flows; and access to personal data by law enforcement authorities that is greater than ever. That is why the aim of the new legislative acts (Regulation, Directive) proposed by the Commission is to strengthen individuals rights by improving the ability to control their data[9] by clarifying the requirement of consent as one possible ground for lawful processing of personal data, by delineating liability of internet users/providers as well as reinforcing the rights of individuals to request the controller to delete unlawfully processed personal data (right to be forgotten).

3. Definition of consent in the EU law

It is worth to mention that the 'consent' is currently defined in Articles 2(h) and 7(a) of Directive 95/46/EC as 'any freely given specific and informed indication' of a data subject's wish to agree to the processing of his personal data. In addition, this agreement must be

[7]Mario Viola de Azevedo Cunha, Luisa Marin, and Giovanni Sartor, *Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web,* in: "International Data Privacy Law", 2012, Pp. 1-18

[8]Albrecht Report 2013, p.1-7

[9] Kosta E., Consent in European data protection law, Martinus Nijhoff Publishers, The Hague 2013, Pp. 261-381

'unambiguously' given in order to make the processing of personal data legitimate. However, national laws have transposed this concept quite differently. Consequently, national supervisory authorities tend to apply variable interpretations of consent. Furthermore, the meaning of 'unambiguously' given consent is interpreted in a differentiated manner: in some member states consent has to be given 'expressly' and in some cases even in writing, while other member states also accept some forms of implied consent. As a consequence, valid consent in one member state may not be legally valid in others, therefore creating uncertainty amongst controllers operating in several member states on whether a data processing operation is lawful or not. Hence, in the proposed Regulation the definition of 'the data subject's consent' of Article 4(8) is remedied by adding the criterion 'explicit' which allows to avoid the confusing parallelism with 'unambiguous'. Moreover, where consent is the legal ground for data processing, Article 7 states that the controller must be able to demonstrate that consent has taken place. A the same time, the Regulation reaffirms that the data subject may withdraw his or her consent at any time, bearing in mind that this will only take full legal effect for future processing. Furthermore, consent is excluded in Article 7(4) as a ground for processing in specific cases of significant imbalance between data controller and data subject, for example in the framework of an employment relationship. Similarly. Article 8 sets out further conditions for the lawfulness of consent for processing of personal data of children below the age of 13 years in relation to services offered to them on-line.

In the context of reinforcing the rights of data subject, it is worth to emphasize that the proposed Regulation enhances administrative and judicial remedies when data protection rights are violated. In particular Article 76 (1) enables certain associations, for example consumer protection associations whose statutory aim includes the protection of personal data, to bring actions, on behalf of one or a group of data subjects whose rights may have been violated, to court. Similarly, article 73 (3) of the proposed Regulation provides that these data protection NGOs, in cases of personal data breaches, may address a supervisory authority in any member state in their own right; without obligation to obtain data subject's authorization to act on his behalf.

As far as the national authorities responsibilities for data protection are concerned, the proposed Regulation strengthens their potential for initiating legal actions by: a) clarifying the conditions for the

establishment and for ensuring the complete independence of supervisory authorities in member states (Articles 46-50); b) providing for fully harmonized provisions for the competences, duties, and powers of the supervisory authorities (Articles 51 to 54); c) and as a result creating legal basis and conditions for an efficient cooperation between supervisory authorities established in EU Member States (Articles 55 to 56); d) introducing the 'one-stop-shop rule that gives companies operating in more than one member state, a single supervisory authority responsible for monitoring their personal-data processing activities in the EU, rather than force a company to deal with multiple bodies in different countries.

4. Enhancing the responsibility of controllers and processors

In the first place, it is crucial to define the above terms; as a result, controller is defined as natural or legal person, public authority, organization, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Secondly, processor, on the other hand, is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. Furthermore, as far as the controller's responsibilities are concerned (article 22 of the Regulation) in the framework of data protection reform, the new legislative acts (regulation, directive) focus on controllers' obligation to be able to 'demonstrate' compliance with the Regulation by adoption of internal policies for ensuring such compliance. The effectiveness of such mechanisms must be verifiable either by internal or external data protection specialists or by data protection certification mechanism envisaged under Article 39. In addition, in order to give data subjects greater control over their personal data, the Regulation sets out further obligations for the controller by requiring him to apply the principles of 'data protection by design' and 'data protection by default' (Article 23).

In the first place, data protection by design means that controllers of data – whether companies or public bodies – take a positive approach to protecting privacy, by embedding it into both technology (for example hardware like computer chips or services like social networking platforms) and into their organizational policies (through, for example, the completion of privacy impact assessments). Secondly, privacy by default means that when a user receives a product or service, privacy

settings should be as strict as possible, without the user having to change them. In this way, everyone feels comfortable to consciously choose the privacy setting within which he feels most comfortable with. Rather than allowing the service provider making a guess about what he might prefer. In addition, service providers should support their users in this by providing user-friendly methods to change privacy settings. Not to mention about the need for transparency enshrined in data processing practices.

5. Responsibility of controllers and processors in the European Case law

In order to exemplify the general parameters for liability of internet users as well as internet data providers in the context of data protection law in the on-line environment, this section discusses the following judgements: Italian Google case, Google Spain SL, K.U. v Finland judgment, Linqvist judgement.

The European jurisprudence has set some general parameters for liability of internet users as well as internet providers in the context of data protection law in the on-line environment. Among many judgements referring to the judicial development of the data protection law one may distinguish Italian Google case. The facts of the case look the following. On September 8, 2006 a video was posted in Google Videos showing a disabled student being bullied and insulted by three of his colleagues (while another student was recording with her mobile phone, and ten more were watching the scene without intervening). More precisely the disabled student, suffering from autism and impairment in hearing and sight, was the object of both verbal and physical abuse. In particular, he was called a "mongolo" (a derogatory term used for people affected by Down syndrome) and in this connection a reference was made to the "Associazione Vivi-Down", a charity providing assistance to persons affected by the Down syndrome. The video, which had duration of about 3 minutes, was viewed by a high number of people (more than 5000 downloads). At a certain point it was the most popular one in the category of "video divertenti" (funny videos). Users of Google video posted various messages comment- ing on the video (starting on 4 October); some flagged the video as being inappropriate and some e-mailed Google requesting for the video to be removed. However, evidence exists only for a flagging on 5 November 2006 and an email

request on the following day (Google stated that it was unable to provide documentation of all comments and flaggings). On the 7th of November, the Italian Postal Police, after a communication from a citizen, requested Google to take down the video, which was removed on the same day. Thus, the video had remained available for about two months after it was initially posted. As a result, the posting of the video gave rise to three distinct lawsuits: 1) the first concerned the four students having an active role in the video (the three abusers and the movie maker). They were identified, thanks to the information on their identities provided by Google, and were condemned by the Tribunal of Turin with a one year sentence (work in social services), for assault and slander. The second lawsuit, still pending in Turin, concerns the teacher and the school (for failing to prevent the offence)[10] The third lawsuit, which is the one here considered, concerns Google, namely its Italian partner company (Google Italy) and its executives. The charges brought against them consisted of criminal defamation and violation of data protection rules. With regard to defamation the indictment was of "concorso in diffamazione aggravata" (co-participation in aggravated defamation), that is of contributing to the defamation of the disabled teenager. With regard to data protection the indictment was that Google Italy was processing personal data, and in particular health data, illicitly, for the purpose of making a profit. The case was decided on 24 February 2010 by the Italian Judge Oscar Magi: all four Google executives were acquitted with regard to the charge of defamation, and three of them were sentenced to a six-months suspended jail sentence for violation of data protection law. The decision occurred to be controversial; by many it was perceived as an attempt to initiate censorship in the internet. However, on the other hand, there were also some voices heard advocating the need to intervene in Italy against the publication of insults and threats against politicians and other public persons in the months preceding the Google incident (internet bloggers in particular were accused of having instigated an aggression against the Prime Minister, Silvio Berlusconi). That is why commentators openly approved the decision, finding it immoral that Google could be exempted from any liability for the damage suffered by innocent people as a consequence of Google's commercial activity

[10] Sartori Giovanni and Viola de Azevedo Cunha, Mario, The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents (May 11, 2010). International Journal of Law and Information Technology. Available at SSRN: http://ssrn.com/abstract=1604411 , pp. 1-2.

(providing user-generated contents), from which it draws huge profits, in particular by collecting advertising (in 2009 USD$22 billions of advertising revenue). Especially that Google was considered to possess technical means to control content and exclude offending postings, however, it refrained from such controls for the sake of cutting costs (by savings on personnel) and maximizing profits (by attracting the vast audience interested in prurient, lurid or offending contents).

Let us now dwell on the charges brought against Google executives: defamation and breaching data protection law. In the former, according to the Italian judge the executives had the legal obligation to prevent the defamation by exercising a preventive control over contents loaded on Google Videos site, but they had not taken such action. That is why the criminal liability of the Google executives for defamation did result from their failure to act: the executives had the legal obligation to prevent the defamation by exercising a preventive control over contents loaded on Google Videos site, but they had not taken such action (according to Art. 40 of the Italian Criminal Code, failing to prevent an event which one has the legal obligation to prevent, amounts to causing it). In addition, according to the prosecutors Google was no mere host provider, but rather a content provider, who had the obligation to correctly process the personal data contained in the uploaded videos and had the duty to avert those crimes that may be prevented by correctly processing the data. Since the failure to correctly process the personal data (i.e. the failure to ensure that only data that could be legally processed were uploaded and made available through the internet) caused the defamation to happen, Google executives in charge of the processing of personal data were liable for defamation[11]. However, the judge did affirm that even though he wished that a law were issued making internet providers liable for Negligence, this had not yet been the case. Given the state of the Italian law, there was no general obligation for hosting providers to monitor the contents of postings on their platforms[12]. Thus, he dismissed the charge for defamation: since Google had no obligation to prevent the upload of offensive materials, it was not criminally liable for defamation

[11] ibidem

[12]"it does not exist, at least until today, a legal codified obligation which imposes to inter- net service providers to exercise prior control over the uncountable series of data that pass every second through the network of the managers or owners of websites (. . .)". Sentenza n. 1972/2010. Tribunale Ordinario di Milano in composizione monocratica. Sezione 4 Penale. P. 103.

subsequent to the upload of such materials. It is worth to mention in this context, that this reasoning mirrors the Art. 15 of the EU Directive on Electronic Commerce, which forbids EU Member States to "impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances".

Another landmark judgement gives European Union citizens a right to be forgotten online, in other words the right for an individual user to have his or her personal online data removed from the web. It is worth to mention that this legal rule has been officialy acknowledged in the judgement Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González (Google Spain v. AEPD), issued by the European Court of Justice. The case concerned a reference for a preliminary ruling made by the Spanish High Court to the CJEU, which arose out of a dispute between Google Inc and Google Spain on the one hand, and Mr Costeja González and the Spanish Data Protection Agency on the other. Let us now dwell on the facts of the above mentioned case; In 2010, Mario Costeja González, a Spanish national, filed a complaint with the Spanish Data Protection Agency ("Agencia Española de Protección de Datos", "AEPD") against La Vanguardia Ediciones SL, a large publisher of daily news in Spain, as well as Google Spain and Google Inc.[13] González, the data subject seeking erasure, contended that whenever a Google search of his name was carried out, the top results listed linked the Internet user to two property auction notices for the recovery of social security debts that Mr Costeja González had owed 16 years earlier, which still appeared on La Vanguardia's website. Furthermore, the applicant claimed that these articles "although truthful, injured his reputation and invaded his privacy."[14] That is why, González demanded that the Spanish newspaper erase them because they were no longer relevant, since the proceedings had concluded more than a decade ago[15]. The newspaper publisher refused to erase the articles because the Ministry of Labour and Social Affairs had ordered their

[13]Case C-131/12, Google Spain SL. v. Agencia Española de Protección de Datos (May 13, 2013), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.
[14]Dave Lee, What Is the "Right To Be Forgotten"?, BBC (May 13, 2014), http://www.bbc.com/news/technology-27394751.
[15]Google Spain SL, Case C-131/12, 15.

publication[16]. Next, the plaintiff demanded that Google remove the link to those stories and thereby eliminate any association to his name.The applicant sought to obtain an order to the effect that the newspaper should alter, delete, or protect this information, and that Google should either delete or conceal the links to those pages.As far as the procedural History of Google Spain v. AEPD is concerned, the Spanish Data Protection Agency (AEPD) ruled that Google was responsible as a data controller for removing results about the plaintiff from its search engine.[17] After the AEPD's decision, Google brought action before the Audiencia Nacional, Spain's highest court, which referred the case to the Court of Justice of the European Union. As a consequence, on June 25, 2013, Advocate General Niilo Jääskinen issued his advisory opinion, finding that Google had no responsibility to remove any links on its search engine based on a privacy claim[18]. He reasoned that suppressing legitimate and legal information already in the public domain would interfere with freedom of expression and undermine the objectivity of information o the Internet[19]. However, the CJEU rejected the Advocate Generals's argument and recognized a broad right to be forgotten under Spain's implementation of Directive 95/46/EC.[20] The court found, in the first place, that Google, as an indexer of information, was processing personal data and therefore subject to the Directive's obligations for data controllers.

Secondly, the court drew upon Articles 12(b) and 14 (a) of the Directive to hold that Google owed a duty to erase information from its search index (Google Spain SL, Case C-131/12) Thirdly, the CJEU rejected Google's argument that imposing a duty to remove personal data violated the principle of proportionality, and that such removal must be addressed to the publisher of the website because the publisher was responsible for making the information public. Furthermore, court reasoned that search engines make access to this information effortlessly available, because they enable users to obtain information about a data

[16]Opinion of Advocate General Jääskinen 19, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014) (Case C-131/12), http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&doclang=EN.
[17]Google Spain SL, Case C-131/12, 17.
[18]Opinion of Advocate General Jääskinen, supra note 87, 138.
[19]Id. 120–34.
[20]Google Spain SL, Case C-131/12.

subject by simply typing the subject's name.[21] What is more, due to their preeminent role in organizing data, search engines like Google are far more likely to interfere with the data subject's right to privacy than the original website publisher. (Id. 87.) Google, on the other ha[22]nd, argued that the least cost avoider for removing access to the information was the website and not the search engine. Hence, the requirement of a search engine to remove content from its index would take insufficient account of the fundamental rights of publishers of websites, of other internet users and of the operator itself[23]. To conclude, according to the recent judgment (ECJ Ruling C-131/12) of the EU Court of Justice where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing (§93 of the ruling) individuals have the right - under certain conditions - to ask search engines to remove links with personal information about them. In this vein, in case of giving consent as a child not being aware of risks by envisaged processing, the new law allows this individual to remove any such data which were made public on Internet at that time. At the same time, the Court explicitly clarified that the right to be forgotten is not absolute but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media (§85 of the ruling). It is also worth to mention that, according to the judgment of the European Union Court of Justice, 'the right to be forgotten' cannot amount to a total deletion of history (Joint Cases C-92/09 and C-93/09 Volker and Markus Schecke and Eifert (2010) ECR 1-000, §48). Hence, a case-by-case assessment is needed considering the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access

[21]Google Spain SL, Case C-131/12, 80.

[22]Michael Rustad, Global Internet Law in a Nutshell, West Academic 2015, p. 218

[23]In the context of the above mentioned judgement of the Court of Justice of the European Union it is worth to mention that the British House of Lords observed that the judgment of the Court is unworkable due to the fact that it does not take into account the effect the ruling will have on smaller search engines which, unlike Google, are unlikely to have the resources to process the thousands of removal requests they are likely to receive. In addition, the House of Lords sub-committee, noted that the expression, 'right to be forgotten' is misleading because Information can be made more difficult to access, but it does not just disappear. Furthermore, they argue that it is "'wrong in principle' to leave it to search engines to decide whether or not to delete information, based on 'vague, ambiguous and unhelpful' criteria. See:European Union Committee - Second Report EU Data Protection law: a 'right to be forgotten'?"23 July 2014 http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/4002.htm, (September 2015)

to that information. The role the person requesting the deletion plays in public life might also be relevant. Moreover, the traditional right to erasure ('right to be forgotten') expressed in the Regulation is further strengthen in such a way that the controller who has made the personal data public is obliged to inform third parties processing the data that the data subject has requested the controller to erase any links to, or copies or replications of that personal data. However, appreciating this provision the EDPS recognizes that it may be in some cases a huge effort to inform all third parties who may be processing such data, as there will not always be clear understanding of where the data may have been disseminated[24].

The K.U. v Finland judgment of the ECtHR limits the duty/right to confidentiality of Internet service providers (and the protection of the privacy of their users), for enabling the protection of the rights of third parties and the prosecution of wrongdoings. The applicant was a 12-year-old boy, who complained that an unknown person had, without his knowledge, placed an advertisement in his name on a dating site. The advertisement contained personal information of the applicant (name, phone number, link to personal page with photo, and description of physical aspects) and had a sexual connotation. The applicant became aware of the advertisement when somebody contacted him for a meeting. The Internet service provider refused to reveal the identity of the IP address-holder, as it was bound by a duty of confidentiality according to Finnish telecommunications law. The Helsinki district court refused to oblige the service provider to disclose identification data in breach of professional secrecy, since there was no explicit legal provision authorizing the disclosure. More precisely, according to that court, malicious mis- representation was not an offence authorizing the police to obtain telecommunications identification data. Other domestic courts upheld this position. The final result was that the applicant never got access to the identity of the person in question, and the managing director of the Internet service provider could not be prosecuted. However, the Strasbourg court found that this outcome violated the right to private life, as defined in Article 8 of the ECvHR, 'a concept which covers the physical and moral integrity of the person'. The right protected by Article 8 does not lead merely to a negative obligation on the state, but might also entail a posi- tive obligation 'inherent in an effective respect for

[24] EDPS 2012, p. 24-25

private or family life'. According to the Court, 'these obligations might involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals among themselves'. While States have a margin of appreciation in fulfilling the obligation arising from the Convention, the latter nevertheless places limits on this margin of appreciation. The Court, while acknowledging that 'freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder obligation on the state, but might also entail a positive obligation 'inherent in an effective respect for private or family life'. According to the Court, 'these obligations might involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals among them- selves'. While States have a margin of appreciation in fulfilling the obligation arising from the Convention, the latter nevertheless places limits on this margin of appreciation. The Court, while acknowledging that 'freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others'[25].

While considering the liability of internet users in the on-line environment, it is also worth to mention the Lindqvist judgment of 2003 which addressed the application of the DPD to personal data posted on Internet websites. Ms Lindqvist, who worked as catechist for a parish in Sweden, set up Internet pages for parishioners preparing for a sacrament. In those pages she provided information about herself and 18 fellow parishioners-catechists, indicating full names, jobs, hobbies, phone numbers, and other matters. Ms Lindqvist posted health related information about a person who had injured her foot and consequently worked half time on medical grounds. As a result, the European Court of

[25]Mario Viola de Azevedo Cunha, Luisa Marin and Giovanni Sartor . Peer-to-peer privacy violations and ISP liability, in International Data Privacy Law, 2012, Vol. 2, No. 2, p. 55 https://www.utwente.nl/bms/pa/staff/marin/marin-peertopeerprivacy violations.pdf

Justice held that the act of mentioning, on an Internet page, individual persons, identifying them by name, and giving information about them, constitutes processing of personal data. Moreover, according to the ECJ 'the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people is not covered by the exception provided for by Article 3(2) of the DPD, which only excludes from data protection the data-processing activities carried out in the course of the private or family life of individuals. Furthermore, the judgment also addressed the relation between the DPD and the general principles of EU law, in particular,the fundamental rights enshrined in the European Convention of Human Rights, such as freedom of expressionin particular. The ECJ stated that member states have a margin of manoeuvre in implementing the DPD, and emphasized the role of national jurisdictions, stating that 'it is for the national courts to ensure a fair balance between rights and interests in question, including the fundamental rights protected by the European order.' The Lindqvist judgment provides a useful frameworkfor understanding how data protection rights can be applied even when no economic activities are involved. Excluding charitable and religious activities from data protection would have made the application of the DPD very uncertain, depending on the qualification ofthe concerned activity. The narrow interpretation givento the private or family life exception is particularly relevant, since it implies the application of data protection to individual users posting online information. To conclude, we then need to establish how to apply the same data protection rules to two very different kinds of data con- trollers: on the one hand bone fide individuals, namely, users processing personal data for their individual purposes, and, on the other hand organizations processing personal information on large scale for commercial purposes.

6. Final remarks

The above described reform constitutes a huge step forward for data protection in Europe, considered by some as "Copernican revolution". The proposed rules will strengthen the rights of individuals and make controllers more accountable for how they handle personal data. Especially that, the online publication of user-generated content including personal data directly concerns a conflict between the user posting the information and the data subject, and thus a conflict between

the user's freedom of expression and the data subject's privacy and data protection rights. However, it also involves the Internet Service Provider, on whose platform the content is published and distributed. As we have seen above, the role of the Internet Service Provider (ISP) can be construed in different ways. On the one hand, the ISP may appear to be co-responsible for the violation of privacy: the ISP contributes the means through which the privacy violation is committed, and does that for a profit (Google Italy case; K.U. v Finland judgment of the ECtHR). Moreover, by making the information easily accessible and searchable the ISP enhances its illicit circulation. On the other hand, the ISP has the role of an enabler, rather than that of an author, of the violations. In fact, by providing users with the possibility of free and uncensored use of its platform, the provider contributes, while aiming at a profit, to the free development of citizens personality, to the growth of civil and political debate, and to the creativity of the Internet. However, the ISP may also be ordered to remove an individual's personal data from the web (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González (Google Spain v. AEPD).

It is undeniable that the multifaceted role of ISPs, and the different legal values involved in their activity, explains why there is an on-going debate over whether and to what extent they should be liable for illegal user-generated contents, the debate that is likely to continue in the future. To conclude, in EU law, which is the focus of this article, two conditions are required for the provider to block or remove illegal content (so preventing the violation or its continuation): first of all, the provider must be aware that the user has carried out a certain activity, and secondly, he must obtain knowledge that the content generated by that activity violates someone else's rights (in particular privacy rights). However, while considering whether to limit the liability of providers it has often been affirmed that the provider cannot be made responsible since the provider cannot reasonably control all user-generated content. However, it has to be also taken into consideration that, in fact, establishing that user-generated content is illegal often involves an uncertain balancing exercise: the legality of the distribution of the content depends on whether, under the particular conditions of the case, the uploader's civil rights (and in particular his or her freedom of expression) should prevail over the third party's privacy rights. By making the ISP responsible for the illegal content hosted in its platform, even without a request by a competent authority, we put the burden of

establishing whether the content is illegal on the ISP[26]. Thus there is a risk of favouring an excessively cautious attitude by the provider, who, to prevent possible liability, would indulge in censorship whenever there is the smallest risk of a judicial decision in favour of privacy, thereby unduly restricting freedom of expression. Not to mention about the risk that those who want to prevent the distribution of information about themselves will threaten to sue providers for privacy violation, to induce the providers to censor the concerned content, even when it expresses legitimate criticism. This is the fundamental legal and political issue that underlies the more specific and apparently technical questions involved in this subject matter, namely the issues of whether the provider or the user is the data controller, of when online distribution can be considered to be a private activity (to which data protection is inapplicable) having limited accessibility, of whether and to what extent the liability exemption for host providers also concerns violations of privacy. Current rules limiting the liability of host providers with regard to user-generated content give the most appropriate balance between the interests and the rights involved. This conclusion does not exclude the need for providers to take initiatives concerning the education of their users with regard to data protection. In particular, platform providers should be urged (by the competent data protection authorities) to provide their users with better information about the need for 1725 other people's privacy rights to be respected, as suggested by the Article 29 Working Party. These precautionary measures would be fully consistent with the limitation of the provider's liability, since they do not impose any censorship on users, but are only meant to make them aware of their pre-existing data protection duties.

REFERENCES

[1.] Council Framework Decision 2008/977/JHA of 27 November 2008, available online: http://eur-ex.europa.eu/LexUri Serv/LexUri Serv .do?uri= OJ:L:2008:350:0060:0071:en:PDF.

[2.] Directive (EC) 95/46 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 (1995) OJ L281/31 ('Directive 95/46/EC').

[3.] EDPS Opinion of 7March 2012, available online:

[26]*Peer-to-peer privacy violations and ISP liability …,* P. 17

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, Pp. 24-25.

[4.] EU Consumer Rights Directive. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (2011) OJ L304/64.

[5.] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337/11.

[6.] European Union Committee - Second Report EU Data Protection law: a 'right to be forgotten'?" 23 July 2014 http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/4002.htmFuster, 7. G., The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing, Switzerland 2014, Pp. 3-33, ISBN:978-3-319-05022-5.

[7.] Gutwirth, S. – Leenes R.- de Hert P. (ed.): Reforming European Data Protection Law, Springer, Dordrecht Heidelberg-New York-London 2015, Pp. 3-15 , ISBN: 978-94-017-9384-1.

[8.] Hustinx P., EU Data Protection Law – Current State and Future Perspectives, High Level Conference: "Ethical Dimensions of Data Protection and Privacy", Center for Ethics, University of Tartu/Data Protection Inspectorate, Tallin, Estonia, 9 January 2013.

[9.] Kosta E., Consent in European data protection law, Martinus Nijhoff Publishers, The Hague 2013, Pp. 261-381, ISBN: 9789004232358.

[10.] Kunert Ch., The European Commission's Proposed Data Protection Regulation: A Copernican Revolution In European Data Protection Law, in: The Bureau of National Affairs 2012, Inc. (800-372-1033), available online: http;//www.bna.com

[11.] Dave Lee, What Is the "Right To Be Forgotten"?, BBC (May 13, 2014),

[12.] http://www.bbc.com/news/technology-27394751.

[13.] Mario Viola de Azevedo Cunha, Luisa Marin Giovanni Sartor, Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web, in: International Data Privacy Law, 2012, p. 1-18.Paul Craig & Grinne de Búrca, EU Law: Text, Cases and Materials, Oxford University Press 5th ed. 2011, Pp. 105-106.

[14.] Proposed EU Data Protection Regulation One Year Later: The Albrecht Report, in: "Privacy &Security Law Report, 12 PVLR 99, 01/21/2013, Pp. 1-7.

[15.] Reding v., The European data protection framework for the twenty-first century, in: "International Data Privacy Law"2012, Vol. 2, No. 3, Pp. 119-129

[16.] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to processing of personal data by the Community institutions and bodies and on the free movement of such data (2001) OJ L 008/1.

[17.] Rosen J, The Right to be Forgotten, 64 Stanley Law Review Online 88, February 13, 2012, Pp. 88-92.

ODPOWIEDZIALNOŚĆ INTERNAUTÓW ORAZ DOSTAWCÓW DANYCH W KONTEKŚCIE REFORM EUROPEJSKIEGO PRAWA O OCHRONIE DANYCH

Streszczenie

25 stycznia 2012 roku Komisja Europejska zainicjowała proces reform unijnych przepisów ochrony danych osobowych motywowany ogromnym wpływem na ludzką egzystencję technologii teleinformatycznych, w szczególności Internetu. Umożliwia on niekontrolowany przepływ danych osobowych jego użytkowników w skali globalnej. Stąd, niezbędne jest, w opinii Komisji, doprecyzowanie odpowiedzialności - z jednej strony - użytkowników Internetu - z drugiej - jego dostawców, co zostało opisane w powyższym artykule.

Słowa kluczowe*: Internetowi dostawcy danych, osoba, której dane dotyczą, administrator danych, podmiot przetwarzający dane osobowe, definicja zgody na przetwarzanie danych*