DOI: 10.12818/P.0304-2340.2017vBIp305

INTERNET LAW TRENDS IN EUROPE: A CASE LAW PERSPECTIVE

TENDENZE DEL DIRITTO DI INTERNET IN EUROPA: UNA PROSPETTIVA GIURISPRUDENZIALE

Nicola Lugaresi[*]

ABSTRACT

In the last few years the Court of Justice of the European Union and the European Court of Human Rights have issued many important decisions concerning Internet law. In particular, the case law has faced, among others, three fundamental aspects: conflicts of jurisdiction, personal data protection and Internet service providers' liability.

This paper aims at analyzing the main decisions, in the framework of the EU legislation, in order to verify whether the Courts are following a precise strategy in their case law. Within the decisions, that may have a broader scope, the relevant legal profiles are singled out in the context of such an assumption.

The answer to the question (is there a strategy?) is positive. While the three aspects may be separately considered, their tight mutual connection shows how Europe is trying to taking on a leading role in Internet governance, counterbalancing the traditional power of the United States and of the big Internet companies (Google, Facebook, Microsoft) on one side, and affirming its values (data protection above all) on the other side.

KEYWORDS: Internet law. Jurisdiction. Personal data protection. Internet service providers. Free speech.

ABSTRACT

Negli ultimi anni, la Corte di Giustizia dell'Unione Europea e la Corte Europea dei Diritti dell'Uomo hanno emanato una serie di importanti sentenze riguardanti il diritto di Internet. In particolare, la giurisprudenza ha affrontato, tra gli altri, tre aspetti fondamentali: i conflitti di giurisdizione, la protezione di dati personali e la responsabilità dei fornitori di servizi Internet.

Il paper mira ad analizzare le decisioni principali, nell'ambito della normativa UE, per verificare se le Corti stiano seguendo una precisa strategia nella loro giurisprudenza. All'interno delle sentenze, che possono avere un oggetto più ampio, i profili giuridici rilevanti sono individuati nel contesto di un tale assunto.

La risposta alla domanda (esiste una strategia?) è positiva. Se anche i tre aspetti possono essere considerati separatamente, la loro stretta interconnessione mostra come l'Europa stia cercando di assumere un ruolo preminente nella governance della Rete, da un lato controbilanciando il tradizionale potere degli Stati Uniti e delle grandi compagnie operanti in Rete (Google, Facebook, Microsoft), e dall'altro affermando i suoi valori (soprattutto la protezione dei dati personali).

***PAROLE CHIARE**: Diritto di Internet. Giurisdizione. Protezione dei dati personali. Fornitori di servizi Internet.Libertà di espressione.*

* Professor of Law. Trento University Law School (Italy).
E-mail: nicola.lugaresi@unitn.it

1 INTRODUCTION: DIFFERENT PERSPECTIVES

Some months ago, at a conference in the United States, the panel I was invited to had a bizarre title: "Has the European Union gone insane?"[1]. I loved that title. It expressed effectively both the puzzled reaction American colleagues show to European Union recent legal developments on some issues concerning the Internet, and the distance between the values across the Atlantic. As an European I had to give a first answer, which was: "no". It is not a folly (to be praised or not), it is a strategy. A further question naturally arises: is it a good, coherent, strategy or is it a bad, inconsistent, strategy?

This paper aims to point out the strategy itself, starting from the analysis of the most relevant and recent EU case law, in particular from the Court of Justice of the European Union (CJEU). The analysis, though, will not be limited to the EU, as interesting inputs are provided by the case law of the European Court of Human Rights (ECtHR)[2], based on the European Convention on Human Rights (ECHR).

This paper will also show three components of this strategy, that can also be seen as separate strategies themselves: the expansion of EU jurisdiction over cases and matters that happen "in cyberspace"; the supremacy of privacy protection (actually, even more, of personal data protection) over other fundamental rights and general interests; the reinterpretation of the role of Internet

1 It was the Computers, Freedom and Privacy Conference 2015 (Alexandria, VA, United States, 12-14 October 2015). Credits for the title go to the journalist, blogger and folksinger Wendy M. Grossman, who conceived, organized and baptized the panel.

2 The European Court of Human Rights, set up in 1959 and based in Strasbourg, rules on alleged violations of the European Convention on Human Rights, signed in Rome in 1950. Both Member States of the Council of Europe (currently forty-seven, including all the twenty-eight Members of the EU) and citizens of those States can directly lodge an application if they deem that civil and political rights protected by the Convention have not been respected. The judgment of the Court is binding on the countries concerned: in case of violations, they should intervene by modifying their legislation and/or their administrative practices. While the Court of Justice of the European Union judgments are based on the EU treaties and EU secondary legislation, the ECtHR judgments can take them into account, but they are nonetheless based primarily on the ECHR, which can create some conflicts.

service providers (ISPs) and, in particular, of their liability for third parties actions.

There is more, though. The EU recent activism in Internet law expresses, along with these three legal trends, a strong political goal: making the EU itself a main actor in the regulation of the Net, opposing (mainly) the United States and its hierarchy of values[3]. Hence, for the most evident example of this cultural clash, a different perspective on the balance between privacy and freedom of speech[4]. Moreover, the EU is trying to set up rules that can regulate its complex relationship with the big Internet companies (usually US based), like Google, Facebook, Microsoft, Twitter. Big dot-com, as a matter of fact, can play different roles: they can violate rules (in different fields, from privacy to taxation to competition and so on), but they are also strong economic actors, and they may, not always enthusiastically, help Member States in law enforcement[5]. It is a bizarre relationship, made of intertwined co-operation, support, assistance, negotiations, bargaining, threats, sanctions. And strained smiles.

2 JURISDICTION EXPANSION

In the last few years there are two cases of the European Union Court of Justice that, not surprisingly, sparked the interest of legal and political commentators on both sides of the Atlantic: *Google Spain*[6] and *Schrems*[7]. Both cases were brought to the Court

3 See MAYER, 2000, p.149.

4 See CHARLESWORTH, 2000, p.167; LESSIG, 2006, p.200; SOLOVE, 2007, p.105; ZITTRAIN, 2008, p.200; SOLOVE, 2012, p.15; STONE, 2012, p.175; LARSON III, 2013, p.91.

5 See the recent Code of Conduct on countering illegal hate speech online (31 May 2016), issued by the EU Commission together with Facebook, Twitter, YouTube and Microsoft; the Code of Conduct includes a series of commitments for the IT companies aimed at combating hate speech online in Europe.

6 CJEU 13 May 2014, case C-131/12 ("*Google Spain*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-131/12&td=ALL last visited on 30 June 2016].

7 CJEU, 6 October 2015, case C-362/14 ("*Schrems*") [http://curia.europa.eu/juris/liste.

of Justice of the European Union. Both cases involved American big dot-com companies. Both cases led to discussions about jurisdiction issues and fundamental values, highlighting the differences between the EU and the US legal approaches.

Google Spain is mainly known for the "right to be forgotten" affirmed and its consequences on the balance between data protection and free speech. The debate concerning the right itself and its implementation, is still open[8]. Nevertheless, its effects on jurisdiction conflicts[9] related to Internet activities (in particular, search engines activities), and the impact on the Net "as we know it", represent the main reason why the debate has been so heated worldwide.

The second of the four final rulings of the judgment stated that, according to Article 4, §1(a)[10] of Directive 95/46/EC[11] (the "*Data protection framework directive*"[12]), the processing of personal data by a search engine operator referred to the territory of a Member State if that operator had, in that territory, a branch or subsidiary promoting and selling advertising space through an activity orientated towards the people living in that State[13].

---

jsf?language=en&jur=C,T,F&num=C-362/14&td=ALL last visited on 30 June 2016]

8 See MAYER-SCHÖNBERGER, 2009, p.169; ROSEN, 2012, p.88; PEGUERA, 2015, p.325; SARTOR, 2016, p.72.

9 On Internet jurisdiction, see GEIST, M.A., Is there a there there: toward greater certainty for Internet jurisdiction, in **Berkeley Technology Law Journal**, 2001, p.1345.

10 According to Article 4, §1(a), Directive 95/46/EC, each Member State shall apply its national provisions where «**the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State**».

11 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.

12 Article 94, §1, of Regulation (EU) 2016/679 of 27 April 2016 has repealed Directive 95/46/EC, with effect from 25 May 2018.

13 CJEU, case C-131/12 cited, ruling n. 2: «**Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell**

Even though it had not been proven that Google Spain was carrying either an indexing activity or a storage activity, the Court, recalling a previous case[14] on a different matter (intellectual property), concluded that the promotion and sale of advertising space run by Google Spain was so closely linked to the main commercial activity of Google Inc. as a search engine[15] that it would have been unacceptable for the processing of personal data by Google to be excluded from the scope of Directive 95/46/CE and, consequently, from the obligations and guarantees laid down by it. A different reasoning would have affected, according to the Court, the protection of fundamental rights and freedoms of individuals[16].

The point is that Article 4(1)(a) of Directive 95/46/EC, enacted more than twenty years ago, when the Internet was something quite different from what it is today, could not foresee the current issues[17]. Its wording leaves room for different interpretations. The notion of establishment, on the other hand, stays in Regulation

---

advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State»; see also §§45-60 of the judgment.

14 CJEU 12 July 2011, case C-324/09 ("*L'Oréal and Others*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-324/09&td=ALL last visited on 30 June 2016]: the Court highlighted the relevance of the jurisdiction rules on the effectiveness («*effet utile*») of EU law (§§62-63).

15 CJEU case C-131/12 cited, §56: «**the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed**».

16 CJEU, case C-131/12 cited, §58: «**it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure**».

17 On article 4 of the Directive 95/46/EC, see MOEREL, L., The long arm of EU data protection law: does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?, in **International Data Privacy Law** 2011, p.28; MOEREL, L., Back to basics: when does EU data protection law apply?, in **International Data Privacy Law** 2011, p.92; COLONNA, L., Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?, in **International Data Privacy Law** 2014, p.203.

(EU) 2016/679 (the new "*General data protection regulation*")[18], even though the wording of the equivalent article is a bit different[19].

The development of the Net, the social interests and the economic dynamics involved nowadays make it harder to define an unambiguous meaning of «*establishment*». Neither Directive 95/46/EC nor Regulation (EU) 2016/679, in the articles devoted to definitions (Article 2 and Article 4, respectively), clarify what an establishment is for their purposes, even though Article 4, §1(16) of Regulation (EU) 2016/679 defines what a «*main establishment*» is.

Recitals, the introductory notes to EU directives and regulations, can help, but they do not solve the issue. Recital 19 of Directive 95/46/EC[20], after stating that the notion of establishment requires an effective and real activity through "*stable arrangements*", acknowledges that the legal form of the establishment itself is not a determining factor. In the same terms, Recital 22 of Regulation (EU) 2016/679 stresses the relevance of a real and effective exercise of an activity[21].

18 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; on the same date the EU adopted Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

19 Article 3, §1, Regulation (EU) 2016/679: «**This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not**».

20 Directive 95/46/EC, Recital 19: «**Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities**».

21 Regulation (EU) 2016/679, Recital 22: «**Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should**

What really matters, in the end, is that national and EU rules, and the obligations imposed therein, are not circumvented by the organizational choices made by the controller. That is why the CJEU found, in *Google Spain*, that a branch or subsidiary promoting and selling advertising space offered by the search engine and orientating its activity towards the people living, is subject to Article 4(1)(a) of Directive 95/46/EC.

In this context the CJEU, in a more recent, but less famous, case, *Weltimmo*[22], confirmed and expanded its approach aimed to broaden the scope of Article 4(1)(a) of Directive 95/46/EC. The case did not concern an extra-EU dispute, but an intra-EU one. A company registered in Slovakia was running a real estate website concerning Hungarian properties. In doing so, it applied questionable commercial practices. The Hungarian data protection authority stepped in, imposing a fine to the company, which challenged the decision for lack of jurisdiction.

The CJEU found that Article 4(1)(a) of Directive 95/46/EC applied, pointing out the criteria to be applied, with some interesting specifications: the extra-territorial activity could be «*even a minimal one*»; the direction towards the foreign Member State could be inferred not only by the territorial position of the goods, but also by the language used; the establishment required not necessarily a branch or subsidiary, being sufficient a «*representative*» dealing with the administrative and judicial proceedings concerning the interests of the controller[23]. The criteria of the judgment share both

---

be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect».

22 CJEU, 1 October 2015, case C-230/14 ("*Weltimmo*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-230/14&td=ALL, last visited on 30 June 2016].

23 CJEU, case C-230/14 cited, ruling n. 1: «**Article 4(1)(a) of Directive 95/46/EC … must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises,**

the goal to expand jurisdiction and the indefiniteness of the wording. The latter reinforces the former. Again, the objective is to limit the chances for companies, whatever their nationality, to bypass EU law on data protection, playing with jurisdiction. While profoundly different to many extents, *Google Spain* and *Weltimmo* have the same target: private companies. Big, and American, in the former. Small, and European, in the latter.

Schrems is different. The preliminary ruling before the Court involved the Irish Data Protection Commissioner for its refusal to investigate a complaint about the transfer of personal data to the United States by Facebook (from its servers in Europe to its servers in the US). Facebook was not the real target: the US surveillance system was. The issue concerned the validity of Decision 2000/520/EC on the *Safe Harbor* scheme[24], regarding transatlantic data sharing for commercial purposes[25]. Mr Schrems contended that the United States were not ensuring an adequate level of protection of his personal data, considering the law and the practices in force in that country. The Court concluded that Decision 2000/520/EC was invalid.

---

through stable arrangements in the territory of that Member State, a real and effective activity - even a minimal one - in the context of which that processing is carried out. In order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned.»

24 On the *Safe Harbor* scheme, see also Commission Staff Working Document, 20 October 2004, SEC (2004) 1323 *[http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf*, last visited on 30 June 2016]; Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU *[http://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF,* last visited on 30 June 2016*]*.

25 See BROWN, 2015, p.23.

The decision is relevant not only for the balance struck between data protection on one side and security[26] and commercial interests on the other side, but also for a jurisdictional issue. It was stated that, notwithstanding Decision 2000/520/EC and notwithstanding the negotiations between the EU and the US, a supervisory authority of a Member State could examine the claim of an individual concerning the protection of his personal data under the *Safe Harbor* scheme[27]. That would mean that each Data Protection Authority in the EU could challenge the regulations of each country involved in the *Safe Harbor* scheme, and their implementation.

It is evident from the case law above that the CJEU has been pursuing some precise and intertwined goals: expand EU jurisdiction in Internet related cases; strengthen EU role in the international arena; affirm EU values against US values; provide a deeper protection to EU citizens. Is it something new? Not really, if we recall *LICRA v. Yahoo*[28] at the turn of this century. Different times,

26 On the relationship between privacy and security, SOLOVE, D.J., **Nothing to hide**: the false tradeoff between privacy and security, Yale University Press 2011, p.21.

27 CJEU, case C-362/14 cited, ruling n. 1: «Article 25(6) of Directive 95/46/EC …, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC … on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, …, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection».

28 The case concerned the sale of Nazi memorabilia through the Yahoo online auction service, following the complaints by the *Ligue contre le racisme et l'antisémitisme* (LICRA) and by the *Union des* étudiants *juifs de France* (UEJF). A French court, the *Tribunal de Grande Instance de Paris*, ruled that Yahoo had to respect French law (which prohibited the display and the sale of such memorabilia) even though the website was located in the US. See Tribunal de Grande Instance de Paris, **ordonnance 22 Mai 2000** *[http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=175,* last visited on 30 June 2016*]*, *ordonnance 11 Août 2000* [http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=219, last visited on 30 June 2016] and *ordonnance 22 November 2000 [http://www.legalis.net/spip.php?page=jurisprudence-*

different courts, different issues, different big dot.com companies, but the main dispute was, even then, about jurisdiction. France, in the end, managed to have Yahoo comply with its requests.

It was not the CJEU then, but a French Court, applying French law and French values. The conflict, though, is similar, and, by the way, France is fighting again, this time against Google and within the framework of a CJEU decision. The *Commission Nationale de l'Informatique et des Libertés (CNIL)*, the French data protection authority, fined Google 100.000 euros for not removing "*right-to-be-forgotten*" requests from global search results. Google had deleted results from EU domains, like ".fr", but not from other domains, like (mainly) ".com". According to Google, delisting search results from all domains would limit the freedom of expression (beside determining more costs for Google itself). According to the CNIL, it is not so, as the Internet content is not removed. Moreover, Google contests the authority of CNIL to control the content that people can access outside France. As in *LICRA v. Yahoo*, one of the aspects faced concerns the fact that the Internet company can reasonably know whether the user is searching from France.

The recent Regulation (EU) 2016/679 deals with the territorial scope in Article 3[29]. As for controller or processors established in the Union, the Regulation will apply if the processing is «*in the context*» of their activities, regardless of where the processing

decision&id_article=217, last visited on 30 June 2016*]*.

29 Regulation (EU) 2016/679, Article 3 («*Territorial scope*»):
«1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law».

takes place. As for controller or processors not established in the Union, the Regulation will apply if the data subjects are in the Union, when the data processing relates to the offering of goods or services, or to the monitoring of individuals' behavior taking place within the EU. We will see the judicial interpretation, but chances are that, notwithstanding the different wording, the criteria and the goals of Directive 95/46/EC will be confirmed.

3 DATA PROTECTION SUPREMACY

The conflict of jurisdictions often hides a conflict of values. It was so at the turn of the century, in *LICRA v. Yahoo*, between France and Yahoo. It was so, recently, in *Google Spain*, between the European Union and Google. Free speech, and censorship, were involved in both cases. In the first case, the clashing interest was the protection of French people from a partial memory of Nazism. In the second case, the protection of EU individuals from a partial memory of themselves, through the "right to be forgotten".

The Court of Justice of the European Union, in *Google Spain*, not only identified and tried to (broadly) delimit the right to oblivion, but also affirmed the supremacy, as a rule, of the rights to privacy and data protection over the rights to free speech, information and enterprise[30]. While the final statement («*fundamental rights under Articles 7 and 8 of the Charter, … override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information*») can be interpreted more or less strictly, it is the discipline itself

30 CJEU, case C-131/12 cited, §§53, 66, 74, and ruling n. 4: «**As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question».**

sketched by the CJEU[31] and by the EU data protection bodies that shows the hierarchy of rights, and therefore, values.

Delisting requests are addressed by the individual (data subject) to the search engine operator (controller), that, considering the merits, may decide to delete the link (or links) to the webpages not allowing the right to be forgotten. Should this not happen, the data subject may ask the delisting of the search results to the competent administrative or judicial authority[32]. The webpage manager may not even know that a delisting request, concerning the contents provided, has been put forward, being therefore deprived of the chance to file a complaint.

The search engine operator must therefore carry out a complex legal assessment[33] concerning fundamental rights, without

31 The CJEU has often faced cases dealing with data protection; see, after *Google Spain*, beyond other cases otherwise cited in this article: CJEU, 17 July 2014, joined cases C-141/12 and C-372/12 ("*YS*"), on the right to access [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-141/12&td=ALL, last visited on 30 June 2016]; CJEU, 11 December 2014, Case C-212/13, ("*Ryneš*"), on the interpretation of the concept of "*purely personal or household activity*" [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-212/13&td=ALL, last visited on 30 June 2016]; CJEU, 16 April 2015, joined cases C-446/12 to C-449/12 ("*Willems*"), on the use of biometrics in passports and travel documents [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-446/12&td=ALL, last visited on 30 June 2016]; CJEU, 16 July 2015, case C-580/13 ("*Coty Germany*"), on banking secrecy [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-580/13&td=ALL, last visited on 30 June 2016]; CJEU 1 October 2015, CJEU, 16 July 2015, case C-615/13 ("*ClientEarth*"), on the concept of personal data and on the right to access [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-615/13&td=ALL, last visited on 30 June 2016]; case C-201/14 ("*Bara*"), on the transfers of personal data among administrative bodies [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-201/14&td=ALL, last visited on 30 June 2016].

32 CJEU, case C-131/12 cited, §77: «**Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly**».

33 The Article 29 Data Protection Working Party, trying to facilitate the search engines operators' activity, issued the «*Guidelines on the implementation of the Court of Justice*

being obligated to hear both parties. Besides, the structure and the wording of the decision express a clear favor for the deletion, that can be carried out even though the contents of the page linked are not violating any law[34]. The resulting hierarchy among fundamental rights and values may not be shared by other legal systems, and protecting European citizens' personal data outside the EU may not be so easy[35].

The data protection supremacy affirmed by the CJEU[36] is not just the outcome of a cultural clash. In *Digital Rights Ireland*[37], concerning the retention of data, generated or processed by the providers of electronic communications services, for purposes of prevention, investigation and prosecution of serious crimes, such as terrorism and organized crime, the Court declared invalid Directive 2006/24/EC ("*Data retention directive*")[38]. The Directive was challenged for its violation of Article 7 («*Respect for private and family life*»), Article 8 («*Protection of personal data*») and Article 11 («*Freedom of expression and information*») of the Charter of Fundamental Rights of the European Union (CFREU)[39].

---

of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/121» (26 November 2014) [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf, last visited on 30 June 2016].

34 CJEU, case C-131/12 cited, ruling n. 3: «**the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful**».

35 See ZHAO, B., MIFSUD BONNICI, 2016, p.128.

36 FINOCCHIARO, 2015, p.779.

37 CJEU 8 April 2014, joined cases C-293/12 and C-594-12 ("*Digital Rights Ireland*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-293/12&td=ALL, last visited on 30 June 2016].

38 See VAINIO, MIETTINEN, 2015, p.290.

39 CJEU, joined cases C-293/12 and C-594-12 cited, §23.

The amount and the quality of the data[40] to be retained by the communications providers allowed to heavily interfere with the privacy of personal communications[41]. The Court found the interference with Articles 7 and 8 of the Charter «*wide-ranging*» and «*particularly serious*»[42]. While Directive 2006/24/EC pursued an objective of general interest[43], the fight against terrorism and other major crimes, the Court affirmed that there was no proportionality of the interference, considering many factors. Persons whose data were retained might not have been linked, even remotely or indirectly, with serious crimes and the Directive did not provide for any exception, such as professional secrecy rules[44]. Moreover, Directive 2006/24/EC lacked of limits[45], procedural[46], subjective[47], spatial[48] and time[49] conditions, safeguards[50], and objective criteria[51]

40 CJEU, joined cases C-293/12 and C-594-12 cited, §26: the data mentioned by Articles 3 and 5 of the Directive 2006/24/CE «**make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place**»; the data «**also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period**».

41 CJEU, joined cases C-293/12 and C-594-12 cited, §27: «**Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them**».

42 CJEU, joined cases C-293/12 and C-594-12 cited, §37.

43 CJEU, joined cases C-293/12 and C-594-12 cited, §41.

44 CJEU, joined cases C-293/12 and C-594-12 cited, §58.

45 CJEU, joined cases C-293/12 and C-594-12 cited, §59.

46 CJEU, joined cases C-293/12 and C-594-12 cited, §61.

47 CJEU, joined cases C-293/12 and C-594-12 cited, §62.

48 CJEU, joined cases C-293/12 and C-594-12 cited, §68.

49 CJEU, joined cases C-293/12 and C-594-12 cited, §63.

50 CJEU, joined cases C-293/12 and C-594-12 cited, §66.

51 CJEU, joined cases C-293/12 and C-594-12 cited, §60: «**Directive 2006/24 simply**

for the action of the competent national authorities on the data retained. According to the Court, therefore, the extent of the interference with the fundamental rights of individuals was not counterbalanced by provisions ensuring its necessity[52].

This was the conclusion in a case involving EU public security. In *Schrems,* where the goal was to protect EU individuals' personal data against extra-EU surveillance, the CJEU applied the same principles. Still, the decision was partially unexpected, considering that the central issue was the *Safe Harbor* scheme, established 15 years earlier by Decision 2000/520/EC[53]. The increased concern for European personal data was expressly linked to Edward Snowden's revelations about the National Security Agency (NSA) and other United States intelligence services. The Court, citing, among others, *Digital rights Ireland* and *Google Spain*, reaffirmed the importance of Articles 7 and 8 of the CFREU[54], finding that the *Safe Harbor* scheme interfered with the data protection of EU citizens[55]. Decision 2000/520/EC did not contain any reference

---

refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law».

52 CJEU, joined cases C-293/12 and C-594-12 cited, §65: «Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary».

53 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce; see also Commission Staff Working Document, 20 October 2004, The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce [http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf, last visited on 30 June 2016]; Communication from the Commission to the European Parliament and the Council, 27 November 2013, on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU [http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf, last visited on 30 June 2016]

54 CJEU, case C-362/14 cited, §39.

55 CJEU, case C-362/14 cited, §87: «**Decision 2000/520 … enables interference, founded on national security and public interest requirements or on domestic legislation of**

to US rules aimed at restraining the privacy intrusions[56], did not impose minimum safeguards against abuses and mistakes[57] and did not provide individuals with legal remedies to pursue in order to challenge the personal data processing[58]. Security matters and commercial interests had to yield to privacy and personal data rights if an adequate level of protection was not ensured.

The European Court of Human Rights, in *Zakharov*[59], followed the same pattern adopted by the CJEU in *Digital rights Ireland* and in *Schrems*, making personal data and privacy prevail over security matters. In *Zakharov,* the issue concerned the Russian system of secret interception of mobile telephone communications and the violation of Article 8 of the European Convention of Human Rights ("*Right to respect for private and family life*"). First of all the ECtHR found that the interference with Article 8 was justified by the «*mere existence of the contested legislation*» and that the applicant was entitled to claim to be a victim of the violation of the Convention even though he could not prove the subjection to actual surveillance[60]. Then the Court recalled the general principles justifying interferences with Article 8, §2 of the ECHR: the interference must be in accordance with the law, pursue a legitimate aim and be necessary to achieve that aim in a democratic society[61].

The Court, analyzing in depth the Russian law, concluded that it neither met the «quality of the law requirement» nor kept

---

the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States», not being relevant «whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference».

56 CJEU, case C-362/14 cited, §88.

57 CJEU, case C-362/14 cited, §91.

58 CJEU, case C-362/14 cited, §95.

59 ECtHR, Grand Chamber, 4 December 2015, application no.47143/06 ("*Zakharov*") [http://hudoc.echr.coe.int/eng?i=001-159324, last visited on 30 June 2016].

60 ECtHR, application no.47143/06 cited, §179.

61 ECtHR, application no.47143/06 cited, §227.

the interference to what is «*necessary in a democratic society*»[62]. The Court stressed, in fact, the lack of «*adequate and effective guarantees*», the «*risk of abuse*» of Russian secret surveillance system, the unsatisfying authorization procedures and interception supervisions rules and the automatic storage of «*clearly irrelevant data*»[63].

The same pattern was followed by the ECtHR in *Szabó and Vissy*[64]. The applicants, members of a non-governmental "watchdog" organization, complained, under Article 8 of the ECHR, for «*unjustified and disproportionately intrusive*» surveillance measures introduced by Hungarian legislation. The abuse, though, was allegedly only potential[65]. The Court, considering the peculiarities of secret surveillance, and recalling its own case law, including *Zakharov*, declared the complaint, and the resulting *in abstracto* review, admissible[66].

On the merits, the Court started from the safeguards criteria pointed out in its case law: the nature of offences justifying interceptions; the categories of people subjected to surveillance; duration limits; procedural rules; precaution in communicating collected data to other agencies and parties; rules on the erasure of collected data[67]. The Court, using the same line of reasoning adopted in *Zakharov*, therefore concluded that Article 8 of the ECHR had been violated, considering the extent of the scope of the surveillance, the overarching role of the executive, the lack of remedial measures, the limited, if any, evaluation of the strict necessity[68].

62 ECtHR, application no.47143/06 cited, §304.

63 ECtHR, application no.47143/06 cited, §302.

64 ECtHR, Fourth Section, 12 January 2016, application no.37138/14 ("*Szabó and Vissy*") [http://hudoc.echr.coe.int/eng?i=001-160020, last visited on 30 June 2016]; the judgment has become final on 6 June 2016.

65 ECtHR, application no.37138/14 cited, §26: «**They submitted that the legal framework was prone to abuse, notably for want of judicial control**».

66 ECtHR, application no.37138/14 cited, §§32-41.

67 ECtHR, application no.37138/14 cited, §56.

68 ECtHR, application no.37138/14 cited, §89: «**Given that the scope of the measures**

Even in an era of terrorism, the protection of individuals' personal data from secret public surveillance is particularly strong[69]. The European Court of Human Rights and the Court of Justice of the European Union apparently share the same concerns and the same vision, making commentators wondering whether the massive monitoring of electronic communications itself has simply been outlawed in Europe[70].

Still, the level of protection of personal data and individuals' privacy is not always so high, and sometimes it has to yield.

In *Bărbulescu*[71], a case not involving public surveillance against crime and terrorism, but private surveillance on the workplace, the ECtHR, apparently overruling its own case law, did not find any violation of Article 8 of the ECHR in a questionable behavior of an employer, who had not only monitored the employee's communications, but also disclosed his private communications to his colleagues.

The employer had fired an employee on the basis of evidence collected through the monitoring of electronic communications in the workplace. The Court, after recalling its own case law on telephone and Internet surveillance[72], stated that there had been

---

could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention».

69 See ZALNIERIUTE, 2015, p.99.

70 ST. VINCENT, S., **Did the European Court of Human Rights just outlaw "massive monitoring of communications"**, Center for Democracy and Technology, 13 January 2016 [https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/, last visited on 30 June 2016].

71 ECtHR, Fourth Section, 12 January 2016, application no.61496/08 ("*Bărbulescu*") [http://hudoc.echr.coe.int/eng?i=001-159906, last visited on 30 June 2016]; the judgment was referred to the Grand Chamber on 6 June 2016.

72 In particular, ECtHR, 25 June 1997, application no.20605/92 ("*Halford")* [http://hudoc.echr.coe.int/eng?i=001-58039, last visited on 30 June 2016]; ECtHR, 16 February 2000, application no.27798/95 ("*Amann")* [http://hudoc.echr.coe.int/eng?i=001-58497, last visited on 30 June 2016]; ECtHR, 3 April 2007, application

no violation of Article 8 of the ECHR. While the Court underlined the differences between this case and the others, the decision is nonetheless not persuasive.

On one side, it is true that in *Bărbulescu* the internal regulations of the employer's firm explicitly prohibited employees from using company electronic resources for personal purposes, but there was no solid evidence that the employee had been given prior notice that his communications might have been monitored, accessed and disclosed. And the Court, oddly enough, did not seem particularly interested in that relevant aspect.

On the other side, considering that the employee was not challenging some personal use of the company electronic resources by the employee, making the transcript of the private communications available to his colleagues was really neither necessary nor justified.

The ECtHR found that the employer was entitled to verify that the employees were «*completing their professional tasks during working hours*» and that the employer's monitoring was, in the case, «*limited in scope and proportionate*»[73], concluding that the balance struck by the domestic authorities was «*fair*»[74]. But the Court did not substantially face the other two issues: the evidence of the prior notice and the unnecessary disclosure of the contents of private communications to other parties. Not surprisingly, the judgment came with a dissenting opinion[75], that put things in (a different?) perspective. The dissenting judge, after an in-depth analysis of workplace privacy and its rules, highlighted the relevance of employees' necessary awareness of Internet workplace policy in force[76] and stressed the principles of necessity and proportionality

---

no.62617/00 ("*Copland*") [http://hudoc.echr.coe.int/eng?i=001-79996, last visited on 30 June 2016]; ECtHR, 26 July 2007, application no.64209/01 ("*Peev*")[http://hudoc.echr.coe.int/eng?i=001-81914, last visited on 30 June 2016].

73 ECtHR, application no.61496/08 cited, §60.

74 ECtHR, application no.61496/08 cited, §62.

75 ECtHR, application no.61496/08 cited, partly dissenting opinion of Judge Pinto de Albuquerque.

76 ECtHR, application no.61496/08 cited, partly dissenting opinion of Judge Pinto de

in its enforcement[77]. In particular, the dissenting opinion focused on the lack of evidence that the applicant had been given notice of the company Internet surveillance policy[78] and on the disclosure of the transcripts of the personal messages, made available to the applicant's colleagues instead of being restricted to the disciplinary proceedings[79]. The employer's interference with the employee's privacy was therefore not justified and, anyway, it went «*far beyond what was necessary*»[80].

The (private) Internet surveillance, in *Bărbulescu*, enjoyed a far broader leeway than the (public) electronic communications surveillance systems under scrutiny in *Zakharov* and in *Szabó and Vissy*. Interestingly, *Bărbulescu* and *Szabó and Vissy* were decided by the same Section of the ECtHR on the same day, so it is not a matter of different sensitivity from different judges. Not surprisingly, Bărbulescu was referred to the Grand Chamber, while *Szabó and Vissy* was not, becoming final.

4 INTERNET SERVICE PROVIDERS BETWEEN LIABILITY AND ROLE REINTERPRETATION

The role of Internet service providers (ISPs) in cyberlaw and in the growth of the Net itself has always been pivotal[81]. It is not just a matter of private companies liability. The discipline of ISPs, or Internet intermediaries, concerns economy, censorship, balance

---

Albuquerque, §12: «**before a monitoring policy is put in place, employees must be aware of the purposes, scope, technical means and time schedule of such monitoring**».

77 ECtHR, application no.61496/08 cited, partly dissenting opinion of Judge Pinto de Albuquerque, §13.

78 ECtHR, application no.61496/08 cited, partly dissenting opinion of Judge Pinto de Albuquerque, §§16-17.

79 ECtHR, application no.61496/08 cited, partly dissenting opinion of Judge Pinto de Albuquerque, §20.

80 ECtHR, application no.61496/08 cited, partly dissenting opinion of Judge Pinto de Albuquerque, §20.

81 On the role of ISPs and their liability, see CARLYLE, 2000, p.331; SARTOR, DE AZEVEDO CUNHA, 2010, p. 356; VAN EECKE, 2011, p.1455; LEITER, 2012, p.169.

among fundamental rights and freedoms[82], public control and much more. The laws affecting ISPs affect the Internet.

Articles 12-15 of Directive 2000/31/EC[83] ("*E-commerce Directive*") are still the norms to refer to[84], as for ISPs role and liability, even though they would need an update, considering how much their activity has changed in these years, and a relocation, considering that their role goes far beyond e-commerce. Still, the recent General Data Protection Regulation has not intervened, confirming and recalling the provisions of Directive 2000/31/EC[85].

It is not surprising, therefore, that the case law of the Court of Justice of the European Union on the topic, crucial in order to understand ISPs' role, is particularly wide and varied. Setting aside, for the time being, the most dated decisions, *Google Spain* is in the spotlight again. The CJEU entrusted to Google the role of adjudicator (if not of judge), as for the right to be forgotten, and enforcer, as for the removal of "illicit" links.

When people turn to Google (or other search engine operators) in order to have their right to be forgotten acknowledged and implemented, it is up to Google to decide whether their request is deserving to be accepted or not. It might not be an easy call, as many factors influence the final choice: delicate legal issues, involving fundamental rights and freedoms, arise.

---

82 See Center for Democracy and Technology, **Intermediary liability protecting Internet platforms for expression and innovation,** April 2010 *[https://cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf,* last visited on 30 June 2016*];* Center for Democracy and Technology, **Shielding the messengers**: protecting platforms for expression and innovation, December 2012 [https://cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf, last visited on 30 June 2016].

83 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*").

84 On the *E-commerce Directive* and the EU and national case law concerning ISPs', see VAN EECKE, 2011, p.1457.

85 Regulation (EU) 2016/679, Article 2, §4: «**This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive**»; see also Recital 21.

Still, the CJEU thought that Google had to play this crucial role: framing the right to be forgotten under Article 12(b) and Article 14, §1(a), of Directive 95/46/EC[86], the Court imposed the role of adjudicator on Google[87]. Moreover, the Court maintained that even when the right to be forgotten was not involved, but the results of the search "appeared" to be inadequate, irrelevant or excessive, Google had to erase, on request, those results[88]. Google had found those results, but it had not created them. Still, it had to be the enforcer, as delisting the results, without any deletion, was deemed sufficient to avoid (or stop) damages to the applicant.

Google did not want that dual role (adjudicator and enforcer), both for practical reasons (more activities, more cost) and ideal reasons (being adjudicator and enforcer meant to be censor as well), but accepted it to avoid liability. Liability is the tool or, better, the weapon, used from public powers against Internet intermediaries: censorship is "outsourced"[89].

That happened in the *Delfi case* too, a highly controversial case brought to the European Court of Human Rights twice: to the

86 See, now, Article 17 of Regulation (EU) 2016/679, entitled «**Right to erasure ("right to be forgotten")**».

87 CJEU, case C-131/12 cited, §77: «**Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question**».

88 CJEU, case C-131/12 cited, §94: «**Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased**».

89 MOROZOV, 2011, p.101: «**Being able to force companies to police the Web according to a set of some broad guidelines is a dream come true for any Government. It's the companies who incur all the costs, it's the companies who do the dirty work, and it's the companies who do the dirty work, and it's the companies who eventually get blamed by the users**».

First Section in 2013[90] and to the Grand Chamber in 2015[91]. Delfi was an Estonian Internet news portal operating in Baltic countries (Estonia, Latvia and Lithuania). Delfi published news and allowed reader to comment. The commenters may have been anonymous, and most of them usually were, writing under pseudonyms. Delfi adopted a policy on public participation ("Rules of comment"), a system of automatic deletion of comments, based on certain stems of obscene words, and a notify-and-take-down system.

An article on the portal, concerning public transports, ignited online debate through a number of comments, some of which contained threats and offensive language against a member of the supervisory board of the company involved in the article. Delfi was deemed liable by domestic courts for third-party comments, notwithstanding the liability exemptions of Directive 2000/31/EC, the removal of the comments as soon as the individual complained, and the acknowledgment that the article in itself was balanced. Delfi went to the ECtHR stating that its freedom of expression had been violated, breaching Article 10 of the European Convention for Human Rights.

Neither the First Section nor the Grand Chamber of the ECtHR found any violation of Article 10.

The central point concerned the qualification of Delfi as a technical, neutral, service provider, as Delfi maintained, or as an active service provider, as the Estonian government maintained. The Court agreed with the Estonian government: hence, the liability of the company. The distinction between "neutral" ISP and "active" ISP is not clear in EU legislation, as Directive 2000/31/EC does not explicitly distinguish the two. The distinction is based more on recitals (in particular, Recital 42[92]) of the Directive than on its

90 ECtHR, First Section, 10 October 2013, application no.64659/09 ("*Delfi*") [http://hudoc.echr.coe.int/eng?i=001-126635, last visited on 30 June 2016].

91 ECtHR, Grand Chamber, 16 June 2015, application no.64659/09 ("*Delfi*") [http://hudoc.echr.coe.int/eng?i=001-155105, last visited on 30 June 2016].

92 Directive 2000/31/EC, Recital 42: «**The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or**

articles. The Court of Justice of the European Union has faced the issue many times (and the ECtHR, in *Delfi*, cited the CJEU case law[93]), but, considering the different activities of ISPs, there is not an uniform interpretation of what "active" means.

The Grand Chamber of the ECtHR started by saying that Delfi was a large, commercial, Internet news portal[94], that the case did not «*concern other fora on the Internet*»[95], and that an Internet portal operating in media publications was something different than a publisher of printed media[96]. Then, speaking of the liability of the authors of the comments, the Grand Chamber stressed the role of anonymity on the Internet (promoting the free flow of ideas and information[97]), and its different degrees (from complete to traceable[98]), before laying the risks of the contents posted anonymously on news portal like Delfi.

---

temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored».

93 Other than *Google Spain*: CJEU, 23 March 2010, case C-236/08 to C-238/08 ("*Google France*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-236/08&td=ALL, last visited on 30 June 2016]; CJEU, case C-324/09 cited; CJEU, 24 November 2011, case C-70/10 ("*Scarlet Extended*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-70/10&td=ALL, last visited on 30 June 2016]; CJEU, 16 February 2012, case C-360/10 ("*SABAM*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-360/10&td=ALL, last visited on 30 June 2016]; CJEU, 11 September 2014, case C-291/13 ("*Papasavvas*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-291/13&td=ALL, last visited on 30 June 2016].

94 ECtHR, Grand Chamber, application no.64659/09 cited, §115.

95 ECtHR, Grand Chamber, application no.64659/09 cited, §116: «**Accordingly, the case does not concern other fora on the Internet where third-party comments can be disseminated, for example an Internet discussion forum or a bulletin board where users can freely set out their ideas on any topics without the discussion being channelled by any input from the forum's manager; or a social media platform where the platform provider does not offer any content and where the content provider may be a private person running the website or a blog as a hobby».**

96 ECtHR, Grand Chamber, application no.64659/09 cited, §126.

97 ECtHR, Grand Chamber, application no.64659/09 cited, §147.

98 ECtHR, Grand Chamber, application no.64659/09 cited, §148.

The Grand Chamber conclusion was that Delfi was liable and that the obligation to take effective measures to avoid or limit hate or violent speech could «*by no means be equated to "private censorship"*»[99], helping to protect, instead, the potential victims[100]. In the end, ISPs, or at least certain categories of Internet intermediaries (income from the online activity was a relevant criterion), could be requested, in order to avoid liability, to remove «*clearly unlawful comments without delay, even without notice from the alleged victim or from third parties*». One can agree or not with the statement of the Court, but it is something quite different from the provisions of Directive 2000/31/EC.

The ECtHR, in a more recent case, *MTE and Index.hu*[101], found that there had been a violation of Article 10 of the ECHR when two ISPs (a self-regulatory body of Internet content providers and an Internet news portal) were deemed liable for offensive and vulgar comments posted on their websites. At a first glance, it looked like there was a conflict with *Delfi*. It was the Court itself that explained (or tried to) why it was not so, building its reasoning on the quality of the incriminated speech. In *MTE and Index.hu* the comments were offensive and vulgar, but, unlike in *Delfi*, they did not constitute hate speech or incitement to violence, and so they did not amount to «*clearly unlawful speech*»[102]. The Court seems quite worried to avoid any broad liability exemption, considering it a risk for the quality of public speech on the Internet[103].

99 ECtHR, Grand Chamber, application no.64659/09 cited, §157.

100 ECtHR, Grand Chamber, application no.64659/09 cited, §158. «**The Court attaches weight to the consideration that the ability of a potential victim of hate speech to continuously monitor the Internet is more limited than the ability of a large commercial Internet news portal to prevent or rapidly remove such comments**».

101 ECtHR, Fourth Section, 2 February 2016, application no.22947/13 ("*MTE and Index.hu*") [http://hudoc.echr.coe.int/eng?i=001-160314, last visited on 30 June 2016]; the judgment has become final on 2 May 2016.

102 ECtHR, Fourth Section, application no.22947/13 cited, §64: «**Furthermore, while the second applicant is the owner of a large media outlet which must be regarded as having economic interests, the first applicant is a non-profit self-regulatory association of Internet service providers, with no known such interests**».

103 ECtHR, Fourth Section, application no.22947/13 cited, concurring opinion of judge

The borders did not seem so sharp, though, and the ECtHR decision leaves some issues open for more discussion. The most relevant issue refers to the implicit necessity of general monitoring[104] for ISPs in order to avoid consequences. There are no mechanisms that may automatically delete all unlawful comments and the ones that can at least help in doing so may have censorship effects. That leads, if an ISPs wants to be on the safe side, to the need to pre-moderate the comments, which would affect the current model of Internet public discussion spaces. And even if the moderation occurs after the publishing (which leaves open the door for liability, anyway), the legal assessment from the ISPs may differ from a following official judgment, as the "illegality" depends on circumstances and interpretation[105]. Not surprisingly, this kind of issues justified the liability exemptions introduced by the E-commerce Directive, still in force.

The CJEU recently provided a new perspective in the case McFadden[106], concerning the copyright infringement liability, for the use by a third party of the wireless local area network, of the owner of a store who gave free access to the WLAN. The Court, considering that McFadden should have been considered as an ISP, according to Directive 2000/31/EC, excluded his liability for the infringement by an anonymous user of the network. On the other hand, the Court said that the person harmed by the infringement may claim injunctive relief against the continuation of that infringement, suggesting, in order to avoid liability, the adoption of a password protected system requiring the identification of the user. In other

---

Kūris, §3: «**this judgment should in no way be employed by Internet providers, in particular those who benefit financially from the dissemination of comments, whatever their contents, to shield themselves from their own liability, alternative or complementary to that of those persons who post degrading comments, for failing to take appropriate measures against these envenoming statements».**

104 VAN EECKE, 2011, p. 1486.

105 VAN EECKE, 2011, p. 1465.

106 CJEU 15 September 2016, case C-484/14 ("*McFadden*") [http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-484/14&td=ALL, last visited on 26 October 2016]

words, the end of anonymity of the whole system after the first violation. What started with an (illusory) statement of a principle, the exclusion of liability for ISPs, ended in rules, conditions and constraints that are likely to lead online intermediaries to shape a different Internet, based on decentralized control and identifiable users.

5 CONCLUSIONS

The European Union has not gone insane. Its strategy aims to affirm its values, through different paths: jurisdiction expansion, data protection (over)emphasizing, ISPs role reinterpretation. The expansion of the jurisdiction is something natural for political organizations and it is not limited to the Net. Though, the Internet arena offers daily chances to stress (and stretch) it. The reinterpretation of the role of ISPs, considering the time passed since Directive 2000/31/EC, is something to be faced. Still, it would be better to act through legislation, and not case law. But the relevance of data protection is the most peculiar profile in the EU approach.

Data protection has moved other sides of privacy (the right to be let alone; anonymity, confidentiality of communications, the right to self-determination) to the background, limiting, at the same time, other fundamental rights (freedom of expression; freedom of information; freedom to conduct a business).

What is at stake is the regulation and the control of the Net and the main counterpart is the US, at times forgetting other about 170 other countries. The control of Net, through "collateral censorship"[107] and induced traceable anonymity, is facilitated by the relationship with ISPs, shaped by ongoing threatening, bargaining and negotiating, liability rules and "recruitment".

There is nothing really new, on the other hand. At the turn of the century, the law of the Internet was dealing with the Nazi-Yahoo case, with the Safe-Harbor negotiations, and with the E-commerce Directive: jurisdiction, data protection, ISPs liability. After more

107 ECtHR, Grand Chamber, application no.64659/09 cited, joint dissenting opinion of judges Sajó and Tsotsoria, §I.

than 15 years the issues are still open. The real change has been in the EU approach, more aggressive, challenging and self-confident, but agreed-upon solutions, in the international context, are far from being found.

The EU is aware that a balance must be struck among the different rights and interests involved. According to Article 85, §1 of the Regulation (EU) 2016/679, «*Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression*»[108]. It is true that Court of Justice of the European Union will be able to step in, but leaving the difficult task to the Member States is going to open other issues, first of all law differences and individuals discrimination, on fundamental rights, across Europe.

REFERENCES

BROWN, Ian. The feasibility of transatlantic privacy-protective standards for surveillance. In **International Journal of Law and Information Technology** , v. 23, n. 1, pp. 23-40, 2015.

CARLYLE, Paul. Legal regulation of telecommunications: the impact on Internet services. In EDWARDS, Lilian; WAELDE Charlotte (eds.). **Law & the Internet**: a framework for electronic commerce. Oxford – Portland: Hart Publishing, pp. 331-342, 2000.

CHARLESWORTH, Andrew. Data privacy in Cyberspace: not national vs. international but commercial vs. individual. In EDWARDS, Lilian;

108 See also Recital 4 of the Regulation (EU) 2016/679: «**The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity**»; see also Recital 153.

WAELDE Charlotte (eds.). **Law & the Internet**: a framework for electronic commerce. Oxford – Portland: Hart Publishing, pp. 79-122, 2000.

FINOCCHIARO, Giusella. La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems. In **Diritto dell'informazione e dell'informatica,** pp. 779-799, 2015.

LARSON, Robert, G.. Forgetting the First Amendment: how obscurity-based privacy and a right to be forgotten are incompatible with free speech**.** In **Communication Law and Policy**, v. 18, n. 1**,** pp. 91-120, 2013.

LEITER, Brian. Cleaning cyber-cesspools: Google and free speech. In LEVMORE, Saul; NUSSBAUM, Martha, C. (eds). **The offensive Internet**: speech, privacy and reputation, Cambridge – London: Harvard University Press pp. 155-173, 2012.

LESSIG, Lawrence. **Code**. Version 2.0. New York: Basic Books, 2006.

MAYER, Franz, C.. Europe and the Internet: the old world and the new medium. In: **European Journal of International Law**, v. 11, n. 1, pp. 149-169, 2000.

MAYER-SCHÖNBERGER, Viktor. **Delete**: the virtue of forgetting in the digital age, Princeton and Oxford: Princeton University Press, 2009.

MOROZOV, Evgeny. **The Net delusion**: the dark side of Internet freedom. New York: Public Affairs, 2011.

PEGUERA, Miquel. In the aftermath of Google Spain: how the "right to be forgotten" is being shaped in Spain by courts and the Data Protection Authority**.** In: **International Journal of Law and Information Technology**, v. 23, n. 4, pp. 325-347, 2015.

ROSEN, Jeffrey. The right to be forgotten**.** In **Stanford Law Review Online,** v. 64, pp. 88-92, 2012.

SARTOR, Giovanni. The right to be forgotten: balancing interests in the flux of time. In: **International Journal of Law and Information Technology**, v. 24, n. 1, pp. 72-98, 2016.

SARTOR, Giovanni; DE AZEVEDO CUNHA, Mario Viola. The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents. In: **International Journal**

of Law and Information Technology, v. 18, n. 4, pp. 356-378, 2010.

SOLOVE, Daniel, J.. **The future of reputation**: gossip, rumor, and privacy on the Internet. New Haven – London: Yale University Press 2007.

SOLOVE, Daniel, J.. Speech, privacy and reputation on the Internet. In LEVMORE, Saul; NUSSBAUM, Martha, C. (eds.). **The offensive Internet**: speech, privacy and reputation, Cambridge – London: Harvard University Press pp. 15-30, 2012.

ST. VINCENT, Sarah. Did the European Court of Human Rights just outlaw "massive monitoring of communications"?, **Center for Democracy and Technology**, 13 January 2016 [https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/, last visited on 30 June 2016].

STONE, Geoffrey, R.. Privacy, the First Amendment, and the Internet. In LEVMORE, Saul; NUSSBAUM, Martha, C. (eds). **The offensive Internet**: speech, privacy and reputation, Cambridge – London: Harvard University Press pp. 174-194, 2012.

VAINIO, Niklas; MIETTINEN, Samuli. Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States. In: **International Journal of Law and Information Technology**, v. 23, n. 3 , pp. 290-309, 2015.

VAN EECKE, Patrick. Online service providers and liability: a plea for a balanced approach. In: **Common Market Law Review**, 2011, v. 48, n. 5, p. 1455-1502, 2011.

ZALNIERIUTE, Monika. An international constitutional moment for data privacy in the times of mass-surveillance. In: **International Journal of Law and Information Technology**, v. 23, n. 2, pp. 99-133, 2015.

ZHAO, Bo; MIFSUD BONNICI, G.P. Jeanne. Protecting EU citizens' personal data in China: a reality or a fantasy**.** In: **International Journal of Law and Information Technology**, v.24, n. 2, pp. 128-150, 2016.

ZITTRAIN, Jonathan. **The future of the Internet and how to stop it**. New Haven – London: Yale University Press, 2008.