EUI Working Papers

LAW 2012/24
DEPARTMENT OF LAW

PROVIDERS' LIABILITIES IN THE NEW EU DATA PROTECTION REGULATION: A THREAT TO INTERNET FREEDOMS?

Giovanni Sartor

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE

DEPARTMENT OF LAW

Providers' Liabilities in the New EU Data Protection Regulation: A threat to Internet freedoms?

GIOVANNI SARTOR

EUI Working Paper **LAW** 2012/24

ISSN 1725-6739

Printed in Italy
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Abstract

In this paper I shall consider certain aspects of the Proposal for a Data Protection Regulation recently advanced by the EU Commission, which is meant to substitute the existing Data Protection Directive as well as the national laws implementing it. In particular I shall examine how the Regulation addresses host providers' liabilities and duties with regard to user-generated content. For this purpose, I shall first highlight some developments in web and cloud services, then I shall consider how web hosting is currently regulated, and finally I shall critically assess the novelties brought about by the Regulation.

Keywords

Data protection, user-generated data, host-provider, liability, e-commerce

Author Contact Details

Giovanni Sartor,

European University Institute,

Villa Schifanoia,

Via Boccaccio 121,

Florence.

Email: giovanni.sartor@eui.eu

PROVIDERS' LIABILITIES IN THE NEW EU DATA PROTECTION REGULATION: A THREAT TO INTERNET FREEDOMS?

*Giovanni Sartor**

1. The User-Generated Internet and the Cloud

As data are moving into the web and over the clouds, hosting is becoming ubiquitous, polymorphous and interconnected.

On the one hand, in the user-generated web, not only we are store our web-pages in the servers of host providers, but we produce and distribute content in multiple ways: we upload our texts, our music, our pictures on various on-line repositories, making them available to a worldwide audiences; we build our public images on social network, where we disclose aspects of our personalities, interact with others, advertise our social and work capacities, create and map our relationships; we create blogs where we present our work, tell our stories, present our initiatives; we express our opinions by intervening in forums and commenting on web-pages and blogs.

On the other hand, in the cloud, we keep our data in remote data farm (storage as a service), we access remotely located software programs (software as a service), we use virtual computers emulated by the provider's hardware and software (computing as a service).

Web hosting and cloud hosting have different functions in principle, which overlap to some extent with the public-private divide (at least concerning individual, rather than corporate usage): the first enables us to make content accessible to others, while the latter offers a remote substitute for the use of one's personal computer (memory, software, computing power); the first provides us with a public space for sharing and communicating, the second with a remotely accessible private space. When putting or accessing content on the web we exercise the freedom of expression and information as well as economic and political freedoms, while when using the cloud for storing the documents we own and the computer tools we need, we exercise not only our property rights, but also, I would argue also our right to autonomy, work, and to the "security of the person", given that our personal computer space has become in a way our "external mind", where we store are memories and often the outcomes and the tools of our work.

However, the borderline between what is public and what private is getting increasingly fuzzy and shifting, as users on the one hand can restrict their audiences on the web, and on the other hand can instantaneously move information from their private space on the cloud into the web, uploading it into some web hosting platform, or even link information in the cloud to web pages, so that it becomes part of the web.

On the web, we can store our content on different platforms, each of which makes our information public in different ways (consider for instance the difference between publishing a movie in an on-line repository, on one's website, on blog, or on one's page). Moreover such platforms often offer the user various choices on the extent to which information can be accessible to others: as on a social network we can decide the circle of friends to whom to circulate information, so in certain blog systems (e.g. WordPress) or repositories (e.g. Scribd), we can choose whether to make the content accessible only to the people we authorise and whether to make it indexable.

At the same time we can connect on various ways the contents of our cloud-folders to the web. By making one of our folders web-accessible, all contents in the folder will have their URL (a universal resource locator, namely, a univocal web address), becoming web-objects, linkable to web pages, and uploadable by whoever clicks on the corresponding links. We may put some limits on sharing, for

instance, protecting links with passwords or limiting access to particular individuals. These functions are now accessible to everybody, since we can get freely 5 or 10 gigabytes of web storage and a larger memory space, with additional functions, at a little price. Even before the emergence of the cloud, one could make accessible to others through the web one's computer resources, as it happens in peer-to-peer network, but when such resources are on the cloud their offer on the web becomes much easier.

Thus in the current situation, users who want to make content available over the Internet have at their disposal various opportunities, through a combination of storage in the web, in the cloud, or in their individual hardware. This makes control over such content more difficult for providers of web hosting services. Users may easily re-upload their material on web-platforms, or may use web services only for linking and indexing content that remains on private spaces (and be re-linked or re-indexed when needed).

Web host providers are not exclusive gate-keepers to the Internet, but they attract their users by offering them enhanced facilities for creating, distributing and accessing content.

In case the user chooses to store the information in a web-platform (YouTube, Facebook, WordPress, Scribd, Flickr, etc.), the outcome, namely, what and how the information is going to be distributed on the web, is the intersection of two choices: the users' choice on what to distribute, on what platform, and with what options, and the providers' design choices on how to shape their platform, enabling what kinds of distribution, with what options for users. While users selects the content to be uploaded and possibly some options in the packages offered by each provider, providers' systems define what package of options are available to users, actualise the chosen possibility, provide the defaults and facilities which direct the users' selection of particular options. Note that users may also choose not to upload the information in a hosting platform, but only make it accessible though links to their individual cloud space, which would make it impossible for the web-provider to interfere with that information. Only the cloud-provider could do that, but at the price of interfering with the property and personal rights of users over their cloud space (note also that the user may prefer to store the information on his or her private hardware, even though with some additional costs and a more limited accessibility).

When a user distributes information through a commercial platform, we must clearly distinguish the information the user freely choses to make public on the platform, from the information which the user gives the provider to comply with the provider's requests. When freely making information public, the user distributes this information, to obtain advantages that result from the distribution itself, not in order to obtain something from the provider in exchange from letting the provider access users' information. This distinction is related to another distinction, namely, the distinction concerning whether the way in which the information is processed by the provider's platform and organisation may be considered neutral.

It seems to me that the providers' activity is neutral only as long as processing is meant to serve the users' aims, namely the function that the user wants to realise by using the provider's platform to distribute her information. Through serving the user's aims (e.g., by facilitating access to the material though indexing), the provider also achieves his own purposes, namely, increasing access to the website, which may lead to revenue from advertisers. However, this result supervenes on the outcome that is aimed at by the user, namely, on the information-sharing functions for the sake of which the user is uploading content on the platform. Neutrality does not cover further activities by the provider, such as using user's information for administrative purposes, or for various commercial interests, such as profiling or providing personalised advertising.

In this paper, I shall restrict my inquiry to user-generated information freely uploaded and neutrally processed by the provider's platform, following the users' choice to submit certain materials to the functions available on that platform. In other words, my analysis addresses the role of the provider as neutral (though self-interested) enabler of the sharing of user generated-information, in the context of web and cloud-hosting. The personal information I am concerned with is not the information

concerning the user himself, but rather the information concerning other people, uploaded by the user and distributed possibly in violation of data-protection rules.

2. The E-Commerce Immunities

Web hosting of user-generated information is addressed by the EU E-Commerce Directive,[1] which exempts providers from liability for hosting illegal information, while maintaining the liability of the users who have uploaded such information. The fundamental justification for these immunities can identified through a simple counterfactual argument, namely, by considering what would happen if providers where held liable, under criminal and civil law, for the illegal information hosted on their platforms: the risk of incurring such liabilities would force providers to police the Internet, to engage in filtering out preventively or removing any content that might lead to their liability. In fact, while being unable to remove all illegal information (given the huge amount of data being put on line, still increasing thanks to the development of new web-services, such as social networks and the connection between the web and cloud), providers would have to be proactive to reduce their liabilities. To clean their huge web premises as much as possible from illegal data they would need to heavily interfere with the content uploaded by their tenants (the users having generated the information): they could reduce false negatives (the distribution of illegal information) only by increasing false positives (the removal of legal information). Thus providers liability would lead to "collateral censorship" (Balkin 2008), which would on the one hand undermine users freedom and on the other hand involve high costs, to the detriment of current business models (free user access supported by advertising), and of the usage of the Internet.[2]

Through the regulation of providers' immunities (and the limitations of such immunities) the conflict of multiple valuable interests and rights is somehow balanced: third parties interests in preventing the distribution of certain data (interests concerning intellectual property, reputation, privacy, regulations on hate speech, etc.), users interests in distributing information (freedom of speech and expression, political and social participation, artistic freedom, economic freedom), users interests in accessing information (such as access to knowledge and culture), the economic interests of providers (economic freedoms), public interests (preventing illegal activities, protecting their victims, promoting creativity, innovation, access to knowledge and economic progress). In the E-Commerce Directive this balance is stuck by Articles 14 (hosting) and 15 (no general obligation to monitor.). According to Article 14, the provider is immune when

- he has no actual knowledge of illegal material, or
- upon obtaining such knowledge or awareness, he acts expeditiously to remove or to disable access
- to the information.[3]

Moreover, according to Article 15, member states may not impose general obligations on providers

[1] 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). In the US, similar immunities are provided by US Digital Millennium copyright act and the Communication Decency Act.

[2] There exists a vast literature on providers' immunities. See among others: Lichtman and Posner (2006), Lemley (2007), Hylton (2007), Grimmelmann (2009a). For European law, a detailed analysis can be found in Spindler et al. (2006). On social network, see also Grimmelmann (2009b), Sartor (2012).

[3] Article 14 (1): Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

- to monitor the information
- to actively to seek facts or circumstances indicating illegal activity.[4]

Here I shall not provide an overall analysis of providers' immunities but I shall limit myself to considering how they bear upon the data protection with regard to user-generated data.

3. Data Protection and Providers' Immunities in EU Law

It is dubious whether the e-commerce immunities also apply to data protection, which is governed by the Data Protection Directive[5] and its national implementations.[6] National judges and data protection authorities have adopted different approaches in this regard,[7] and even recent EU documents directly addressing data protection with regard to user-generated content (such as the Article 29 Working Party's Opinion 5/2009 on online social networking) seem wary of making reference to the E-Commerce Directive.

This view may be supported by a literal interpretation of Article 1 (5), of the E-Commerce directive, according to which the E-Commerce Directive does not apply to issues covered by the Data Protection Directive.[8]

Failure to apply the e-commerce immunities to the data Protection Directive might lead to what me may call "data protection exceptionalism": while the e-commerce immunities would cover liability for infringement of intellectual property, defamation, hate speech, incitement to crime, etc., they would not apply when the data uploaded and distributed in the providers' platforms is illegal because of a violation of data protection. According to this view, whether the provider would be considered liable or not would only depends on data protection law: we have to rely only on the Data Protection Directive (and its implementations) to construct the regulation of web-hosting with regard to the illegal processing of user-generated personal information.

---

[4] Article 15: 1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

[5] 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 (Data Protection Directive).

[6] The Data Protection Directive is complemented by the Directive on privacy and electronic communications (Directive 2002/58/EC the processing of personal data and the protection of privacy in the electronic communications sector), recasting Directive 97/66/EC.

[7] For instance the e-commerce immunities are not even mentioned in the recent Italian decision where three Google executives where condemned as a consequence of the distribution of a video containing sensitive personal data over YouTube (case Google-Vividown, decided by the Tribunal of Milan on 24 February 2010, sentenza n. 1972/2010). For a critical analysis, see Sartor and Viola de Azevedo Cunha (2010). For a review on cases web hosting and data protection, see Viola de Azevedo Cunha et al. (2012).

[8] Article 1 (5): "This Directive does not apply to . . . questions relating to information society services covered by Directives 95/46/EC and 97/66/EC." This idea is developed in recital 14: The protection of individuals with regard to the processing of personal data is solely governed by 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 and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries".

I believe that data protection exceptionalism should be rejected: even the existing law allows us to conclude that, contrary to the literal reading of Article 1 (5) of the Data Protection Directive, the e-commerce exemption applies horizontally, covering any kind of illegal content, including illegally uploaded personal data. We can achieve this outcome through a restrictive interpretation of Art 1 (5), namely by arguing that this article refers to the Data Protection Directive only the "questions relating to information society services covered by Directives 95/46/EC", which do not include providers' immunities with regard to user-generated data. In other terms, the E-Commerce Directive defers to data-protection law for the specification of what processings of personal data are illegal, while giving providers immunity for all illegal processings taking place on their platform (including those processings that are illegal because of the violation of data protection law).

However, certain limitations of the liability of host providers could also be obtained independently of the E-Commerce Directive, on the basis of an appropriate interpretation of provisions of the Data Protection Directive. First of all Article 1 excludes from the Data Protection Directive the use of personal-data in merely personal activities. Thus, as long as the users' activity, as supported by the providers' infrastructure, can be considered merely personal, no issue of data protection emerges. This would be the case when the user stores his information on the cloud, maintaining such information inaccessible to others, or also when the information is make accessible only to a restricted circle of people. Secondly, the data-protection Directive provides for the distinction between two addressees of the data protection rules, the controller and the processor, the first deciding on what data to process, for what purposes, the second implementing the choices of the first.[9] It is not clear how responsibilities for illegal processing are shared by the controller and the processor. We could limit the liability of the provider by assuming that when engaging in a neutral activity with regard to user-generated data, the provider only acts as a processor, and by arguing the a processor has no general obligation to monitor or check the inputs he receives from the activity of the controller, both with regard to the uploaded data, and to the ways in which this data are neutrally processed in the provider's platform. This understanding of the controller-processor relationships would allow us to map the provider-user distinction of the E-Commerce Directive into the controller/processor distinction of the Data Protection Directive.

4. Knowledge of Illegality and On-Line Censorship

After having argued for the application of the e-commerce immunities to host providers, we need to consider how such immunities should be interpreted in order to best balance all interests at stake, namely, the interests of possible victims, but also the interest of on-line speakers (uploaders), listeners (downloaders), and providers.

In particular, we have to examine the provision of Article 14 (1), of the E-Commerce Directive, according to which a provider is immune only as long as he "has no actual knowledge of illegal material, or upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information".

[9] Data Protection Directive, Article 2 (1): (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws orregulations, the controller or the specific criteria for his nomination may be designated by national or Community law; (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Knowledge of the illegality of a certain piece of data involves 2 aspects:

1. the factual knowledge the piece is hosted on the provider's server;
2. the legal knowledge that the piece violates the law.

To examine the interpretive issues emerging from this provision we need to focus on the concept of knowledge. According to the most common understanding of this concept, we have knowledge when we believe something that is true, which means that the concept of knowledge includes at least two elements: belief and truth.[10] A person knows a proposition p when both of the following hold: (a) the person believes that p is the case and (b) p is indeed the case. Thus for the provider to know that he is hosting illegal material both of the following must hold: (a) the provider believes that he is hosting illegal material and (b) the provider is in fact hosting illegal material. Our interpretive problem pertains to (a), namely, we need to examine what it means for the provider to know that he is hosting illegal material.

One possible answer follows from assuming that factual knowledge is enough. According to this perspective (which corresponds to the principle according to which ignorance of the law is no excuse, "*ignorantia legis non excusat*"), the provider would be obliged to remove or make inaccessible a piece of data (a text, a picture, a photo, a movie) from his platform whenever he knows that the piece is on the platform, and the piece is happens to be illegal. So considering our notion of knowledge as true belief, for the obligation of the provider to be triggered, all of the following should hold, under this interpretation: (a1) the provider believes that a certain piece is on the platform, (b1) the piece is indeed on the platform, (b2) the piece is illegal.

According to the second perspective, the provider would be obliged to remove the piece only when he knows that both the piece is on platform and it is illegal. Thus all of the following should hold, under this second interpretation: (a1) the provider believes that a certain piece is on the platform, (a2) the provider believes that the piece is illegal, (b1) the piece is on the platform, and (b2) the piece is illegal.

Note the difference: according to the first interpretation, for the obligation to take down to be triggered one element is missing, namely, (a2), the provider's belief that the hosted content is illegal: the provider would be obliged to take down also the material he considers to be legal (or more probably so), under pain of being liable in case his judgement were considered to be wrong by the competent authority.

Thus, the first interpretation would put the provider in a difficult situation, and would presumably lead to what we called collateral censorship. We have to distinguish here different epistemic conditions, depending on the nature of the illegal content. In some cases the only difficulty consists in knowing that a certain piece of content is on the platform. Once this knowledge is achieved, establishing whether the piece is illegal is rarely straightforward. This may be the case, for instance, when a right-holder complains about a copyright violations consisting in mere duplication of a registered work (though it may be doubtful whether the right holder may have consented to the publication, or whether the use of the work may be considered as fair use, or fall into a copyright exception). In other cases, however, assessing illegality is much more difficult: even if the provider knows that a certain material is on his platform, he may remain in doubt (and thus fail to have a belief) concerning the illegality of such a material. This is the case in particular when competing constitutional rights are involved: consider for instance how it may be difficult to assess whether copyright have been infringed in the

[10] For the idea of knowledge as true belief, see recently (Goldman 1999,ch. 1). According to other authors, for having knowledge, also justification is needed (a true belief held without a plausible ground would not constituteknowledge), as argued already by Plato in the dialogues Meno and Theaetetus. Therefore only true and justified belief would provide knowledge. Others have argued that this is not yet sufficient to obtain knowledge (following the seminal contribution by Gettier 1963), and have provided additional conditions. This important philosophical debate, however, is not very relevant for our purpose since all those conceptions include at least the elements we have mentioned, namely, belief and truth.

creation of a new work inspired by a previous one (intellectual property v. freedom of expression), or whether by making statements about a person her data protection rights are infringed (data protection v. freedom of expression).[11]

In all such situation of legal uncertainty, making the provider liable for hosting illegal information would provide it with a strong incentive to remove any piece of material on whose legality he has even a small doubt, since even in such a case the expected potential loss would outweighs the marginal benefit the provider derives from keeping that particular piece on line (alongside with all other material in the platform).[12]

One possible way out of this situation would consist relaying on the provider's assessment of the illegality of the content. This could be obtained by conditioning providers' liability also to some degree of certainly in legal knowledge,[13] namely, on the provider's knowledge in the illegality of the user-generated content.

Such knowledge would only exist when the provider in good faith believes both that a certain content is on its platform, and that the content is most probably illegal rather than legal.[14]

---

[11] In such cases, in fact, we may even wonder whether there are objective standards conclusively determining whether the material is legal or illegal, or whether this qualification will depends upon a discretional decision by the judge. But this would take us into the legal theory debate on the objectivity of legal knowledge and on the determinacy of the law, i.e., on whether there is only one right answer to each legal issue (as claimed by Dworkin 1977) or whether the law may sometimes be incomplete or undetermined (as affirmed by Hart 1994), and whether such an answer, even if it exists, is accessible to a legal reasoner endowed with non-superhuman skills.

[12] To clarify the point, let us suppose that the provider is able to assess the probability $p(i_d)$ of the illegality i_d of certain piece of data d . Let us also assume that in case the piece is really illegal and it is not removed, the provider will have to pay a compensation c_d, while if the piece remains on line, the provider will gain a benefit b_d (the expected additional advertising revenue to be obtained consequent to assesses to that piece of data). Given this arrangement, if the provider leaves the piece on line, his expected loss is $c * p(i_d)$, while his expected gain is b_d. So, the expected outcome (gain minus loss) is $b_d - c_d * p(i_d)$. If he decides to take off the piece, the outcome is 0, no gain and no loss, Clearly, the provider will leave the material on line only when $b_d - (c_d * p(i_d)) \geq 0$

Assuming for instance that the compensation will be 100, while the gain to be obtained by leaving the material on line is 1 (usually the marginal gain a provider can obtain by making one additional piece available is quite low), we have that, for the provider to keep the material on line it must be that: $1 - (100 * p(i_d)) \geq 0$

This will hold only in the few cases when that the probability of illegality $(p(i_d))$ is less (or equal) to 1%. In all other cases, the provider will prefer to take down the information to prevent potential losses.

[13] I assume that belief and knowledge can come in degrees, even though I cannot enter here a discussion on the matter, see Haack (1993) and Goldman (1999).

[14] Let us assume that the provider has to assess the legality of a set of pieces of data $S = L \cup I$, where L is the set of the legal pieces and I is the set of the illegal ones (the set S may be, for instance, the set of pieces he is requested to take down by the data subject). Any mistake (taking down legal material or letting online illegal material) will have a social cost. Let c be the average social cost of taking down a legal piece l and c_i the average cost of letting an illegal piece i on line. For simplicity's sake, let us assume that the number of legal and illegal pieces in S is the same: $|L| = |I|$, ($|X|$ indicates the cardinality of a set X, namely, the number of its elements). Then the objective is to minimise the following social cost:

$$c_l * |L_{out}| + c_I * |I_{in}|$$

where L_{out} is the set of legal pieces that are taken out and I_in is the set of the of illegal pieces which are left in.

To simplify the calculations lets us assume that the two kinds of mistakes (keeping illegal data on line on line and taking out legal data), have on average the same cost, so that the objective becomes minimising the following sum:Let us also assume that the provider can only state whether a piece of information is more probably illegal or more probably legal, and then when making such evaluation he does better than chance, namely. In other words let us assume that when the provider says that a piece of information is more probably legal there is a chance higher than 50% that it is legal.

Then we get a better outcome (a lower value for $|L_{out} + I_{in}|$) by authorising the provider to let on line all content he believes in good faith to be more probably legal, rather that telling him to take down all materials he is requested to take down (this assumes that the provider acts in good faith according to his beliefs). We also get a better outcome in this way than by making the provider liable for any illegal material he leaves on line, a choice which, as we have seen would lead him

The legality-judgement by the provider however, could be substituted with a mechanism that invites the parties (the data subject and the uploader) to make their legality-assessments, and which induces such assessments to be sufficiently reliable. This could be obtained, for instance, by adopting a notice and takedown procedure such as that introduced by the US Digital Millennium Copyright Act with regard to copyright infringements. According to the DMCA, the uploader who considers that his rights are infringed sends a notice to the provider, who takes down the material and informs the uploader; if the uploader replies with a counter notice (claiming that the uploaded material is legitimate), then the provider will put the material back, unless the right-holder starts a lawsuit. The actions by the right-holder and the uploader signal the probability that the material is legal or illegal: the notice signals the probability that it is illegal (according to the judgement of the right holder), but the counter notice signals that it should be legal (according to the uploader), and the decision to sue by the right-holder, again signals the probability that it is illegal (according to more serious evaluation, which involves the cost of starting the lawsuit).[15]

Additionally (or alternatively), we may introduce the judgement on illegality (a presumptive judgment, subject to judicial review) by a body that is better placed and more competent than the provider, i.e. in particular, by a data protection supervisor. Under such arrangements the provider should enjoy the immunity as long as he, when reached by a notice of data-protection violation, informs both the uploader and the data protection authority and follows the indications from that authority.

Combining these ideas, we could design a mechanism like the following:

- alleged victim sends notice of illegal piece of content to provider
- provider takes down piece in case he considered in good faith that the piece is most probably illegal, otherwise leave it on-line
- in any case provider informs uploader
- if uploader does not respond or is anonymous, provider takes piece down (in case it was left it on line)
- if uploader sends counter-notice, provider informs victim
- in the latter case if victim does not bring lawsuit or involves data protection authority, provider puts back piece (in case is was taken down)

This would involve the parties in (the alleged victim and the uploader) in the procedure and would induce the parties themselves to assess the merit of their case and make consequential choices, while

(Contd.)

to take down all risky materials. Assume for instance that the provider's judgement on legality or illegality is correct in the 60% of cases.

Then the number of mistakes will be $|L\_out| + |I_{in}| * 0.4$ which is inferior (given the assumption that $|L| = |I|$) to $|L_{out}|$, the number of mistakes we will obtain if the provider were to take out all materials he is asked to remove, for fear of undergoing liability in case he is mistaken.

The model here proposed can be developed by considering the possibility that a more serious damage is caused by leaving the data on line then by removing it (or vice versa), and by considering the different prior probabilities that the data are legal rather an illegal (see also the next footnote).

[15] For instance, assume that before the lawsuit there is a very small chance that a randomly taken piece of material is illegal (e.g., 1%). Assume also that the chance that a piece is illegal goes up to 50%, when the right holder sends notice of a data protection violation, and that the provider has a 60% chance of judging correctly when requested to determine whether a piece is legal or illegal. Under these assumptions, with regard to those pieced that are claimed to be illegal by the right-holder, we get a better outcome by relying on the provider's judgment, rather than by taking down (or leaving on line) all such pieces. However, assume that a counter notice by the uploader signals that there is a 80% chances the data is legal (only those who have good grounds would react to the notice). Then it is better if the provider does not exercise his judgment with regard to the counter-noticed pieces, but leaves all materials on line. Where he to apply his judgement (which is correct in the 60% of the cases), he would make things worse: the materials he would wrongly discard would exceed the materials he would rightly preserve. On the contrary, the fact that there is no counter notice may signal that the material is probably illegal, so that it is better to take it down, regardless provider's judgment. And so on.

making use also of the good faith assessment of the provider (a similar solution, with regard to copyright violations, is currently under discussion in Canada).

5. Providers' Liability in the New Regulation

Let us now address the changes that the new Proposal for a Data Protection Regulation[16] introduces with regard to providers' liability. First of all, we need to ask ourselves whether the doubts concerning privacy-exceptionalism (i.e., the idea that commerce immunities do not apply to data protection) have been removed. This seems indeed to be the case, according to the clear statement of Article 2 (3), according to which the 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."

A possible residual uncertainty may arise in connection with Article 88 of the Regulation, according to which references to the Data Protection Directive "shall be construed as references to this Regulation". Such references also include the above mention Article 1 (5) (a) of the E-Commerce Directive, which should therefore be read as: "Art. 1, par. 5: "This Directive does not apply to . . . questions relating to information society services covered by Data Protection Regulation."

Thus, on the one hand the Regulation is without prejudice to the application of the E-Commerce Directive (whose immunities should therefore cover also user-generated data involving a data protection violation), and on the other hand e E-Commerce Directive does not apply to questions covered by the Data Protection Regulation. A clarification on this regard would be welcome, even though the issue may be addressed though interpretation, namely, arguing as above that the questions covered by the Data Protection Directive concern what processings are illegal, while the Directive exonerates the providers for certain illegal processings taking place in their platforms (including those illegal for violating data protection).

Moving down to specify previsions, we need to consider certain rights of the data subject which entail corresponding obligations of the controller. Whether such obligations apply to the provider with regard to user-generated data neutrally processed depends on whether the provider, when exercising this activity, can be considered a controller.

If providers are qualified as controllers, they are charged with very burdensome tasks. For instance, according to Article 14, they would be required to chase any person mentioned in a blog, social network, or forum, to inform that person that data about him or her is on the platform and provide any "information needed to guarantee fair processing.[17] There is a limitation to this requirement, namely

[16] COM(2012) 11/4 Draft Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). For a precise analysis of the Regulation, see Kuner (2012). See also De Hert and Papaknstantinou (2012).

[17] Article 14 (1): Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer; (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (c) the period for which the personal data will be stored; (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data; (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (f) the recipients or categories of recipients of the personal data; (g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission; (h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

the provision of Article 14 (5) (b), according to which the controller is exonerated from such an obligation when "data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort", but it remains to be established when an effort may be considered "disproportionate", a concept that invites highly discretional evaluations by data protection authorities and judges.

On the other hand, if the users uploading the data were the only controllers (consider for instance a person publishing a blog with comments on political and social issues at a local level, or a person putting on line his or her CV, including information about previous employment relationship with individual work givers), then the formalities established by Article 11 seem indeed too burdensome.

6. The Right to Be Forgotten

Article 17 (1) grants data subjects the "right to be forgotten and to erasure", namely, the power to obtain 'from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data".[18] This right, as it has been observed (Rosen 2012) seems to fail to distinguish between two kinds of on-line user-generated material:

1. material about the data subject which the data subject herself has put on the providers' platform
2. material about the data subject that other users have put on the providers' platform.

It seems to me that case (1) is uncontroversial: a data subject should have the right to eliminate all personal information she has chosen to upload on the provider's platforms. More generally, I think that the very idea of a neutral processing of user-generated data (processing meant to satisfy users aims) entails that the user should be given in principle the possibility of withdrawing any data, personal or not, he or she has uploaded.

The controversial aspect of this right concerns case (2), namely whether the data subject should have the power of ordering the provider to erase content about herself uploaded by other users (who could have created such content, or have obtained it by reproducing or modifying content originally published by the data subject). Since the obligation only concerns controllers, the decisive point seems to be whether the provider could be considered as a processor or a controller with regard to such personal data. For instance, we may ask whether Wikipedia is a processor or a controller with regard to personal data published by Wikipedians on Wikipedia's pages.

Let us first assume that the provider is a processor, while only the user-uploader is a controller with regard to third-parties user-generated data neutrally processed. In this case the data subject wishing the data to be erased according to 17 (1), should request the user to take down the data he has uploaded. The user should then consider whether to take the data down or whether to leave them on the platform, facing the risk of a lawsuit. The data subject could also request the provider to take down the material, but in this case, given that the provider only is a processor, the data subject should refer to the discipline of the e-commerce immunities, according to which a provider becomes liable when he knows that he is hosting illegal data (which would raise the issue of knowledge of illegality we discussed above).

[18] Article 17 (1): The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons.

Let us now assume that on the contrary that also the provider (besides the user) is considered to be a controller with regard to user-generated data concerning third parties. Then a provider would have the obligation to take down from his platform the content uploaded by any users, whenever the provider is requested by the concerned data subjects, according to art. 17 (1). This would mean that providers would become law enforcers for data protection, exercising this power-duty against their users, who would be deprived of the possibility to object and resist. If the provider-controller would fail to take down privacy infringing content, not only will the provider have to compensate the damage, but it will also be subject to a severe sanction (art. 77), as we shall see in the next section. Under such conditions, as shown above, providers seems to have no choice by to remove any content which has a non-null chance of being considered illegal, without paying attention to any objections.

It seems to me that this second way of understanding Article 17 (1) could involve a serious infringement of fundamental rights of Internet users, and in particular, an unacceptable limitation of freedom of expression.

Let us now consider Article 17 (2), according to which the controller who has made personal data publicly available has the obligation to "take all reasonable steps, including technical measures, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data."[19] Also the implications of this rule are far from clear. Let us consider again the two possible qualifications of the provider, when allowing public access to user-generated personal data concerning third parties, namely, as a processor or as a controller.

Following the first qualification (the host provider is a processor), the obligation to contact anybody hosting the third-parties' personal data would only fall upon the user-uploader, who would be the only controller. To meet the request by the data subject, the user would have to contact anybody "processes" copies of the uploaded data (both users-controllers and providers-processors), and inform them of the erasure request. This would put a serious burden on the user (even though only reasonable steps are required). In particular, the user would be forced to engage in a search over the whole Internet even when the data subject had given his consent to the publication of the data (e.g., to the publication of a photo) and has then changed her mind. In many cases, it may not be clear what is meant by the "data the publication of which the controller is responsible". Assume for instance that some comments were made in a blog post upon a person (e.g., about a public persons' financial problems or sentimental affairs), and that similar comments are later published on the Internet (in blogs, forums, etc.). Do these other comments contain the same data as published in the original post? Is this the case also when the same information was obtained from other sources and expressed in different ways?

Following the second interpretation (also the host provider is a controller), Article 17(2) would concern the case where data originally uploaded in the provider's platforms have been reproduced and copies have been made accessible over the Internet in the platforms of other providers (or in the servers of individual users). The provider should then contact all entities hosting copies on the data and inform them of the data subject's request. This information would then trigger for all other providers (who would also be controllers of anything they host) the obligations to take down the data, according to 17 (1). Under this interpretation, thus, the request by the data subject will start a global chase for any instance of the data, involving all providers hosting total or partial copies of such data. All providers would have to interfere with the choices of their users, removing data uploaded by the latter or making such data inaccessible. The erasure order would not only concern copies of the data,

[19] Art. 17 (2): Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

but also links to them, which would require search providers to interfere with methods for indexing and searching for content.[20]

It seems to me that under both interpretations the implementation of the right to be forgotten is likely to raise notable uncertainties and costs, and endanger freedom of expression. The second interpretation (viewing the host provider as the controller) is likely to cause a most serious threat to freedom of expression: the request to take down the data would spread virally over Internet, bringing with it the obligation to "clean" any server from the unwanted information or of links to it, and obligation which is severely sanctioned as we shall see.

A further critical aspect of the proposed regulation of the right to be forgotten is the insufficient breadth and strength of the exceptions provided for the obligation to remove data. Such exceptions are mentioned in Article 80, according to which "Member States shall provide for exemptions or derogations . . . for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

First of all, we may wonder whether the "reconciliation" of data protection and freedom of expression should be completely delegated to national legislation, even though freedom of expression is a most important fundamental right, recognised in art 11 of the European Charter of Fundamental right as the "freedom to hold opinions and to receive and impart information".

Secondly, it seem that the exceptions to the right to be forgotten (the right to have information erased) are very narrowly framed, as concerning "solely" journalistic purposes and artistic or literary expression.

For instance, the notion of "journalistic purposes" could be understood as only applying to materials published by registered journalists, or in registered journals. This would allow unrestricted censorship of the emerging citizens' journalism (publication of information and opinion by non-professional people in blogs, forums, etc.). Non-qualified individuals or organisation (such as WikiLeaks) would be obliged to take down any information that, while addressing social or political or social matters, mentions individual persons.[21] If the notion of journalism were limited to information on recent events, activities aimed at informing people about the past (e.g., the preparation of a Wikipedia page on past political scandals) would similarly become illegal as soon as names are made. Thus it seems that exceptions covering "solely" journalistic and artistic/literary fails to cover the extent of the "right to impart information", as established on the UN Human Rights Declaration and by the EU Charter of Fundamental Rights.

In section 83 of the regulation, there is an also exception to the obligation to forget, with regard to data published by "bodies" conducting "historical, statistical and scientific research", when the publication of such data is "necessary to present research findings". Again, consider a passage in a Wikipedia-page mentioning individuals involved in a past event (e.g. a political scandal, a crime, etc.). We may wonder whether the individual having contributed the article is a "body" and whether the re-publication of other people's findings would count "presenting research findings". Some cases of this kind have been addressed in different ways in different jurisdictions, according to how they understand the need to balance data protection and freedom of expression. I am not putting into question that a proportionality based approach may be needed to address such issues, but the Regulation seems to go beyond that, ordering censorship whenever the strict grounds for an exceptions based on journalism or historical research are not available.

[20] On how interventions on search methods may have a negative impact on Internet freedoms, see Lemley et al. (2011).

[21] On citizens' journalism on the Internet, see for instance Benkler (2011).

7. Sanctions for Those Who Do Not Forget

Let us now consider the sanctions for violations of the right to be forgotten. According to Article 79 (5) (a) anyone who violates the right to be forgotten[22] would be subject to the sanction of Article 79 (5), namely "a fine up to 500 000 EUR, or in case of an enterprise up to 1 of its annual worldwide turnover". In addition the violator would have to compensate the damage suffered by the data subject, according to Article 77 (1).[23]

Since individual users would viewed as controllers, the provision in Article 79 (5), threatening such a high penalty for the refusal to take down illegal information, would induce uploaders to capitulate to any request to remove information unwanted by the concerned data subject, whenever there is even a minimal risk that the information will be considered to be illegal. This would entail a serious impairment to freedom of expression: uploaders would face the choice between yielding to the request, or risking the penalty in case they were unable to satisfy the authorities that they had posted the data "solely for journalistic purposes or the purpose of artistic or literary expression," and that in the particular case freedom of expression should prevail over data protection, according to a proportionality assessment.

If additionally also providers were viewed as controllers, then according to 17 (1) the data subject could asks the host provider to remove allegedly infringing data uploaded by his individual users. In case the data were not removed, the provider would face not only civil liability, but also, the sanction of Article 79 (5). To avoid risking the sanction, providers would have to engage is censorship whenever they receive a request to erase personal data. To illustrate the dramatic effects this might have, consider the application of the right to be forgotten to Wikipedia: all propositions including persons' names would have to be deleted under request by the concerned data subjects. Thus each data subject mentioned in Wikipedia's pages could compel Wikipedia to selectively clean their pages from every statement they do not like. To prevent such censorial excesses, I think that providers should be should be exempted at least from the administrative sanctions when maintaining on line illegal material while believing in good faith that it is (probably) legal.

On the contrary, if providers were considered only as processors, they would not be subject to the administrative sanctions for not complying with the right to be forgotten, which apparently apply only to controllers. Under this interpretation, providers would only run the risk of having to compensate the damage according to Article 77 (1), which is complemented by the provision of 77 (3), which excludes liability "if the controller or the processor proves that they are not responsible for the event giving rise to the damage".

[22] Article 79 (5) (a): Anyone who, intentionally or negligently . . . does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17.

[23] Article 77 (1): Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.

8. Conclusion

It is now time for me to conclude this summary analysis of the liability of host providers in the new Data Protection Regulation.

It seems to me that the Regulation provides for a significant progress in the EU law on the matter. While enhancing the protection of data subjects, the regulation puts on-line freedom of speech on a safer ground, by clarifying that providers' immunities introduced by the E-Commerce Directive also apply to data protection.

However, I think that an adequate discipline for the hosting of user-generated data, which pays due attention to on-line freedom of speech, would require some modifications.

First of all it should be clarified that providers are not data controllers, when they neutrally process user-generated data. Under such conditions, the users-uploaders should be considered to be the only controllers.

Moreover, providers should not be liable for keeping data on line when they believe in good faith that the data might be legal, and no competent authority has yet ordered the removal. This should be complemented by designing a notice and take down procedure where also uploaders are given the chance to express their view, and data protection authorities have the power to express a binding (though presumptive, being subject to judicial review) assessment of illegality.

Finally, the sanction for the violation of the right to be forgotten should be reconsidered with regard to both providers and to individual users (and possibly limited to the case when the injunction of a data protection authority is at issue), since the threat of such a serious punishment is likely to have a chilling effect on freedom of speech.

References

Balkin, J. M. (2008). The future of free expression in a digital age. *Pepperdine Law Review 36*, 101–18.

Benkler, Y. (2011). A free irresponsible press: WikiLeaks and the battle over the soul of the networked fourth estate. *Harvard Civil Rights-Civil Liberties Law Review*.

De Hert, P. and V. Papaknstantinou (2012). The proposed data protection regulation replacing directive 95/46/ec: A sound system for the protection of individuals. *Computer law and security review 28*, 130–42.

Dworkin, R. M. (1977). Hard cases. In *Taking Rights Seriously*, pp. 81–130. Cambridge, Mass.: Harvard University Press. (1st ed. 1975.).

Gettier, E. (1963). Is justified true belief knowledge? *Analysis* 23, 121–3.

Goldman, A. (1999). *Knowledge in a Social World*. Oxford: Oxford University press.

Grimmelmann, J. (2009a). The Google dilemma. *New York School Law Review*, 939–50.

Grimmelmann, J. (2009b). Saving Facebook. *Iowa Law Review 94*, 1137.

Haack, S. (1993). *Evidence and Inquiry*. Oxford: Blackwell.

Hart, H. L. A. (1994). *The Concept of Law* (2nd ed.). Oxford: Oxford University Press.

Hylton, K. N. (2007). Property rules, liability rules and immunity: An application to cyberspace. *Boston University Law Review 87*, 1–39.

Kuner, C. (2012). The European Commission's proposed Data Protection Regulation: A Copernican revolution in European data protection law. *Privacy and Security Law Report*, 11, 1–15.

Lemley, M., D. S. Levine, and D. G. Post (2011). Don't break the internet. *Stanford Law Review Online 64*, 34.38.

Lemley, M. A. (2007). Rationalising internet safe harbours. *Journal on Telecommunication and High Technology Law 6*, 101–19.

Lichtman, D. and E. A. Posner (2006). Holding internet service providers accountable. *Sup. Ct. Econ. Rev. 14*, 221.

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online 64*.

Sartor, G. (2012). Social networks e responsabilità del provider. *AIDA*.

Sartor, G. and M. Viola de Azevedo Cunha (2010). The Italian Google-case: Privacy, freedom of speech and responsibility of providers for user-generated contents. *International Journal of Law and Information Technology*, 1–23.

Spindler, G., G. M. Riccio, and A. Van der Perre (2006). Study on the liability of internet intermediaries. Markt/2006/09/E. Service Contract ETD/2006/Im/E2/69.

Viola de Azevedo Cunha, M., L. Marin, and G. Sartor (2012). Peer-to-peer privacy violations and isp liability: Data protection in the user-generated web. *International Data Privacy Law*, 1–18.


European
University
Institute
European University Press