# Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?

Giovanni Sartor*


## Abstract

- This article examines host providers' liabilities and duties with regard to user-generated content, focusing on the novelties contained in the 'Proposal for a Data Protection Regulation', recently advanced by the EU Commission.
- First it considers how the Proposal addresses the contentious overlap of e-commerce immunities and data protection rules.
- Then it considers providers' knowledge that illegal personal information has been uploaded on their platform, and examine whether such knowledge should terminate providers' immunity.
- Finally, it critically assesses the right to be forgotten, newly introduced in the Proposal, and the sanctions for its violation.


## Introduction

User-generated information is processed on providers' platforms in a way resulting from the intersection of two choices: users' choices on what to distribute, on what platforms, and with what options, and providers' choices on how to shape their platforms, enabling what kinds of distribution, with what options to offer to their users. In the following I shall consider whether the latter choices may be sufficient to ground a responsibility of providers for violations of data protection law, focusing on the 'Proposal for a Data Protection Regulation' recently advanced by the EU Commission. The Proposal, currently being examined by the EU Parliament and Council, is meant to provide a new framework for data protection, substituting the Data Protection Directive (95/46/EC) and the national laws implementing it.

My inquiry is limited to information freely uploaded by users and neutrally processed by providers' platforms. Thus, I shall only address the role of providers as neutral (though self-interested) enablers of the sharing of user-generated information, in the context of web and cloud-hosting. Through serving users' aims (eg by facilitating access to the uploaded material through indexing), providers also achieve their own purposes, and, in particular, they foster access to their websites, which may lead to additional revenue from advertisers. However, this result supervenes on an outcome that is aimed at by the users, for the sake of which users are uploading content to the platforms, namely, making the uploaded information easily accessible on the web.

## The e-commerce immunities

Web-hosting of user-generated information is governed in the EU by the E-Commerce Directive,[1] which exempts providers from liability for hosting illegal content, while maintaining the liability of the users who have uploaded such content. The fundamental justification for these immunities can be 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 liabilities would force providers to police the Internet, to engage in filtering out or removing any content for which they may be liable.

In fact, while being unable to filter or remove all illegal information (given the huge amount of data being put online—still increasing thanks to the development of web and cloud-services)—providers would have to be proactive to limit their liabilities. To clean

* University of Bologna, Law Faculty-CIRSFID and European University Institute of Florence. E-mail: giovanni.sartor@gmail.com.

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 USA, similar immunities are provided by US Digital Millennium Copyright Act and the Communication Decency Act.

their huge web premises as much as possible from illegal data, they would need to interfere with content uploaded by their tenants (users having generated the information): providers 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',[2] 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.[3]

Through the regulation of providers' immunities (and the limitations of such immunities), multiple valuable interests and rights are somehow balanced: third parties' interests in preventing the distribution of certain data (interests concerning intellectual property, reputation, privacy, 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 participation in knowledge and culture), the economic interests of providers (and their market freedoms), public interests (preventing illegal activities, 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, providers are immune when

- they have no actual knowledge of illegal material, or
- upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the information.[4]

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

- to monitor the information
- to actively to seek facts or circumstances indicating illegal activity.[5]

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

## 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[6] and its national implementations.[7] National judges and data protection authorities have adopted different approaches,[8] 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 reading of Article 1 (5), of the E-Commerce directive, according to which the E-Commerce Directive

2 JM Balkin, 'The future of free expression in a digital age' (2008) 36 Pepperdine Law Review 101–18.

3 There exists a vast literature on providers' immunities. See among others: D Lichtman and EA Posner, 'Holding Internet service providers accountable' (2006) 14 Sup. Ct. Econ. Rev. 221; MA Lemley, 'Rationalising Internet safe harbors' (2007) 6 Journal of Telecommunication and High Technology Law 101–19; KN Hylton, 'Property rules, liability rules and immunity: An application to cyberspace' (2007) 87 Boston University Law Review 1–39; J Grimmelmann, 'The Google dilemma' (2009) New York School Law Review 939–50. For European law, a detailed analysis can be found in G Spindler, GM Riccio, and A Van der Perre, 'Study on the liability of Internet intermediaries' Markt/2006/09/E. Service Contract ETD/2006/Im/E2/69 (2006). On social network, see also J Grimmelmann, 'Saving Facebook' (2009) 94 *Iowa* Law Review 1137.

4 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.'

5 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.'

6 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).

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

8 For instance the e-commerce immunities are not even mentioned in the recent Italian judgment 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 G Sartor and M Viola de Azevedo Cunha, 'The Italian Google-case: Privacy, freedom of speech and responsibility of providers for user-generated contents' (2010) *International Journal of Law and Information Technology* 1–23. For a review of cases on web hosting and data protection, see M Viola de Azevedo Cunha, L Marin, and G Sartor, 'Peer-to-peer privacy violations and ISP liability: Data protection in the user-generated web' (2012) 2 *International Data Privacy Law* 1–18.

does not apply to issues covered by the Data Protection Directive.[9]

Failure to apply the e-commerce immunities to data protection might lead to what we may call 'data protection exceptionalism': while the immunities would cover every other liability for user-generated content—from infringements of intellectual property, to defamation, hate speech, incitement to crime, etc.—they would not apply to user-generated violations of data protection. According to this view, whether the provider would be considered liable or not when hosting third parties' private data would only depend 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.

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 E-Commerce Directive, the e-commerce exemption applies horizontally, covering every kind of illegal content, including illegally uploaded personal data. We can achieve this outcome through a restrictive interpretation of Article 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 processing of personal data are illegal, while giving providers immunity for all illegal processing taking place on their platform (including processing that is illegal because of violations 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 in the Data Protection Directive. First of all, Article 3 excludes from the Data Protection Directive the use of personal data in 'purely personal or household activity'. Thus, as long as the users' activity, supported by the providers' infrastructure, can be considered purely personal, no issue of data protection emerges. This would be the case when the user stores her information on the cloud, making such information inaccessible to others, or also when the information is 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 what data to process, for what purposes, the second implementing the choices of the first.[10] 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 that a processor has no general obligation to monitor or check the inputs he receives from the controller, both with regard to the uploaded data, and to the ways in which these data are neutrally processed on the provider's platform. This understanding of the controller–processor relationship would allow us to map the user–provider distinction in the E-Commerce Directive into the controller–processor distinction in the Data Protection Directive.

## Knowledge of illegality and online censorship

After having argued for the application of the e-commerce immunities to user-generated information violating data protection, we need to consider how such immunities should be understood in order to best balance all the interests at stake, namely, the interests of possible victims (data subjects), but also the interest of online speakers (uploaders), listeners (downloaders), and providers (enablers).

In particular, we have to examine the provision of Article 14 (1), of the E-Commerce Directive, according

9 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.'

10 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 or regulations, 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.'

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.'

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

1. the factual knowledge that 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.[11] A person knows that *p* is the case 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 materials both of the following must hold: (a) the provider believes that he is hosting illegal materials and (b) the provider is in fact hosting illegal materials. Our interpretive problem pertains to (a), namely, we need to examine what it means for the provider to believe that he is hosting illegal materials.

One possible answer follows from assuming that a true factual belief 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 lose his immunity, and thus be obliged to remove or make inaccessible a piece of data (a text, a picture, a photo, a movie) from his platform whenever he has the true belief that the piece is on the platform, and the piece happens to be illegal (even though the provider does not believe that the piece is 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 also take down material he considers to be legal (or more probably so, or possibly so), under threat of being liable in case his judgement were considered to be wrong by the competent authority.

Thus, the first interpretation puts the provider in a difficult situation, and would presumably lead to 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 whether a certain piece of content is on the platform. Once this knowledge is achieved, establishing whether the piece is illegal is straightforward. This may be the case, for instance, when a right-holder complains about a copyright violation consisting in the mere duplication of a registered work (though it may be doubtful whether the right-holder has consented to the publication, or whether the use of the work may be considered as fair use, or fall into a copyright exception). More often, 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 form a precise 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 has been infringed in the creation of a new work inspired by a previous one (intellectual property versus freedom of expression or artistic freedom), or whether a person's data protection rights are infringed by the public statement of another person (data protection versus freedom of expression).[12]

In situations of legal uncertainty, making the provider liable for hosting illegal information would

11 For the idea of knowledge as true belief, see recently A Goldman, *Knowledge in the Social Word*. (Oxford: Oxford University Press, 1999) ch. 1. According to other authors, in order to have knowledge, justification is also needed (a true belief held without a plausible ground would not constitute knowledge), as argued 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 E Gettier, 'Is justified true belief knowledge?' (1963) 23 Analysis 121–3), 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.

12 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 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, ie, on whether there is only one right answer to each legal issue or whether the law may sometimes be incomplete or undetermined, and whether such an answer, even if it exists, is accessible to a legal reasoner endowed with non-superhuman skills. Without going into that debate, I assume that we

provide him with a strong incentive to remove any piece of material on whose legality he has even a small doubt; even when a piece appears to be more probably legal, the expected potential loss would outweigh the marginal benefit the provider derives from keeping that particular piece online (alongside all the other materials on the platform).[13]

One possible way out of this perplexity would consist in relying on the provider's assessment of the illegality of the content. This could be obtained by also conditioning liability on some degree of certainty in legal knowledge,[14] namely, in making the provider liable only when he has the belief the he is hosting illegal user-generated content. Such a belief will only exist when the provider accepts in good faith both that certain content is on its platform, and that the content is more probably illegal rather than legal.[15] This, however, seems to make legal enforcement very difficult. How can we assess the existence of the illegality belief in the provider's mind? A proxy for that, however can be given by the "objective" possibility of achieving a sufficient degree of certainty in such an assessment with a reasonable effort, under the given circumstances. So, the provider's belief in the illegality (of a content he knows to be in his platform) should be excluded when a reasonable person, under such circumstances, could still possibly doubt that the content might be legal.

The legality-judgement by the provider could also 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 (DMCA) with regard to copyright infringements. According to the DMCA, the (alleged) right-holder who considers that her 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

have the cognitive skills that allow as to answer such questions in many cases, though with degrees of doubt. It may also be argued what is here at issue is not so much the truth of the proposition that a certain content is legal or illegal, but the forecast that the compentent authority will consider the content to be legal or illegal, a forecast that we often can (and do indeed) make, though with degrees of doubt.

13 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 a 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 suffer a cost (for a fine/compensation) $c_d$, while if the piece remains online, the provider will gain benefit $b_d$ (the expected additional advertising revenue to be obtained consequent to accesses to the piece of data $d$). Given this arrangement, if the provider leaves the piece online, his expected loss is $c_d{}^*p(i_d)$, 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 the piece offline, the outcome is 0, no gain and no loss. Clearly, the provider will leave the material online only when

$$b_d - (c_d * \mathrm{p}(\mathrm{i_d})) \geq 0$$

Assuming for instance that the fine/compensation will be 100, while the gain to be obtained by leaving the material online 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 online it must be that:

$$1 - (100 * \mathrm{p}(\mathrm{i_d})) \geq 0$$

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

14 I assume that belief and knowledge can come in degrees, even though I cannot enter into a discussion on the matter here, see S Haack, *Evidence and Inquiry* (Oxford: Blackwell, 1993) and Goldman (n 10).

15 Let us assume that the provider has to assess the legality of pieces of data in a set $S = L \cup I$, 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 the provider is requested to take down by the data subject. Any mistake (taking down legal material or allowing online illegal material) will have a social cost. Let $c_l$ be the average social cost of taking down a legal piece $l$ and $c_i$ the average cost of allowing an illegal piece $i$ online. Then the objective is to minimize the following social cost (the expression $|X|$ indicates the cardinality of a set $X$, namely, the number of its elements):

$$c_l{*}|\mathrm{L_{out}}| + \mathrm{c_i}{*}|\mathrm{I_{in}}|$$

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 online and taking off legal data), have on average the same cost, so that the objective becomes minimizing the following sum

$$|L_{out}| + |I_{in}|$$

Let us 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. In other words we assume that when the provider says that a piece of information is more probably legal (illegal) there is a higher chance than 50 per cent that it is legal (illegal). For simplicity's sake, let us also assume that the number of legal and illegal pieces in $S$ is the same:

$$|L| = |I|.$$

Then we get a better outcome (a lower value for $|L_{out}| + |I_{in}|$) by authorizing the provider to leave online all content he believes in good faith to be more probably legal (assuming that he acts accordingly), rather that telling him to take down all the materials he is requested to take down. We also get a better outcome in this way than by making the provider liable for every illegal material he leaves online, a choice which, as we have seen would lead him to take down all risky materials.
Assume for instance that the provider's judgement on legality or illegality is correct in 60 per cent of cases. Then the number of mistakes will be $(|L| + |I|)^*0.4)$. Given the assumption that $|L| = |I|$, this is $2L^*0.4 = L^*0.8$, which is inferior to $|L|$, the number of mistakes we will obtain if the provider were to take out all materials he is asked to remove (including pieces legally online), for fear of undergoing liability in case he were mistaken.
The model here proposed can be developed by considering the possibility that more serious damage is caused by leaving the data online 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).

notice signals the probability that it is illegal (according to the judgement of the right-holder), but the counter notice signals that it may on the contrary 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).[16]

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

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

- the alleged victim sends notice of the privacy-violating piece of content to the provider;
- the provider takes down the piece if he considered in good faith that the piece is most probably illegal, otherwise he leaves it online;
- in any case the provider informs the uploader;
- if the uploader does not respond or is anonymous, the provider takes the piece down (in case it was left online);
- if the uploader sends a counter-notice, the provider informs the victim;
- in the latter case, if the victim does not bring a lawsuit and does not involve a data protection authority, the provider puts back the piece (if it is was taken down).

This would include both parties (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 also making use of the good faith assessment of the provider.

## Providers' liability in the new regulation

Let us now address the changes that the new EU Proposal for a Data Protection Regulation[17] introduces with regard to providers' liability. First of all, we need to ask ourselves whether all doubts concerning privacy-exceptionalism (ie the idea that commerce immunity does 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'. Thus it seems that the immunities also apply to data protection, their general coverage not being limited by the Regulation.

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'. In fact, such references also include the above-mentioned Article 1 (5) (a) of the E-Commerce Directive, which might 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 also cover user-generated data involving data protection violations), and on the other hand the 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 through interpretation, namely, arguing as above that the Data Protection Directive establishes what processing is illegal, while the Directive exonerates the providers for certain illegal processing taking place

16 For instance, assume that before the lawsuit there is a very small chance that a randomly taken piece of material is illegal (eg 1 per cent). Assume also that the probability that a piece is illegal goes up to 50 per cent, in case the right-holder sends notice of a data protection violation, and that the provider has a 60 per cent chance of judging correctly when requested to determine whether a piece is legal or illegal. Under these assumptions, with regard to those pieces that are claimed to be illegal by the right-holder, we get a better outcome by relying on the provider's judgement, rather than by taking down (or leaving online) all such pieces.

However, assume that a counter notice by the uploader signals that there is an 80 per cent chances the data are legal (only those who have good grounds would react to the notice). Then it is better that the provider does not exercise his judgement with regard to the counter-noticed pieces, but leaves all the materials online. Were he to apply his judgement (which is correct in 60 per cent 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 of the provider's judgement. And so on.

17 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 C Kuner, 'The European Commission's proposed Data Protection Regulation: A Copernican revolution in European data protection law' (2012) 11 Privacy and Security Law Report 1–15. See also P De Hert and V Papaknstantinou, 'The proposed data protection regulation replacing directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 Computer Law and Security Review 130–42.

on their platforms (including those being illegal for violating data protection law).

Moving down to specific provisions, we need to consider certain rights of data subjects, which entail corresponding obligations of data controllers. Whether such obligations apply to providers neutrally processing user-generated data depends on whether such providers, when exercising this activity, can be considered as controllers.

If providers were controllers, they would be 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 to provide him or her with any 'information needed to guarantee fair processing'.[18] There is a limit to this requirement, namely 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.

## 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'.[19] The definition of this right, as it has been observed[20] fails to distinguish two kinds of user-generated personal information:

1. information about the data subject which the data subject herself has put on a provider's platform;
2. information about the data subject that other users have put on a provider's 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 neutral processing of user-generated data (processing meant to satisfy users' aims) entails that users should in principle be given the possibility of withdrawing any data they have uploaded (users should maintain full ownership of all data they upload).

The controversial aspect of this right concerns case (2), namely whether a 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 to comply with such orders only concerns controllers, the decisive point seems to be whether the provider could be considered a controller or only a processor with regard to such personal data. For instance, we may ask whether Wikipedia is a controller or a processor with regard to personal data published by Wikipedians on Wikipedia's pages.

Let us first assume that the provider is only a processor with regard to user-generated data (concerning an identifiable third party), while the user having uploaded that data is their only controller. In this case the data subject wishing the data to be erased according to Article 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 the data on the platform, facing the risk of a lawsuit. The concerned data subject could also request the provider to take down the data, but in this case, given that the provider is only a processor, the data subject could not rely on Article 17 (1). The data sub-

18 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.'

19 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.'

20 J Rosen, The right to be forgotten. (2012) 6 Stanford Law Review Online.

ject's request could only be based on the e-commerce regulation, 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).

Let us now assume, on the contrary, that providers (besides users) are also considered as controllers with regard to user-generated data concerning third parties. Then a provider would have the obligation to take down from his platform content uploaded by any users, whenever the provider is requested by the concerned data subjects, according to Article 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 a provider-controller failed to take down privacy-infringing content, not only will the provider have to compensate the damage, but he will also be subject to a severe sanction (Art. 77), as we shall see in the next section. Under such conditions, providers seem to have no choice but to remove any every content has a non-null chance of being considered illegal on data-protection grounds, 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 the 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'.[21] We need to address the case where personal data, originally uploaded to a provider's platform, have been reproduced and copies of such data have been made accessible over the Internet on the platforms of other providers (or in the servers of individual users). We distinguish again the two possible qualifications of the original provider, namely, as a processor or as a controller.

Let us first assume that the user who has uploaded other people's personal data is the only controller of such data, while the host provider is their processor. Then the obligation to contact every third party who is processing the data would only fall upon the user. To meet the request by the data subject, the user would have to contact everybody who possesses 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 initially given his consent to the publication of the data (eg to the publication of a photo) and has then changed his mind. In many cases, it may not be clear what is meant by 'data the publication of which the controller is responsible'. Assume for instance that in a blog some comments were posted concerning a person (eg, observations about a public persons' financial problems or sentimental affairs), and that similar comments are later published elsewhere on the Internet (in blogs, forums, etc.). Do these other comments contain the same data as published in the original post? Is this also the case when the same information is obtained from other sources and expressed in different ways?

Let us now assume that the host provider is also a controller with regard to other people's personal data uploaded by a user. The provider should then contact all entities hosting copies of 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) an obligation to take down the data, according to Article 17 (1). Under this interpretation, thus, the request by the data subject will start a global chase for every 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, but also links to them, which would require search providers interfering with their methods for indexing and searching.[22]

It seems to me that under both interpretations the implementation of the right to be forgotten is likely to cause uncertainties and costs, and endanger freedom of expression. The second interpretation (viewing the host provider as a controller) is likely to cause the most serious threat to freedom of expression: the request to

21 Article 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.'

22 On how interventions on search methods may have a negative impact on Internet freedoms, see M Lemley, DS Levine, and DG Post, 'Don't break the Internet' (2011) 64 Stanford Law Review Online 34.38.

take down the data would spread virally over Internet, bringing with it the obligation to 'clean' any server of the unwanted information or links to it, an obligation whose violation can be severely punished 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 legislations, even though freedom of expression is a most important fundamental right, recognized in Article 11 of the European Charter of Fundamental right as the 'freedom to hold opinions and to receive and impart information.'

Secondly, it seems that 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 organization (such as Weakileaks) would be obliged to take down any information that, while addressing social or political or social matters, mentions individual persons.[23] If the notion of journalism were limited to information concerning recent events, activities aimed at informing people about the past (eg inputting information on a Wikipedia page concerning past political scandals) would similarly become illegal as soon as the people involved are called with their names. Thus it seems that exceptions covering 'solely' journalistic and artistic/literary purposes may fail to cover the full extent of the 'right to impart information', as established on the UN Declaration of Human Rights, the European Convention of Human Rights and the EU Charter of Fundamental Rights. It is true that the case law of the European Court of Human Right (see particularly the *Steel and Morris v UK* judgment App. No. 68412/01, ECHR 15 Feb 2005) may support a broad conception of 'journalistic purposes,' but the distinction between journalism and other manifestations of freedom of expression remains highly controversial.

In Section 83 of the Regulation, there is an 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 (eg a political scandal, a crime, etc.). We may wonder whether an individual having contributed the page is a 'body' and whether the republication of other people's research outcomes would count as 'presenting research findings'. Some cases of this kind have been addressed in different ways in different jurisdictions, according to how each jurisdiction understands 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 exception based on journalism or historical research are not available.

## 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[24] 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 per cent of its annual worldwide turnover'. In addition the violator would have to compensate the damage suffered by the data subjects, according to Article 77 (1).[25]

23 On citizens' journalism on the Internet, see for instance Y Benkler, 'A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate' (2011) *Harvard Civil Rights—Civil Liberties Law Review*.

24 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.'

25 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.'

Assuming that individual uploaders would be 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, providers were also viewed as controllers, then according to Article 17 (1) the data subject could ask the host provider to remove allegedly infringing data uploaded by individual users. If 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 in 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: any sentence including persons' names would have to be deleted under request by the concerned data subjects. Thus every data subject mentioned in Wikipedia's pages could compel Wikipedia to selectively clean their pages from every statement he or she does not like. To prevent such censorial excesses, I think that providers should be exempted at least from the administrative sanctions when maintaining online illegal content while believing in good faith that such content is (possibly) 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'.

## Conclusion

It seems to me that the Regulation provides for significant progress on data protection with regard to user-generated data. While enhancing the protection of data subjects, the regulation puts online 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 online 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, user-uploaders should considered to be the only controllers.

Moreover, providers should not be liable for keeping data online when they believe in good faith that the data might be legal, and no competent authority has yet ordered its removal. This could be complemented by designing a notice and take down procedure where uploaders are also 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 sanctions for the violation of the right to be forgotten should be reconsidered with regard to both providers and individual users. In particular, the administrative sanction of Article 79 (5) should be limited to cases where the injunction of a data protection authority is disregarded, since the threat of such a serious punishment is likely to have a chilling effect on freedom of speech, forcing providers into collateral censorship.

*doi:10.1093/idpl/ips034*
*Advance Access Publication 11 December 2012*