International Journal of Law and Information Technology Vol. 18 No. 4 © Oxford University Press 2010; all rights reserved
doi:10.1093/ijlit/eaq010 Advance Access published on 24 August 2010

The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents

Giovanni Sartor and Mario Viola de Azevedo Cunha*

Abstract

In a recent decision of the Tribunal of Milan three Google executives were convicted for violating data protection law, in connection with the online posting of a video showing a disabled person being bullied and insulted. This paper, after illustrating the facts of the case and the reasoning of the judge, discusses the main issue at stake, namely, the role and responsibilities of providers of platforms for user-created contents with regard to violations of data privacy.

Keywords: privacy; data protection; freedom of speech; user-generated contents; videos; ISP liability; internet; google

1 The facts of the case

On September 8, 2006 a video was posted in Google Videos showing a disabled student being bullied and insulted by three of his colleagues (while

* Giovanni Sartor is Professor of Legal informatics and Legal Theory at the European University Institute (Florence) and Professor of Computer and Law at the University of Bologna; Mario Viola is a PhD Candidate at the Law Department of the European University Institute (Florence) and LLM in Private Law from Rio de Janeiro State University (Brazil).

another student was recording with her mobile phone, and ten more were watching the scene without intervening). More precisely the disabled student, suffering from autism and impairment in hearing and sight, was the object of both verbal and physical abuse. In particular, he was called a "mongolo" (a derogatory term used for people affected by Down syndrome) and in this connection a reference was made to the "Associazione Vivi-Down", a charity providing assistance to persons affected by the Down syndrome. The video, which had duration of about 3 minutes, was viewed by a high number of people (more than 5000 downloads). At a certain point it was the most popular one in the category of "video divertenti" (funny videos). Users of Google video posted various messages commenting on the video (starting on 4 October), apparently some flagged the video as being inappropriate and some e-mailed Google requesting for the video to be removed. However, evidence exists only for a flagging on 5 November 2006 and an email request on the following day (Google stated that it was unable to provide documentation of all comments and flaggings). On the 7th of November, the Italian Postal Police, after a communication from a citizen, requested Google to take down the video, which was removed on the same day. Thus, the video had remained available for about two months after it was initially posted.[1]

The posting of the video gave rise to three distinct lawsuits. The first concerned the four students having an active role in the video (the three abusers and the movie maker). They were identified, thanks to the information on their identities provided by Google, and were condemned by the Tribunal of Turin with a one year sentence (work in social services), for assault and slander. The second lawsuit, still pending in Turin, concerns the teacher and the school (for failing to prevent the offence). The third lawsuit, which is the one here considered, concerns Google, namely its Italian partner company (Google Italy) and its executives.

The prosecutor of Milan started criminal proceedings against four leading Google executives (David Drummond - former president of Google Italy, George De Los Reyes - former member of the board of Google Italy, Peter Fleisher – Google Privacy Counsel for Europe and Arvind Desika - head of the Google Videos Project in Europe). The charges against them were the following: criminal defamation and violation of data protection rules. With regard to defamation the indictment was of "concorso in diffamazione aggravata" (co-participation in aggravated defamation), that is of contributing to the defamation of the disabled teenager. With regard to data protection the indictment was that Google Italy was processing personal data, and in particular health data, illicitly, for the purpose of making a profit. The Vivi-Down association, the Municipality of Milan,

[1] Sentenza n. 1972/2010. Tribunale Ordinario di Milano in composizione monocratica. Sezione 4 Penale. Available at http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf (16.04.2010). P. 102/103.

and the father of the disabled student joined the proceedings as "parti civili" (parties damaged by the crime, requesting compensation), but the father later abandoned the suit. The case was decided on 24 February 2010 by the Italian Judge Oscar Magi: all four Google executives were acquitted with regard to the charge of defamation, and three of them were sentenced to a six-months suspended jail sentence for violation of data protection law.[2] The decision sparked lively reactions, also at the international level. In its blog, Google affirmed that the ruling "attacks the very principles of freedom on which the internet is built".[3] The US ambassador in Italy, David Thorne, said that he disagreed "that Internet service providers are responsible prior to posting for the content uploaded by users"[4] arguing that "free Internet is an integral human right that must be protected in free societies" (as affirmed by the US Secretary of State, Hillary Clinton).[5] Many viewed this decision as an attempt to initiate censorship in the internet, and indeed in Italy there had been discussions on the need to intervene against the publication of insults and threats against politicians and other public persons in the months preceding the Google incident (internet bloggers in particular were accused of having instigated an aggression against the Prime Minister, Silvio Berlusconi).[6] Other commentators approved the decision, finding it immoral that Google could be exempt from any liability for the damage suffered by innocent people as a consequence of Google's commercial activity (providing user-generated contents), from which it draws huge profits, in particular by collecting advertising (in 2009 USD$22 billions of advertising revenue).[7] They considered that Google had the technical means to control content and exclude offending postings, and it refrained from such controls only to cut costs (by savings on personnel) and maximize profits (by attracting the vast audience interested in prurient, lurid or offending contents). So, as one of the prosecutors, Mr. Alfredo Robledo, affirmed, the decision was not about censorship but about finding a balance between free enterprise and the protection of human dignity.[8] In the days after the decision,

[2] Sentenza n. 1972/2010. Tribunale Ordinario di Milano in composizione monocratica. Sezione 4 Penale. P. 108.

[3] The Official Google Blog. 'Serious threat to the web in Italy' (2010). Available at http://googleblog.blogspot.com/2010/02/serious-threat-to-web-in-italy.html (29.04.2010).

[4] Thorne, 'Statement by Ambassador David Thorne: Ruling in Google Court Case' (2010). Available at http://italy.usembassy.gov/viewer/article.asp?article=/file2010_02/alia/10022205.htm (29.04.2010).

[5] Donadi,. 'Larger Threat is Seen in Google Case' (2010). The New York Times. . Available at http://www.nytimes.com/2010/02/25/technology/companies/25google.html (29.04.2010).

[6] 'Berlusconi e il governo approvano il decreto per controlare internet'. Available at http://revenews.info/berlusconi-e-il-governo-approvano-il-decreto-per-controllare-internet_post10615.html (29.04.2010).

[7] Google investor relation. 2010 Financial Tables. Available at http://investor.google.com/financial/tables.html (10.05.2010).

[8] 'Caso Google: la replica della Procura' (2010). L'Espresso. Available at http://espresso.repubblica.it/dettaglio/Caso-Google-replica-la-Procura/2122058 (29.04.2010).

speculations continued, online and offline, as to the decision's possible grounds until the written opinion of the court was released, on the 12th of April, more than one month before the date it was expected. In this paper we will address the main issues considered in the decision, and we will present the reasoning of the judge before providing some general considerations.

2 The dismissed charge for defamation

Since the accused were absolved from a charge of defamation, it is sufficient to give only brief attention to this issue, just to consider the peculiar reasoning of the judge. The crime of defamation is described in Art. 595 of the Italian Criminal Code: an individual commits defamation by offending someone else's reputation in communicating with other people, and the sanction is increased when information is disseminated through the press or other media. A preliminary issue concerned the fact that defamation can only be prosecuted when there is a request (*querela*) by the offended person, and the offended student withdrew his allegations from the proceedings. However, the judge overcame this procedural hurdle by assuming that also the Vivi-Down Association and the whole category of people affected by the Down syndrome were defamed in the video, and were therefore able to request the prosecution to continue.

According to the prosecutors, the criminal liability of the Google executives for defamation did result from their failure to act: the executives had the legal obligation to prevent the defamation by exercising a preventive control over contents loaded on Google Videos site, but they had not taken such action. Given this legal obligation, their failure to take preventive measures against the uploading of offensive videos amounted to causing the defamation (according to Art. 40 of the Italian Criminal Code, failing to prevent an event which one has the legal obligation to prevent, amounts to causing it). This conclusion was reached by referring to the Italian Data Protection law: according to the prosecutors Google was no mere host provider, but rather a content provider, who had the obligation to correctly process the personal data contained in the uploaded videos and had the duty to avert those crimes that may be prevented by correctly processing the data. Since the failure to correctly process the personal data (i.e. the failure to ensure that only data that could be legally processed were uploaded and made available through the internet) caused the defamation to happen, Google executives in charge of the processing of personal data were liable for defamation.The judge responded by affirming that even though he wished that a law were issued making internet providers liable for Negligence, this had not yet been the case. Given the state of the Italian law, there was no general obligation for hosting providers to

monitor the contents of postings on their platforms.[9] Thus, he dismissed the charge for defamation: since Google had no obligation to prevent the upload of offensive materials, it was not criminally liable for defamation subsequent to the upload of such materials. The argument of the judge on this regard was confusing since on the one hand, he expressed his wish for a negligence-based liability, but on the other hand, he affirmed that monitoring each posting would be impossible, so that an obligation to this effect could not be accomplished (compliance is non-requirable, "inesigibile"). To make these statements consistent we may interpret them as follows: the judge wished for the legislator to impose an obligation on providers to take precautionary measures, which would not be so strict as to require the human examination of every single uploaded video, but would be effective to render providers liable for defamation in cases like this one. It is interesting, however, that the judge did not mention, as a ground for the non-liability of the provider, the exemption provided for by Legislative Decree nº 70 of 9 April 2003, which implemented the EU Directive on Electronic Commerce.[10] According to Art. 16 of this Legislative Decree, an information society service provider is not liable for the information stored by a recipient of the service, on the condition that "(a) the provider does not have actual knowledge of the fact that such activity or information is illicit and, as regards claims for damages, is not aware of facts or circumstances from which the illicit activity or information is apparent; or (b) upon obtaining such knowledge or awareness through the communication of the competent judicial or administrative authority, acts expeditiously to remove or to disable access to the information." Moreover, according to Art. 17 of the same decree, there is no general duty of surveillance on providers of services of transmission, caching or hosting, to monitor the information that they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. The Italian legislator issued this rules in order to implement Art. 15 of the EU Directive on Electronic Commerce, which forbids EU Member States to "impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances

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

[10] 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).

indicating illegal activity."[11] This EU regulation corresponds, with regard to non-copyright issues, to the US Communications Decency Act of 1996 (CDA), which states, in its section 230(c), that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another content provider."[12] The CDA, unlike the E-Commerce Directive, covers all circumstances, apart from copyright infringements, which are regulated by the Digital Millennium Copyright Act (DMCA).[13] It seems to us that the non-application of the exemption follows from the fact that the judge believed that the Google's activity (in providing the Google Videos service) did not fall into mere hosting, but rather consisted in providing the contents uploaded by the users. According to the judge, Google was a content-provider rather than a mere host-service provider, and, therefore, could not use this exemption.[14] As we shall see in the following, the argument is that Google provides its platform as a commercial activity, and, as part of such activity, stimulates the upload of user-created videos without any control. Thus, the inclusion and subsequent delivery of the contents have to be seen as part of the commercial activity of Google itself, and not only as activity of its users.

3 Liability under data protection law: processing health data without authorization

Let us now move to the second charge against Google, for which the executives were convicted. This is the crime of "illicit treatment of personal

[11] This seems to imply, contrary to the assumption of the judge, that "*Service providers do not have to turn into cyber patrols, at least they cannot be forced to. Article 15(1) indicates that no general obligation exists for service providers to monitor information they transmit or store. A general obligation to actively seek facts or situations indication illegal activity does not exist either. Surely, with a general obligation the exemptions of the Articles 12, 13 and 14 would not be that meaningful.*" Looder, 'Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market'. In Looder and Kaspersen (editors), *eDirectives: Guide to European Union Law on E-Commerce* (Kluwer Law International: The Hague 2002). P. 89.

[12] Available at http://www.fcc.gov/Reports/tcom1996.txt (29.04.2010).

[13] The DMCA, Title 512 "exempts ISPs from liability for hosting copyright infringing materials in a set of 'safe harbours', but only on certain terms, such as the disclosure of the identity of infringers on request, subscription to a detailed code of practice relating to notice, 'take down'and 'put back', and the banning of the identified repeat infringers from access. By contrast, section 230(C) of the Communications Decency Act (CDA) provides total immunity in respect of all kinds of liability bar that relating to IP, so long as the content in question was provided by a party other than the ISP." (Edwards. 'The Fall and Rise of Intermediary Liability Online'. In Edwards and Waelde (editors), *Law and the Internet*. 3.ed. (Hart Publishing: Oxford and Portland, Oregon 2009). P. 64.)

[14] In a case regarding MySpace, a French judge reached a similar conclusion, considering that MySpace was not a mere hoster because it profits from the videos posted by users through advertisement (T.G.I. Paris [réf.], 22 juin 2007). *See* Strowel, 'Google et les nouveaux services en ligne: quels effets sur l'économie des contenus, quels défis pour la propriété intellectuelle. In Strowel and Triaille (editors), *Google et les nouveaux services en ligne: impact sur l'économie du contenu et questions de propriété intellectuelle* (Larcier: Bruxelles 2008). P. 44-45. In another French case, regarding DailyMotion, although the court did not consider DailyMotion as a publisher or content provider, the court considered it "*liable for providing internet users with the means to commit copyright infringements*". See Edwards, 'The Fall and Rise of Intermediary Liability Online'. P. 72.

data" (*trattamento illecito dei dati*), contained in Art. 167 of the Italian Data Protection Code[15]. It is perpetrated when someone, with a view to obtaining a gain or to causing harm, processes personal data in breach of certain provisions of the same code[16]. Among the provisions whose violation constitutes this crime are Arts. 23 and 26, according to which sensitive data can only be processed when two conditions are satisfied: (a) the consent of the data subject, given in writing; and, (b) an authorisation by the Data Protection Authority, which should also indicate precautionary rules to be followed.[17] Furthermore, health data (data revealing the health condition of the data subject) are considered as sensitive data according to Art. 4 of the Code.[18] Combining these elements the crime for which the Google executives were convicted becomes apparent: with the purpose of obtaining a gain they participated in the processing of the video containing health data of the disabled teenager without his consent (or of his tutors) and also without obtaining the authorisation of the Data Protection Authority. The conviction raises a number of legal issues, which we will address in the following sub-sections:

1. Is Italian data protection law applicable?
2. Did the video contain personal data, and in particular health data?
3. Who processed the video?
4. Should Google have requested the consent of the disabled teenager in order to process his data?
5. Should Google have informed the uploaders about data protection requirements?
6. Could Google be liable under civil law (tort liability)?
7. Is Google exempted from liability as a host-service provider?
8. Is there an exemption for freedom of expression?

[15] Legislative Decree nº 196 of 30 June 2003, known as Personal Data Protection Code, which replaced both the Legislative Decree nº 171 of 13 May 1998 and the Law nº 675 of 31 December 1996. It implemented EU directives 95/46/EC and 2002/58/EC, and regulates all processing of personal data in both public and private sectors, including the internet and telecommunications.

[16] 1. Any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of Sections 18, 19, 23, 123, 126 and 130 or else of the provision made further to Section 129 shall be punished, if harm is caused, by imprisonment for between six and eighteen months or, if the offence consists in data communication or dissemination, by imprisonment for between six and twenty-four months, unless the offence is more serious.2. Any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of Sections 17, 20, 21, 22(8) and (11), 25, 26, 27, and 45 shall be punished by imprisonment for between one and three years if harm is caused, unless the offence is more serious.

[17] Sensitive data may only be processed with the data subject's written consent and the Garante's prior authorisation, by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations (Article 26(1) of the Italian Data Protection Code).

[18] Sensitive data include data able to reveal the health condition of the data subject (Article 4(1)(d) of the Italian Data Protection Code).

On the basis of the answers to these questions we shall develop some general consideration concerning the liability of providers of platforms for user-generated contents.

3.1 *Is Italian data protection law applicable?*

The judge had to address the preliminary issue pertaining to the applicable law: does Italian data protection law apply to the Google Videos data-processing, which involves activities taking place exclusively or mostly in the US? In fact, a data processing operation is subject to the Italian Data Protection Code only if one of the following conditions is satisfied:

1. The operation is performed by an entity established in Italy or
2. The operation is performed by an entity that is not established in the European Union using instruments that are located in Italy, not merely for the transit of the data in the EU territory

According to the judge, the first condition was satisfied in the case at hand, since the data processing for Google Videos was performed by Google Italy, the Italian subsidiary company of Google Inc, established in Milan. This conclusion is linked to the following assertions (though it is hard to see a clear logical connection): (a) Google Italy was the "operative and commercial hand" of Google Inc; (b) as the other subsidiaries, it was substantially a part of the group operating as a single unit, under the direction of Google Inc; (c) Google Italy had the possibility of linking advertising to the videos using the service Google AdWords. In reality, it appears that the servers for the system where located in US, where all computer processing took place, while controls on contents where performed in Ireland, through the Irish subsidiary of Google. With regard to Google AdWords, it does not seem that its use was governed by Google Italy, since links are created on the basis of the choices of the users, and the links in Google AdWords do not take people to the videos, but link the page of videos to the web-site of the advertisers. We interpret the argument of the judge as follows. Google Italy takes part in a commercial process that also includes the processing of the videos uploaded in Italy. It does so by promoting the Google Videos service and the related advertising (through Google AdWords). Thus, it can be seen as (indirectly) participating in this process, even though the servers processing the videos are located outside Italy and run by Google Inc. So, according to the judge, Google Italy was involved in the processing of the Italian videos in the US. This legal responsibility was not inapplicable on the factual basis that all decisions and controls are performed outside Italy, since this was merely a strategy adopted by Google to avoid being subject to Italian law. The way in which the issue of the applicable law is dealt in this decision seems to be one of the decision's weaknesses, and it is a pity that the judge has not explained the reasons behind his decision on this point in more detail.

In fact, the Italian Data Protection Authority has in the past considered that data processing performed by Google in the US, even with data transmitted by Italian users, was not governed by Italian law.[19]

3.2 *Did the video contain personal data, and in particular health data?*

Assuming, with the judge that the Italian Data Protection Code applies (though this is very dubious, as we have observed), we have to consider whether the conditions for a data protection crime are satisfied, namely, whether personal data have been processed in violation of a criminal norm.

First of all, we need to consider whether the video contained personal data, a question to which the judge did not devote particular attention, assuming without arguments that the video contained personal, and in particular health data, concerning the disabled student. We indeed agree with this conclusion, but will shortly discuss it since it is not obvious. It is indeed unquestionable that images (or videos) posted on the internet may contain personal data. This is the case when they represent an individual who is identifiable on the basis of the image and the further information associated to it. This was indeed the case for the disabled student in the video. The issue is whether these personal data can be considered as sensitive data, revealing the health condition of the student. The image of a person may reveal sensitive data about him or her (bodily features may indicate ethnic origin, dress may indicate religion, etc.), but it seems odd to subject to data protection requirements all such images, even when they reveal data that the subject did not intend to hide, and did necessarily or even intentionally communicate by his or her appearance (as when wearing religious or political symbols). A clue to address this issue may be found in the Article 29 Working Party's Opinion on online social networking, according to which images on the internet did not contain sensitive data "*unless the images are clearly used to reveal sensitive data about individuals.*"[20] In the case under analysis, however, we can indeed say that images did aim at revealing and spreading sensitive data about the victim, since the offenders highlighted the fact that the victim was a disabled person. Moreover, the title of the video posted (which added some extra information to the video) pointed out the information regarding the health status of

[19] See Provvedimento del 3 novembre 2009. Garante per la protezione dei dati personali. Available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1687662 (29.04.2010).

[20] Article 29 Data Protection Working Party. 'Opinion 5/2009 on online social networking'. Adopted on 12 June 2009. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf (29.03.2010). P. 8.

the victim.[21] It is true the perpetrators mis-labelled the disabled student as having Down syndrome rather than his real health condition (autism), but what mattered was the implication of disability.

3.3 *Who processed the video?*

Having established that the video contained personal health data concerning the disabled student, we have to consider whether these data were processed by Google. This may seem indeed the case, given the broad spectrum of operations listed under the heading of "processing" (*trattamento*) in the Data Protection Code: "the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank".[22]

A different view could however be held, namely, that the Videos were processed by the students uploading the video and that Google only provided the tools for such processing. It is important, hence, to distinguish the different roles of data controller and data processor. According to the Italian Data Protection Code, the former is "any natural or legal person, public administration, body, association or other entity that is competent [. . .] to determine purposes and methods of the processing of personal data and the relevant means, including security matters"[23] and the latter is "any natural or legal person, public administration, body, association or other agency that processes personal data on the controller's behalf".[24]

It seems that the students uploading the video qualify as data controllers. In fact the Italian Data Protection Code provides for an exemption from Data Protection norms for people processing data for private purposes, but the exemption does not cover the distribution (*diffusione*) of the data through unrestrictedly accessible sites: the individuals uploading other people's personal data on such sites will qualify as data controllers.[25]

[21] The UK Information Commissioner adopted a similar view regarding the processing of names and, in a certain extent, also of images: "Religion or ethnicity, or both, can often be inferred with varying degrees of certainty from dress or name. For example, many surnames are associated with a particular ethnicity or religion, or both, and may indicate the ethnicity and religion of the individuals concerned. However, it would be absurd to treat all such names as "sensitive personal data", which would mean that to hold such names on customer databases you had to satisfy a condition for processing sensitive personal data. Nevertheless, if you processed such names specifically because they indicated ethnicity or religion, for example to send marketing materials for products and services targeted at individuals of that ethnicity or religion, then you would be processing sensitive personal data." (UK Information Commissioner's Office. 'The Guide to Data Protection'. Available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.pdf (30.03.2010). P. 24.

[22] Article 4 (1)(a) of the Italian Data Protection Code.

[23] Article 4(1)(f) of the Italian Data Protection Code.

[24] Article 4(1)(g) of the Italian Data Protection Code.

[25] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971

This has been affirmed by the Article 29 Working Party in its opinion concerning online social networking: when users go beyond a purely personal or household activity (such as when they use "other technology platforms to publish personal data on the web") they become data controllers. Thus, they are subject to data protection obligations, and in particular have to collect the consent from the data subjects whose information (or images) they are making available on the internet.[26]

It remains to consider the position of Google. It may be qualified in three ways: either it only provides tools for its users, or it is a data controller jointly with the users, or it has the role of a data processor, processing the data for the users. Clearly, the judge rejected the first option and accepted that Google is either a data controller or a data processor. It may be argued that this distinction is not relevant for our purposes since both data controllers and data processors are subject to the Data Protection Code. We may however wonder whether some data protection requirements may not apply to the processor, in particular when the data controller collected the processed data. Thus, in this case it may indeed be argued that the requirement of obtaining the consent of the data subject and of asking the authorisation of the Data Protection Authority only concerns the data controller. It is clear from the provisions of the Italian Data Protection Code that the data processor should act on behalf of the controller and following the controller's instructions. So the processor's liability should pertain to the processor's choices, not to those choices that pertained to the controller. Since the controller (the students) were uploading the data concerning a third party, it should have been their responsibility to ask for consent and more generally comply with the rules pertaining to the collection of data.

3.4 *Should Google have requested the consent of the disabled teenager in order to process his data?*

On the basis of what we have just observed, the judge concluded that Google, in cooperation with the malicious students had processed health data illicitly, i.e., without the consent of the data subject. The judge however aimed at avoiding a too broad conclusion, namely, the conclusion that the provider of an internet platform commits a data protection crime whenever illicit information is posted in that platform, and in particular, whenever health information is posted without consent of the data subject. For this purpose, the judge developed two arguments. The first argument consists of observing that the obligation to request the consent

[26] Article 29 Data Protection Working Party. 'Opinion 5/2009 on online social networking'. Adopted on 12 June 2009. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf (29.03.2010). P. 6.

is not applicable to a provider when a user posts information about a third party. In fact, in order to comply with such an obligation, it would be necessary that the provider controls each image, and in case the image contains personal information (and health information in particular), the provider should refuse the image until there is evidence of consent of all individuals who are recognisable in the image, a consent that must be written when health data are at issue. Thus the judge argues that in the case of user-generated contents the provider is exonerated of the obligation to obtain consent from the data subject, since fulfilling it would be impossible (*inesigibile*). The second reason for excluding the liability of Google, which is also sketched by the judge, concerns the fact that the Google Executives could not have known that the Video had been uploaded without the consent of the data subject, and, therefore, they could not have had the required *mens rea*. To synthesise the judge's view in this regard, we may say that according to him Google did not commit a crime by not requesting the consent, since first of all it was exempted from the obligation to request it, and second, if it were not exempted, it did not have the required criminal attitude. It seems that on the basis of these considerations the judge should have concluded that there was no criminal liability for Google, and should have absolved the executives for the crime attributed to them. However, the judge found a different way to come to a positive conclusion establishing Google's liability, as we shall see in the following section.

3.5 *Should Google have informed the uploaders about data protection requirements?*

The judge grounded the criminal conviction of the Google executives on the fact that Google processed the video without taking adequate precautionary measures, to avoid privacy violations, and in particular without adequately informing the users (the students uploading the videos) of their data protection obligations (not to post illegally third party's personal information and in particular health data). It is hard to see, however, how such behaviour could be the basis for Google's criminal liability. Let us first consider the obligation to inform the Data Protection Authority. It is true that according to Art. 17, in order to process health data Google should have asked an authorisation from the Data Protection Authority, and then complied with the precautions established by that Authority. However, the precautions to be observed, under the threat of a criminal sanction, should be only those established by that authority. Thus, Google might have violated Art. 17 only for not asking an authorisation from that authority, knowing that it was likely that Google's users would upload health data about third parties. We can guess that Google did not ask for that authorisation, assuming, and wishing, that its data processing would be governed only by US law, as was also indicated to Google by the

Data Protection Authority. It seems that, even if according to the judge Google violated Art. 17, this was due to an inevitable mistake regarding Italian law (namely, the wrong assumption that processing would only be governed by US law), a mistake that, according to a famous decision of the Italian Constitutional Court (n. 364 of 1988)[27] excludes criminal liability. Let us now consider the obligation to provide information about the data processing. It is true that Art. 13 of the Data Protection Code requires that the "data subject as well as any entity from whom or which personal data are collected" should be "informed of the scope and purpose of the use of the data, and of the existing data subject's rights".[28] However, this provision is meant to provide the data subject with this information so that he or she can decide whether to provide the data and is enabled to exercise his or her access rights. This provision does not seem to be applicable to the present case, where it was clear to the uploaders how the data would be processed and accessed. It may be argued, as we shall see in the next section, that Google should have told them not to upload illegal data, but the latter duty is distinct from the criminally sanctioned obligation to inform data subjects about scopes and purposes of the data processing and on access rights.

3.6 *Could Google be liable under civil law (tort liability)?*

The exclusion of a criminal liability does not prevent Google from being liable under civil law. In fact, Art. 13 of the Italian Data Protection Code may apply, which establishes that "whoever causes damage to another as a consequence of the processing of personal data shall be liable to pay damages". This is a no-fault liability for dangerous activities, which includes also moral damages, and can only be avoided if the author of the damage shows that all measures that could prevent the damage were adopted. Thus, if it could be proved that informing the students about their obligations and liabilities would have prevented the uploading of the video, than Google could be liable. In fact, Google should indeed have provided better notice about the need to comply with data protection rules. In fact, the Article 29 Working Party has affirmed, in its opinion concerning online social networking, that the service provider should be required to

[27] Available at http://www.giurcost.org/decisioni/1988/0364s-88.html (10.05.2010).

[28] Here is the text of Art. 13: "1. The data subject as well as any entity from whom or which personal data are collected shall be preliminarily informed, either orally or in writing, as to:a) the purposes and modalities of the processing for which the data are intended;b) the obligatory or voluntary nature of providing the requested data;c) the consequences if (s)he fails to reply;d) the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data;e) the rights as per Section 7;f) the identification data concerning the data controller and, where designated, the data controller's representative in the State's territory pursuant to Section 5 and the data processor."

inform the users "about the privacy risks to themselves and to others when they upload information, (. . .) that uploading information about other individuals may impinge upon their privacy and data protection rights" and "that if they wish to upload pictures or information about other individuals, this should be done with the individual's consent."[29] It is true that Google listed, among the conditions for the use of the service, the generic requirement that uploaders should respect rights of every person, including privacy, but this reference may be considered insufficient, considering the specific privacy risks involved in distributing user-generated videos. Therefore, if a connection can be established between the failure to provide information and the uploading of the video, then Google may be responsible for torts, but this is beyond the scope of the judge's decision that only addressed criminal liability. It is not by chance that the Google executives settled an agreement with the father of the disabled teenager to compensate damages, as highlighted by the judge in his decision.[30] This would not be a liability for publishing illegal information, but for omitting certain basic precautionary measures. The obligation to inform users about data protection requirements seems compatible even with the liability exemption for host providers, since complying with this obligation does not require any censorial intervention with regard to the uploaded information.

3.7 *Is Google exempted from liability as a host-service provider?*

One of the arguments by Google's defence was that Google should not be liable, being a host service provider. To respond to this observation the judge discusses at length the appropriate legal qualification applicable to Google, and in particular whether Google Italy, as provider of the Google Videos service, is a mere host provider or a content provider. This distinction is significant with regard to the exemption from liability provided by the E-Commerce Directive (and its implementation in the Italian law), an exemption which only applies to host-service providers, namely, to providers whose servers store and make available contents that are produced, selected and uploaded by their users. In fact, according to Article 14 of the E-Commerce Directive (and of Article 16 of the respective Italian Law), the activity of host-service providers "consists of the storage of information provided by a recipient of the service." When the Directive was passed the

[29] Article 29 Data Protection Working Party. 'Opinion 5/2009 on online social networking'. Adopted on 12 June 2009. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf (29.03.2010). P. 7.

[30] In his motives, the judge refers to the settlement as evidence that a damage was suffered by the teenager (Sentenza n. 1972/2010. Tribunale Ordinario di Milano in composizione monocratica. Sezione 4 Penale. P. 91)."

phenomenon it addressed – hosting - consisted mainly in websites (html pages and related documents) uploaded by the users. The host-provider made available the server (disk-space and processor) for storing the web-site, connection from that server to the internet, and the software (the web-server) that would provide access to the website (by typing a domain name or using a search engine). Web hosting has dramatically changed in the last years: user-generated content is now uploaded into platforms that facilitate and support users in preparing content and making it available (among the most popular: i-tunes for videos, Facebook for personal information, Wordpress for Blogs, Twitter for short messages, etc.). Most platforms are run by commercial companies who make profit by associating advertisements with the user-generated materials, often (as in the case of Google) by selecting the ads on the basis of the contents of such materials. Therefore, the issue addressed by the judge is whether a provider may still be a mere host provider, when it enables uploading of content, its preparation, and its subsequent distribution, indexes such content to facilitate retrieval, and links it to advertising, and does all that for a profit. The judge's conclusion was that Google was no mere host provider; it is an "active hosting provider", and thus a content provider. As a consequence, the exclusion of liability provided by E-Commerce Law would not apply to Google Videos (and similarly, it should not apply to YouTube, Facebook, Wordpress, etc.). To support this decision the judge refers to a recent decision (decision 49437 of 2009)[31] of the Italian Court of Cassation (*Corte di Cassazione*), which has affirmed the criminal liability for violation of intellectual property of a website (the Swedish site Pirate Bay) supporting peer-to-peer exchange of digital contents. The Court of Cassation argued that by providing access through indexes to the content uploaded by users (rather than only enabling communication) the website owners would participate in the crime committed by the users. If Judge Magi's approach to the notion of a "host provider" was adopted by Italian law, it would have a broad impact on providers of platforms for user-generated contents, going beyond data protection: the clause exempting host providers from liability would not apply to platform-providers, so that they would be in principle liable for all content uploaded on their sites. To classify Google as a content provider Judge Magi considered various factors. Among them are the facts that Google actively stimulated the upload of videos, that it promoted the upload of user-generated materials without controls, in order to overcome competition from other websites, and that it actively contributed to the organisation of the videos, indexing them and linking them to advertising. This conclusion contradicts a recent decision of the European Court of Justice, preceded by an opinion of Advocate General

[31] Available at http://blog.quintarelli.it/files/cassazione-sentenza-49437-2009.pdf (29.04.2010).

Miguel Poiares Maduro,[32] which affirms that an internet service provider is exempt from liability "for the data which it has stored at the request of a recipient of that service unless that service provider, after having become aware, because of information supplied by an injured party or otherwise, of the unlawful nature of those data or of activities of that recipient, fails to act expeditiously to remove or to disable access to those data."[33] According to the Court, the exemption covers services provided at a distance, by means of electronic equipment for the processing and storage of data, at the individual request of a recipient of services, and normally in return for remuneration. Thus, the mere fact that the referencing service is subject to payment, that Google sets the payment terms or that it provides general information to its clients, cannot have the effect of depriving Google of the exemptions from liability provided for in the E-Commerce Directive. Liability may only concern, according to the Court, the order or selection of links pointing to advertisement, or text produced by Google accompanying such links. It cannot concern the user-provided content, nor its indexing, when indexing has a neutral nature, i.e., being meant to facilitate access to all the uploaded materials. It seems that, contrary to the view of Judge Magi, to identify a content provider one cannot focus on the commercial nature of the service provided, on the fact that upload and access were advertised and promoted, nor even on the fact that the service was paid. The focus must be on the connection between the provider and the information on the website, distinguishing the provider's role with regard to different kinds of information. Therefore, it may be discussed whether, given the functioning of AdWords (which we shall describe in the following), Google is a content provider with regard to certain aspects of its advertised links, but certainly it is not a content provider with regard to the videos autonomously uploaded by the users (even if the upload results from a marketing campaign by Google).

3.8 *Is there an exemption for freedom of expression?*

Neither the judge nor the parties have considered a possible exemption with regard to freedom of speech and, in particular, literary and artistic expression.[34] The temporary processing aimed at the publication and distribution of literary and artistic works is governed by Art. 137 of the

[32] Available at http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79909077C19080236&doc=T&ouvert=T&;seance=CONCL (29.04.2010).

[33] Judgment of the European Court of Justice (Grand Chamber, 23 March 2010) on Joined Cases C-236/08 to C-238/08. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008J0236:EN:HTML (29.04.2010). Paragraph 109.

[34] On freedom of expression according to Italian law, see Zeno-Zenchovich, *La liberta` di espressione. Media, mercato e potere nella società dell'informazione* (Il Mulino, Bologna, 2004).

Data Protection Code, according to which no consent by the data subject is required and no authorisation from the Data Protection Authority is needed, "for the purposes of publication or occasional circulation of articles, essays and other intellectual works also in terms of artistic expression." Thus, if the video was considered an artistic expression of thought (even though an aberrant one) the data protection crime attributed to Google would not have been committed. Obviously, the students would still have faced the charges for assault, libel and defamation, but no data protection violation would have been committed (at least by illegally processing health data). We shall not pursue this argument further, since it would require a careful consideration of various aspects, such as the different rights and values involved, the fact that the data subject was a teenager, etc. However, we hope that it may contribute to show the difficulty of the task of Google as gatekeeper of its video platform: not only would it have to control whether private or sensitive data is published, but it would also have to check whether the exemption for freedom of expression is satisfied.

4 What is missing

Let us summarise the basic legal argument of the judge. The legal (and moral fault) that the judge attributes to Google is the following: Google promoted the unrestricted and uncontrolled upload of content by users, rather than limiting itself to providing high-quality videos, as other companies did. Google knew that such a policy would have led to the upload of illegal materials, but they still adopted this policy in order to enter this segment of the market, pursuing profit. Moreover, still in order to pursue its profit, Google did not adopt precautionary measures that could have prevented the upload of illegal materials: Google did not exercise preventive control over items being uploaded, it did not establish any filter to identify potentially damaging materials and it did not inform potential uploaders that certain pieces of information (personal and in particular health data) would violate data protection and expose uploaders to legal sanctions. Thus, Google is criminally liable for the data protection crimes consisting in processing health data without the necessary precondition: informing the data subject, obtaining his or her consent, having the authorisation by the Data Protection Commissioner. It seems to us that this way of approaching the issue submitted to the judge shows not only a particular orientation in legal policy, but also a one-sided failure to understand the nature of the interests and values at issue. It is true, Google is profiting from people uploading materials on the internet. Through the activity of hundreds of thousands of users-uploaders Google obtains the availability of a huge repository of interesting materials that hundreds of millions of users-downloaders access. By indexing this materials and making it searchable, Google can extract profits from it.

This is basically done by providing the users searching for a video (or for any other kinds of information) with different kinds of outputs. On the one hand, the "natural" outcomes of the research are shown, namely, links to the videos that supposedly are more relevant to the query of the user (according to Google's search engine). These appear on the left side of the screen. On the other hand, on the right of the screen commercial advertisings are shown, related to the query. For instance if you search on YouTube (or Google Videos) for Beatles, on the left you will find links to videos of Beatles' songs available on YouTube, while on the right you will find links to TV shows, movies related to the Beatles, but also computer games and perfumes. Similarly, if you look for Glassworks, aiming at finding videos concerning this work by Philip Glass, you are going to find on the left videos of various artists performing pieces from Glassworks (with the possibility of purchasing the tracks from online stores by pushing the appropriate button), while on right you see links pointing to producers or sellers of insulating glasses, glass ceramics, glass craft, and other related items. Similarly, if you type "student" you get on the left various videos about students, mostly student-created (funny student . . ., sexy student . . ., student arrested in class, etc.) and on the right you find links to advertised courses, programs, etc.

This outcome can be explained by considering that people interested in targeted advertising can purchase AdWords from Google. This means that advertisers specify the words that should trigger their ads-links and the amount they are ready to pay when a user will click on such links. In this way they enter an auction which determines whether their ad-link is going to be listed and in what position (those offering more getting a higher position, according to the mechanism of a second-price Dutch auction). Besides that, the ranking is also determined by the quality of the ads, which is measured by Google on the basis of a number of factors, such as the ads' performance (how much they are clicked through, the relevance of the AdWords to the linked-to contents, the quality of the linked-to pages). Thus, providing a platform for video contents is certainly a commercial profit-driven process, but profit is the by-product of a user-driven activity, and (at least it is argued by Google) this activity is organized in such a way as to benefit the different categories of users involved (both commercial and non-commercial users).

The essential aspect of the platform-providing activity is that it enables user-driven uploading and advertising, for profit. It is true; Google takes advantage of it, but is this sufficient for making it liable for possible undesirable consequences of such activities (e.g., defamation, copyright infringement, violation of privacy)? There is indeed a legal saying *cuius commoda eius et incommoda*, who enjoys the benefits (*commoda*) of an activity also has to bear the inconveniences (*incommoda*) caused by that activity. Following this idea, it may be argued, as Judge Magi does, that since Google profits from the activity it enables through its platform, it should

cover the losses engendered by such activities, and possibly even be subject to criminal liability when such activities have a criminal nature.

4.1 *What commoda and incommoda?*

We need however to take a broader vision of the advantages and disadvantages related to the use of a platform like YouTube and Google Videos, a vision which takes into account individual opportunities as well as social effects. The context is indeed that of the so-called Web 2.0, namely, the recent development of the web characterized by the increased significance of user-generated contents. Here the Web is not only the infrastructure through which people can communicate, engage in economic and administrative activities, access information and cultural contents. It has also become the place where people can express themselves, construct their public images, interact with friends and acquaintances, engage in the production of knowledge, participate in culture, and contribute to social and political debate. This is performed through a number of different infrastructures and software tools, which enable new dimensions of the web: sharing content (texts, photos, videos, music, etc.), blogging, commenting, cooperative production of contents, social networking, etc. It is true, uploading content and making it accessible to everybody was already possible before the advent of the Web 2.0. Since its beginning, the internet allowed for file-sharing and e-mail based discussion groups. Creation and distribution of digital content was subsequently greatly facilitated by the development of the world-wide-web, which enabled the creation of websites of linked pages and documents. However, the platforms of the Web 2.0 represent an important advance: in combination with the increased power and availability of computer tools for individual and cooperative productivity, these platforms enormously facilitate the active participation of the users. Thanks to such platforms, hundreds of millions of amateurs (and professionals) engage and collaborate in the production of news, software, literary works, photos, movies, etc.[35] This takes place in the non-organised "crowdsourcing" of content repositories available on the web (YouTube, Google Videos, Flickr, Twitter, MySpace, Facebook, etc.): such repositories (and their section) gather separate individual contributions into collective works, whose value vastly exceeds the value of contributions they contain. More self-conscious kinds of participation in a collaborative effort are provided by open source projects for the production of software (Linux, Firefox, OpenOffice, Tex and Latex distributions, etc.), or intellectual contents (like Wikipedia). These multiple efforts are combined with emerging ways of filtering and organizing information,

[35] See Lessig, *Remix: Making Art and Commerce Thrive in the Hybrid Economy* (Penguin Press, 2008).

which build upon free individual choices, by aggregating such choices into outcomes that are relevant to others (blogs get organized into clusters around relevant hubs, individual preferences are combined into reputation ratings, user-reactions to spam contribute to filtering systems, links to web-pages are aggregated into relevance indexes)[36]. It has indeed been affirmed by Tim O' Reilly (who had a decisive role in coining the term "Web 2.0") that Web 2.0 is about harnessing collective intelligence, namely, managing, understanding, and responding to massive amounts of user-generated data.[37] According to some authors a new form of production is emerging, which may overcome some limitations of the market and of the firm, supporting human development and cooperation.[38] In this framework, web companies play a decisive role: they work for a profit, but this profit is obtained by providing opportunities to individual and groups and by aggregating and feeding back to individuals (or companies) the outcomes of individual choices, as aggregated information. While this is usually done for free, related activities generate revenues: when commercial information is provided to an individual a price is paid by the advertised company, and aggregated information resulting from individual choices may also be priced to companies (e.g. data on consumer tastes). User-generated contents are usually provided for free to the platform, although there may be cases where a reward is provided for participating in an online collection of information or menial work. In this way individual creativity, motivated by the most varied of concerns, often not inspired by commercial purposes, is combined with profit-seeking activity of web companies. This profit seeking activity is clearly self-interested, but it may still be neutral, in the sense of being oriented to enable users' action (e.g. opportunity to express oneself, to present oneself, to engage in auctions and other exchanges), and to provide relevant feedback to the same users, by organizing and aggregating user-originated information (e.g. reputation information provided in auction, ranking of sites for web searches, etc.). Therefore, the profit-driven activity of the platform providers delivers tools for individual creativity, and organizes information provided by individuals so that it becomes social knowledge, on the basis of which further services can be provided to the individuals or to commercial entities. When the "generativity of the internet"[39] is at its best, individual

[36] On the various ways in which information is provided and aggregated, see Sunstein, *Infotopia: How Many Minds Produce Knowledge* (Oxford University Press, Oxford 2006).

[37] O'Reilly, `What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software`; O'Reilly, 2005, available at http://oreilly.com/web2/archive/what-is-web-20.html (10.05.2010); O'Reilly and Battelle, `Web Squared: Web 2.0 Five Years On`; O'Reilly, 2009, available at http://assets.en.oreilly.com/1/event/28/web2009_websquared-whitepaper.pdf (10.05.2010).

[38] See in particular Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press: New Haven, Conn. 2006).

[39] See Zittrain, 'The generative internet' (1994). Harvard Law Review Vol. 119:1974-2006. P. 1993; Zittrain, *The Future of the Internet* (Yale University Press, New Haven, Conn. 2009).

contributions are supported by platforms that compete to attract users by offering a broader set of choices and opportunities for individual creativity, as well as access to relevant information. Thus, as individuals generate new contents, providers generate better services to accommodate and aggregate such contents. In this way individual needs, as well as individual and constitutional rights are satisfied (freedom of expression, communication, access to and contribution to culture, economic freedom), in an economy able to sustain and develop itself largely through self-organisation and self-regulation.

4.2 *The issue of the responsibility of the provider*

Things do not always proceed in the idyllic way we have just described. Providers themselves may take initiatives that violate the interests (and indeed the rights) of their users. They may violate the EU data protection requirements by collecting or transmitting personal data without the users' consent or in any case beyond the limits established by the law. As we observed above the issue of the application of EU data protection law to data collected in the EU and accessible from the EU, but processed outside of it requires a clarification from the EU data protection authorities and in particular by the Art. 29 Working Party. In those cases where the EU data protection law applies, providers should obviously be liable for all civil or criminal violation they commit by illegally processing personal data of their users. The case we are considering, however, pertains to a different issue, namely, to the liability of the providers for processing illicit information about third parties uploaded by their users. As we have seen above, Judge Magi, while considering Google criminally liable for not taking precautions and not informing uploaders about their liabilities, argues that the law does not require providers to have human inspection of every uploaded content, since this would be impossible to accomplish. We would argue that even if controlling all content before it is uploaded would involve huge costs on providers, this is not in principle impossible, and ways to enable a pervasive control could indeed be identified. Thus, the supposed "impossibility to control" does not adequately explain the exemption of providers from liability for user-generated contents. The reason for the exemption rather lies on the further rights and collective interests involved, namely, in the freedom-rigths of the users, and in the social benefits delivered through the unrestricted exercise of these rights. As it has often been observed, establishing provider's liability for user-generated content presupposes authorising the provider to exercise the controls that may prevent its liability, i.e., empowering it to exclude all those contents that might generate liability. The provider would then become the gatekeeper of the internet, exercising a preventive and proactive control over the distribution of user-generated content. Any potentially controversial information would then likely be prevented

from reaching public accessibility. In particular, any user-generated information concerning third parties would likely be blocked by the concerned provider, fearing incrimination of criminal or civil liability for violation of data protection (or intellectual property). Users' freedom to express their views and to participate in the creation of culture would suffer unacceptable constrains, and similarly, the generativity of the internet would be compromised.[40]

As we have observed above, EU laws (as well as US laws[41]) have found a reasonable way of balancing internet freedoms and the protection of third parties by a two tiered framework: platform providers are exempted from liability for illegal user-generated content, but the exemption does not apply if the provider was informed of the illegality and failed to take action. It has been argued that this model should apply also to data privacy, in order to achieve an appropriate balance between privacy and freedom of expression.[42] In Europe it may be wondered whether this model concerns also to data protection, given that the EU Directive explicitily states that the providers' limitations do not affect data protection. We think that platform providers should indeed be fully liable (no exemption) when processing users-data they have requested or extracted from the users' online activity (this information should indeed be subject to the usual data protection requirements); on the contrary, they should be exempted when processing content uploaded by the users. Providers indexing and delivering user-generated content do not play the role of data controllers; they are rather processors giving effect to the requests of their users (and this should indeed be the providers' role, if the users' free choices are to be respected). We think that it would be important to remove the present uncertainty concerning the application of data protection rules to host providers, hopefully in the liberal direction we have suggested. Italian law shows a particular attention for the need to prevent the providers' preventive censorship: improving upon the EU Directive (which requires providers to remove content they know to be illegitimate), Italian law makes the exemption inapplicable only when the provider fails to remove illegitimate content after having been asked by a judicial or administrative authority or fails to inform such an authority after having known that illegitimate content has been uploaded.[43] In the present case Google complied with the regulation of providers' liability, by removing the video when requested by the Italian police. Moreover, it had earlier complied with police by providing

[40] For a discussion of free-speech issues involved in the regulation of providers' liability, see Balkin 'The Future of Free Expression in a Digital Age' (2008). Pepperdine Law Review, Vol. 36: 101-18.

[41] Albeit that the CDA provides for complete immunity.

[42] Solove, *The Future of Reputation* (Yale University Press: New Haven, Conn. 2008).

[43] On the liability of internet service providers according to Italian law, see Pagallo, 'Sul principio di responsabilità giuridica in rete' (2009), Il Diritto dell'informazione e dell'informatica, Vol 25: 705-34.

the information that enabled the students uploading the video to be identified and charged with the crimes they had committed (assault and libel). Finally, as we observed above, the fact that a provider acts for a profit does not exclude the applicability of the liability-exemption, as long as the profit is an effect of enabling and facilitating users' activity. This has been affirmed in the above-mentioned decision of the European Court of Justice, according to which the hosting exemption applies even when the provider displays paid advertising links, as long as the content of the advertising is established by the users. On the other hand, the exemption fails to cover providers whose action goes beyond the "natural function" of the platform, namely, beyond enabling and supporting the user's activities (uploading, searching for relevant contents, advertising): providers are fully liable when they generate the content or skew the functioning of the platform toward their particular interests (in the detriment of neutrality). As long as the provider's profit is achieved by enabling the user, there is no conflict between search for profit and provider's exemption.

5 Conclusion

It seems to us that the decision of the Italian judge is defective in various regards. First of all, it fails to address some of the fundamental prerequisites of criminal liability, namely, establishing the applicability of Italian criminal law, and determining whether the required *mens rea* existed in this case. Secondly, it fails to provide a precise analysis of why Google's omission to inform users about privacy law would qualify as a failure to inform data subjects about the processing of their data. Thirdly and most important, it fails to conceptualise the role of platforms providers in the context of the web 2.0, and their enabling function with regard to user-driven generation of contents. Contrary to the opinion of the judge, it seems to us that even with regard to the violations of data protection, the current rules limiting the liability of host providers with regard to the contents published in their web sites would give the most appropriate balance between the interests and the rights involved in cases like the one here presented. These considerations do not exclude the need that providers take some initiatives concerning the education of their users with regard to data protection. In particular, platform providers should be urged (by the competent data protection authorities) to provide their users with better information about the need that other people's privacy rights are respected, as suggested by the Article 29 Working Party. We think that such precautions would be fully consistent with the limitation of the provider's liability since they do not impose any censorship on users, but are only meant to make them aware of their pre-existing data protection duties.