The Flow of Personal Data on the Internet: The Italian and European Google Cases*

Francesco Giacomo Viterbo**

Abstract

The recent judgement of the European Court of Justice of 13 May 2014 (hereinafter: the Judgement) focused on the activity of the Google platform as a provider of indexed content, including personal data; this activity consists of locating information published on the web by third parties, indexing it automatically, storing it temporarily, and finally, making it available to internet users according to a particular order of preference. The Court has stated that these operations must be classified as 'processing' (within the meaning of Directive 95/46), and are activities that can be distinguished from and are additional to the activities carried out by publishers of websites, and have additional effects on the data subject's fundamental rights. This means that, especially in an online environment, the types of data processing, as well as the rules to be applied are becoming more diversified, even when considering the rights that can be exercised by data subjects. The key question to be answered is therefore not *whether*, but *how* data protection principles and rules have to be applied in each specific case.

This can be illustrated by the measures set forth by the Italian *Garante per la protezione dei dati personali* (hereinafter: the *Garante*) in order to bring the processing of personal data carried out under Google's new privacy policy into line with the Italian Data Protection Code. These measures tackle the problem of applying 'criteria for making data processing legitimate' and 'principles relating to data quality' on the internet, and focus on the legal requirements for the data subject's prior consent with respect to a wide array of features offered to its users. It is exactly on this ground that one point of connection between the Data Protection Directive and the e-Privacy Directive will be analysed. The measures seem to emphasise the role of data subjects' consent in the area of marketing and behavioural advertising, where there is

* Case C-131/12 *Google Spain SL, Google Inc.* v *Agencia Española de Protección de Datos (Aepd), M. Costeja González* (European Court of Justice Grand Chamber 13 May 2014); Autorità Garante per la protezione dei dati personali, 10 July 2014 'Decision Setting Forth Measures Google Inc. is Required to Take to Bring the Processing of Personal Data under Google's New Privacy Policy into Line with the Italian Data Protection Code'.

** Associate Professor of Private Law at the University of Salento.

no room for contractual agreements. Nonetheless freedom of contract within the scope of personal data protection does not seem to be ruled out. In this context, personal data are not negotiable goods and cannot be treated in the same way as any other kind of tradable commodity.

I. The Case of Google/Aepd, M. Costeja González on the Processing of Personal Information in the Online Environment: Introductory Remarks

The recent case of *Google/Aepd, M. Costeja González* is a break with the past in that the European Court of Justice (CJEU) has established the legal approach to be followed for the protection of

[1] Case C-131/12 *Google Spain SL, Google Inc.* v *Agencia Española de Protección de Datos (Aepd), M. Costeja González* (European Court of Justice Grand Chamber 13 May 2014), available at www.eur-lex.europa.eu, and in *Computer Law Review International,* 77 (2014). This judgement has been implemented by the Data Protection Authorities represented in the Data Protection Working Party (WP 29) through the publication of the following document: 'Guidelines on the implementation of the Court of Justice of the European Union Judgement on 'Google Spain and Inc. v. Agencia Española de Protección de Datos (Aepd) and Mario Costeja González' C-131/12', adopted on 26 November 2014. In Italy the Judgement has been followed by the 'Decision Setting Forth Measures Google Inc. is Required to Take to Bring the Processing of Personal Data under Google's New Privacy Policy into Line with the Italian Data Protection Code' adopted by Autorità Garante per la Protezione dei Dati Personali 10 July 2014, available at www.garanteprivacy.it (document web no 3295641). The Judgement has raised a 'global' debate on the mentioned legal issues: see M. Schmidt-Kessel, C. Langhanke and I. Gläser, 'Recht auf Vergessen und piercing the corporate veil-zugleich Anmerkungen zur Google-Entscheidung des EuGH, Rs. C-131/12 Google Spain SL und Google Inc.' *Zeitschrift für Gemeinschaftsprivatrecht*, 192-197 (2014); P. De Hert and V. Papakonstantinou, 'How the European Google Decision May Have Nothing to Do with a Right to Be Forgotten', available at https://www.privacyassociation.org/privacy_perspectives/post/how_the_european_google_decision_may_have_nothing_to_do_with_a_right_to_be (last visited 20 October 2015); C. Kuner, 'The Court of Justice of EU's Judgement on the 'Right to be Forgotten': An International Perspective', available at http://www.ejiltalk.org/the-court-of-justice-of-eus-judgment-on-the-right-to-be-forgotten-an-international-perspective/ (last visited 20 October 2015); J.W. Kropf, 'Google Spain SL v. Agencia Española de Protección de Datos (AEPD). Case C-131/12' 108 *The American Journal of International Law*, 502-509 (2014); O. Linskey, 'Control over Personal Data in a Digital Age: *Google Spain* v *AEPD and Mario Costeja Gonzalez*' 78 *Modern Law Review*, 522-534 (2015); in Italy, see G. Resta and V. Zeno Zencovich eds, *Il diritto*

personal data in the online environment.[1] This case typifies the main challenges posed by the flow of personal information on the internet. It may be summarised as follows.

A Spanish citizen, Mr Costeja González, lodged a complaint with the data protection supervisory authority (Aepd) against a company that publishes a daily newspaper with a large circulation and against Google Spain and Google Inc. Mr Costeja González explained that if an internet user entered his name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of that newspaper, published many years earlier, on which an announcement mentioning his name had appeared for a real estate auction connected with attachment proceedings for the recovery of social security debts. He stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years, and that reference to them now was entirely irrelevant. Therefore he requested, first, that the publisher of newspaper be required to remove or alter those pages so that the personal data relating to him no longer appeared, or to use certain tools in order to protect the data. Second, he requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that these data ceased to be included in the search results.

It is well known that, generally speaking, search engines are services that help their users to find information on the web.[2] However, in the context of the so-called Web 2.0, search engines are only one facet of a much more complex environment that every day creates an infinite number of threats to the fundamental rights of individuals. Indeed the relationships between providers and users have become more and more complex, and need to be better analysed.

First, most content available online is user-generated: this potentially means that all users of the internet may participate in 'writing' the web.[3]

all'oblio su internet dopo la sentenza Google Spain (Roma: Roma TrE-Press, 2015), 1-281.

[2] For a more detailed definition of a 'search engine', see Data Protection Working Party (WP 29), Opinion 1/2008 on data protection issues related to search engines, adopted on 4 April 2008, para 2, available at http://ec.europa.eu/.

[3] M. Viola de Azevedo Cunha, L. Marin and G. Sartor, 'Peer-to-peer Privacy Violation and ISP Liability: Data Protection in the User-generated Web' 2 *International Data Privacy Law*, 50 (2012).

The evolution of web communities and hosted services such as social network services ('SNS') is a relatively recent phenomenon. SNS are information society services (as defined in Art 1 para 2 of Directive 1998/34/EC as amended by Directive 1998/48/EC), which can broadly be defined as online communication platforms that enable individuals to join or create networks of like-minded users. They provide tools that allow users to post their own material, including personal data, for the purpose of generating a description or 'profile' of themselves (user-generated content, such as a photograph or a diary entry, music or video clip or links to other sites), and provide a list of contacts for each user with which the user can interact.[4] In many cases, individuals' profiles can be found by everyone through search engines if they are not protected against this.

The advent of social media has given everyone a number of platforms on which it is possible to create content, as well to find and disclose personal information on a large and permanent scale. Google offers a wide array of features to its users, ranging from a web search engine (Google Search) to email (Gmail); from online mapping (Street View on Google Maps) to the marketing of advertising space (DoubleClick); from a browser (Google Chrome) to social networking (Google +); from online payment services (Google Wallet) to a virtual store for purchasing apps, music, movies, books and magazines (Google Play); from services allowing users to search for, display and post videos (YouTube) to text storage, sharing and revision services (Google Docs and Google Drive); from satellite imaging software (Google Earth) to statistical analysis and monitoring tools to study website visitors (Google Analytics); and so on. Among the other most popular platforms used worldwide we can name Facebook for personal information, Wordpress for blogs, Twitter for short messages, e-Bay for auctions; this list is far from being exhaustive.[5] Information that in the past would not have been

[4] For more details, see Data Protection Working Party (WP 29), Opinion 05/2009 on online social networking, adopted on 12 June 2009, paras 1-2, available at http://ec.europa.eu/. For more details on the issues related to relationships between social networks and users as a field for applying the civil law, see C. Perlingieri, *Profili civilistici dei social networks* (Napoli: Edizioni Scientifiche Italiane, 2014), 11-105.

[5] M. Viola de Azevedo Cunha, L. Marin and G. Sartor, n 3 above, 51.

published in the mass media may now feature on social media, thereby creating 'news' that may then be taken up and more broadly disseminated by the traditional media. Likewise, the activity of search engines and of the other online platforms plays a decisive role in the overall dissemination of such information, in that it renders it accessible to any internet user who makes a search on the basis of the data subject's name, including internet users who would not otherwise have found the news published on a web page or by the traditional media. This has created an interdependent relationship between social media and the mass media; the barriers between them are breaking down.[6]

Furthermore, the digitization of modern communications makes it possible for governments, private corporations and individuals to collect vast amounts of personal data around the globe. Corporations are keen to use the same or similar technologies to gauge consumer habits, with the objective of personalising advertising, and in doing this they manage a huge amount of personal data.

Needless to say, online services are often provided 'free' in exchange for a user's personal data. Meanwhile, the providers of those services do not merely allow or give access to content hosted on the online platform, but take advantage of these activities, in return for payment, by, for example, allowing advertising to carried out by undertakings who wish to use this tool in order to offer their goods or services to the internet users, in such a way that advertising is tailored to each available user-profile. Likewise, SNS generate much of their revenue through advertising, which appears alongside the web pages that are set up and accessed by users. Therefore, the platforms mentioned above such as Google Search are mostly run by commercial companies who usually make a profit by associating advertisements with both the internet users' search terms and the user-generated materials, often by selecting the ads on the basis of

[6] N. Witzleb, D. Lindsay et al, 'An Overview of Emerging Challenges in Privacy Law', in N. Witzleb, D. Lindsay et al eds, *Emerging Challenges in Privacy Law* (Cambridge: Cambridge University Press, 2014), 3. The creation of search engines has carried out a further ground where information and data circulate, which was previously unknown: A. Mantelero, 'Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy', in G. Resta and V. Zeno Zencovich eds, n 1 above, 135.

the content of such material: users who post large amounts of information about their interests on their profiles offer a refined market to advertisers who wish to serve targeted advertisements based on that information.

Along with this economic interest pursued by Web 2.0 operators behaving as profit-seeking private companies, a paramount importance has to be attached to the function of the internet in society, ie the public interest in sharing and networking knowledge, news and any kind of information available on the World Wide Web. Nowadays, it is generally acknowledged that 'the web has become a forum where everyone can effectively exercise their civil, economical, and political rights' and that 'it is the place where one can develop one's social personality'.[7] Moreover, the recent 'Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to human rights for Internet users', adopted on 16 April 2014 at the one-thousand one-hundred ninety-seventh meeting of the Ministers' Deputies, has declared that the 'Internet has a public service value' and that 'People, communities, public authorities and private entities rely on the Internet for their activities and have a legitimate expectation that its services are accessible, provided without discrimination, affordable, secure, reliable and ongoing'.[8] This certainly justifies the legitimate interest of individuals in having access to the online environment, as the CJEU stated in para 81 of the Judgement. Much more doubtful is whether the fundamental right of freedom of expression, understood as 'the freedom to receive and impart information and ideas', in Art 11 of the European Charter of Fundamental Rights, may also be a legitimate basis for having access to all information published on the web, as well as for processing personal data in any circumstances.[9]

[7] M. Viola de Azevedo Cunha, L. Marin and G. Sartor, n 3 above, 51. On the 'generativity' of the internet, see J. Zittrain, 'The Generative Internet' 119 *Harvard Law Review*, 1974-2040 (2006).

[8] See para 3 of the document, available at https://wcd.coe.int/ViewDoc.jsp?id=2184807 (last visited 20 October 2015).

[9] 'The Court emphasizes the right of individuals to remove their personal data from the results generated by search engines, but barely mentions the right to freedom of expression, and never refers at all to Art 11 of the Charter of Fundamental Rights. It also states (para 81) that the right to data protection generally overrides the interest of the general public in finding information relating to a data subject's

II. The Issue of Personal Data Protection in the Online Environment: Four Problematic Aspects

The issue of personal data protection in the online environment raises a number of problematic aspects regarding the safeguards of fundamental rights of individuals.

First, given that user-generated content often concerns third parties, and content providers (eg search engines) help to make publications on the internet easily accessible to a worldwide audience, the production and distribution of user-generated content on the web may even be socially dangerous – we may consider, for instance, defamation, violations of copyright, participation in criminal activities, offences against the dignity of the weak and so forth. *Inter alia*, the online distribution of user-generated content disclosing third parties' personal information can amount to a violation of data protection rights, as well of the right to respect for private and family life and of other fundamental rights, since it may take place outside the conditions laid down in data protection legislation.[10] A good illustration of this is the Italian case of *Google/ Vivi Down*, which concerned a group of teenagers who recorded themselves insulting and physically assaulting an autistic boy;[11] the video, despite its sensitive content, was uploaded onto the Google-

name, while at the same time stating that the balance between the two must depend on the specific case at issue': C. Kuner, n 1 above.

[10] M. Viola de Azevedo Cunha, L. Marin and G. Sartor, n 3 above, 51-52.

[11] Tribunale di Milano 12 April 2010 no 1972, *Foro italiano*, II, 279 (2010), which sentenced three Google executives to six months' imprisonment for the violation of Art 167(1)(2) of decreto legislativo 30 June 2003 no 196 (Personal Data Protection Code, hereinafter: the Code); however the sentence has been overruled by the judgement of the Corte di Appello di Milano, Sezione Penale, I, 27 February 2013 no 8611, *Foro italiano*, II, 593 (2013), which has in turn been upheld by the Corte di Cassazione 17 December 2013 no 5107, *Giurisprudenza italiana*, 2016 (2014). For particularly detailed analyses, 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' *International Journal of Law and Information Technology*, 15 (2010); R. Mendez, 'Google Case in Italy' *International Data Privacy Law*, 137 (2011); N.C.N. Hampson, 'The Internet is not a Lawless Prairie: Data Protection and Privacy in Italy' *Boston College International and Comparative Law Review*, 477 (2011); G. Cassano, 'Google v. Vividown. Responsabilità 'assolute' e fine di internet?' *Vita notarile*, 2 (2010); and G. Resta, 'Diritti individuali e libertà della rete nel caso Vivi Down' *Giurisprudenza di merito*, 1577 (2013).

Videos platform by a user, with the obvious consequence of shamefully violating the privacy and dignity of that boy.[12]

Second, the personal information posted online by a user, which is frequently done on social networks, can create a rich profile concerning that person's interests and activities. Furthermore, according to para 37 of the Judgement, 'the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users' access to that information may, when users carry out their search on the basis of an individual's name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject'. Personal data published on social network sites and then stored and indexed by search engines can be used by third parties for a wide variety of purposes, including unlawful purposes, which may put the fundamental rights of data subjects at great risk because of such problems as identity theft, financial loss, discrimination and other violations of their dignity.[13]

Third, according to the analysis of the CJEU, the effect of the interference with those fundamental rights of the data subject is heightened because of the important role played by the internet and search engines in modern society, which render the information contained in this environment 'ubiquitous'.[14] This makes the exercise of the right to ask for personal information to be deleted or removed from the web, ie the so-called 'right to be forgotten' (or 'right to oblivion') much more difficult.[15]

[12] Google-Videos was an online service provided by Google Inc. It was a platform on which users could upload and share videos at any time at no charge. This service has recently been incorporated into the platform provided by YouTube which has been purchased by Google Inc.

[13] See Data Protection Working Party (WP 29), n 4 above, para 1.

[14] See the para 80 of the Judgement.

[15] For more details, see European Commission, 'Factsheet on the 'Right to be Forgotten' ruling (C-131/12)', 3 June 2014, available at http://ec.europa.eu/justice/newsroom/data-protection/news/140602_en.htm (last visited 20 October 2015). It is possible to note that the case at issue may not even be concerned with the right to be forgotten. As already explained, a 'right to be forgotten' would essentially include a 'right to delete' or 'to have deleted', but this is not what the Judgement does. It did

Fourth, most of the online operators, in their role as service providers, collect and process vast amounts of user data, including IP addresses, detailed reports of past online behaviour and personal data provided by users themselves when signing up to use personalised services.[16]

With this background, it is time to focus on the current debate on the application of Directive 95/46 which, according to Art 1, has the object of protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and of removing obstacles to the free flow of such data. But before discussing *whether* data protection legislation may be applied, it is necessary to distinguish between two significant categories of subjects who are involved in the complex environment of the internet.

On the one hand, at least two subsets of subjects operating in the online environment can be identified: service providers and content providers. On the other hand, we can consider the legal position of users and third parties, namely both individuals who need personal data protection (data subjects), and advertisers, ie undertakings who ask for a contract with providers in order to use the web as a platform on which to offer their goods or services.

Although a wide variety of services and content are provided in the online environment, the scope of this paper will cover the activities of search engine providers, as well as those of other intermediary service providers, with the aim of assessing the extent

not ask for the deletion of the information from the original source: P. De Hert and V. Papakonstantinou, n 1 above. Furthermore, the original information will still be accessible using other search terms or by direct access to the publisher's original source: see the Working Party 'Guidelines' adopted on 26 November 2014, n 1 above, 2. In the opinion of many scholars, the right to be forgotten represents the biggest threat to free speech on the Internet in the coming decade. It 'could make Facebook and Google, for example, liable for up to two percent of their global income if they fail to remove photos that people post about themselves and later regret, even if the photos have been widely distributed already': J. Rosen, 'The Right to Be Forgotten' 64 *Stanford Law Review Online*, 88 (2012). In the recent Italian debate, see G. Finocchiaro, 'Il diritto all'oblio nel quadro dei diritti della personalità', in G. Resta and V. Zeno Zencovich eds, n 1 above, 29-42; and S. Rodotà, *Il diritto di avere diritti* (Roma-Bari: Laterza, 2012), 213-221.

[16] See Data Protection Working Party (WP 29), Opinion 1/2008 on data protection issues related to search engines, para 1.

of their obligations under Directive 1995/46, as well as the entitlements of users playing the role of data subjects.[17] The following analysis will not focus on third party advertisers, for whom the application of data protection law does not seem to be disputed.

III. The Issue of *Whether* the Data Protection Directive Applies to Service/Content Providers. Two Key Arguments: the Definition of 'Processing of Personal Data' and the Effectiveness of Protection

Before the Judgement, Opinions 1/2008 and 05/2009 adopted by Data Protection Working Party clarified the cases in which the issues related to the application of Directive 1995/46 seem to be less problematic.

It is interesting to note that a 'key conclusion' of both these Opinions was that the Data Protection Directive generally applies to the processing of personal data by both search engines and SNS providers, even when their headquarters are outside the European Environment Agency (EEA).[18] According to this analysis, the combined effect of Arts 4(1)(a) and 4(1)(c) of the Data Protection Directive is that its provisions apply to the processing of personal data by search engine providers and by SNS providers, in both cases when they are multinationals, and even when they do not have an establishment in the territory of a Member State.[19] In this case it can be sufficient that

[17] Users may be distinguished according to whether they hold an account that has been created following registration for 'authenticated' access to Google's features – these being the so-called 'authenticated users' – or hold an account under which they use those features without having first authenticated themselves – these being the so-called 'non-authenticated users'; there is an additional group of users, ie the so-called 'passive users', whose data may be acquired by the provider although they do not use its features directly: see para 1 of the 'Decision Setting Forth Measures Google Inc. is Required to Take to Bring the Processing of Personal Data under Google's New Privacy Policy into Line with the Italian Data Protection Code' adopted by Autorità Garante per la Protezione dei Dati Personali 10 July 2014, n 1 above.

[18] See point no 1 of para 5 of Opinion 05/2009 on online social networking, and para 4.1.2 of Opinion 1/2008 on data protection issues related to search engines.

[19] Art 4(1)(a) states that a Member State's data protection law should be applied when certain operations of personal data processing by the controller are carried out 'in the context of the activities of an establishment' of that controller on the territory

the provider makes use of equipment, automated or otherwise, in the territory of a Member State (for example, it makes use of a cookie or similar software device) for the purpose of processing personal data, in order that the data protection law of that Member State should apply.

From this perspective the Working Party has confirmed that a provider who processes user data, including IP addresses and/or persistent cookies containing a unique identifier, falls within the scope of the definition of 'controller' under the Directive. This conclusion is related to both search engine providers and SNS providers in their role as service providers when they are collecting and processing vast amounts of data concerning users and even third parties, on their own initiative, and it means that they have corresponding responsibilities towards data subjects.[20] When they are required to do so, they provide all the 'basic' services related to user management (eg the registration and deletion of accounts), and they also determine the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties. Therefore, in the view of the Working Party, data protection law should generally apply in relation to the processing of user data by service providers.

According to Opinion 1/2008, a different approach would be required for cases in which online service providers fulfil their role as 'content providers' (or 'web hosting providers'). This occurs, for instance, when search engines process information, including personal information, by crawling, analysing and indexing the World Wide Web and other sources of user-generated content that they make searchable and therefore easily accessible through these

of a Member State. Art 4(1)(c) states that a Member State's data protection law still applies where 'the controller [...] for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community'. See also the 'Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites', adopted on 30 May 2002 by the Data Protection Working Party.

[20] See para 3.1 and point no 2 of para 5, of Opinion 05/2009 on online social networking; see para 4.1.2 of Opinion 1/2008 on data protection issues related to search engines.

services.[21] In this regard the Working Party remarks that the Data Protection Directive does not contain a special reference to the processing of personal data by 'information society services that act as selection intermediaries'.[22]

This explains why there is an ongoing debate over whether and to what extent the Personal Data Protection law may apply to the activity of such intermediaries, as well over whether and to what extent they should be liable for illegal user-generated content. However, the debate only comes to a focus on the former question, which seems to be separate from the latter, although the two issues continue to affect each other.

Indeed, according to some scholars, the liability exemptions for service providers provided by Art 14(a)(b) of the e-Commerce Directive (2000/31/EC) with regard to content generated by users should also apply to violations of the Personal Data Protection law.[23] The rationale for such an interpretation would be the principle of neutrality, which is connected with the aforementioned pivotal role played by internet service providers (ISPs) in our information society, if we consider, for instance, that search engines play a crucial role as a first point of contact for accessing information freely on the internet. In this case, the principal controllers of personal data would be the 'information providers', ie the users who have uploaded

[21] See para 4.2 of Opinion 1/2008 on data protection issues related to search engines. See also M. Viola de Azevedo Cunha, L. Marin and G. Sartor, n 3 above, 58.

[22] See para 4.2.2 of Opinion 1/2008 on data protection issues related to search engines.

[23] See both G. Sartor, 'Search Engines as Controllers: Inconvenient Implications of a Questionable Classification. Case C-131/12, Google Spain and Google Inc. v. AEPD et Costeja Gonzalez' 21 *Maastricht Journal of European and Comparative Law*, 564-575 (2014); and M. Viola de Azevedo Cunha, L. Marin and G. Sartor, n 3 above, 66: 'it seems to us that even with regard to third parties' data protection, the current rules limiting the liability of host providers with regard to user-generated content give the most appropriate balance between the interests and the rights involved'. Art 14 of Directive 2000/31, entitled 'Hosting', provides 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'.

content, including the personal data of third parties, inasmuch as the search engine provider, acting as an intermediary, cannot have practical control over the personal data involved, and the scope of its intervention is limited to the possibility of removing the data from its servers.[24] From this perspective, Directive 95/46 should only apply to users whenever they go beyond a 'purely personal or household activity'.[25] This is illustrated by the landmark *Lindqvist* case of 2003, in which the CJEU stated that the Data Protection Directive applied to the activity of a Swedish catechist who posted on web pages, on her own initiative, information, including sensitive data, about herself and some other parishioner-catechists.[26] In this judgement the Court did not intend the expression 'transfer of data to third countries' to cover the loading, by an individual in the territory of a Member State, of data onto an internet page. Such reasoning of the Court was taken into consideration by Advocate General Jääskinen in the case at issue in order to argue that the internet search engine service provider cannot be generally considered as having the position of data controller.[27] In this view, a national data protection authority could not require an internet search engine service provider to withdraw information from its index except for the cases in which this service provider has not complied with the exclusion codes on a web page or in which a request emanating from the website regarding an update of cache memory has not been complied with.[28]

[24] M. Viola de Azevedo Cunha, L. Marin and G. Sartor, n 3 above, 66.

[25] Directive 95/46 does not apply to the processing of personal data 'by a natural person in the course of a purely personal or household activity', pursuant to Art 3(2). In its Opinion 05/2009 on online social networking, the Working Party has affirmed that when users go beyond a purely personal or household activity they become data controllers. In this case they are subject to data protection obligations, and in particular they have to collect the consent from the data subjects whose information (or images) they are making available on the web.

[26] Case C-101/01 *Gota Hovratt* v *Bodil Lindqvist* (European Court of Justice 6 November 2003) available at www.eur-lex.europa.eu; for a particularly detailed analysis see T.M. Ubertazzi, 'Sul bilanciamento tra libertà di espressione e privacy' *Danno e responsabilità*, 386 (2004).

[27] Case C-131/12 *Google Spain SL, Google Inc.* v *Agencia Española de Protección de Datos (Aepd), M. Costeja González*, Opinion of Mr Advocate General Jääskinen delivered on 25 June 2013, n 1 above, paras 79, 84 and 89.

[28] See ibid paras 93 and 99.

Using a completely different approach towards the issue of ISP liability for illegal user-generated content, it is possible to note that a search engine provider, when operating as an 'intermediary service provider', may become jointly responsible for violations of privacy and of data protection rules committed by users, insofar as it supplies the means through which the violations are committed, by making the information ubiquitous and searchable; furthermore it does that for a profit. Therefore both the service provider and the user could be considered as data controllers, and the Personal Data Protection Directive could apply to them both. However, from a rather different perspective, which became dominant with the leading case of *Vuitton* v *Google* of 2010, such a conclusion would be possible only when the service provider does not limit itself to an intermediary role, so only when it has played an active role of a kind that gives it knowledge of, or control over, the personal data.[29] Indeed, according to what the CJEU says in para 114 of that judgement with regard to the application of the liability exemptions in Art 14 of the e-Commerce Directive, it would be necessary to examine whether the role played by the service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, or active, pointing to a knowledge or control of the data that it stores. In the latter case those exemptions would not be applicable to the service provider, and its liability could be based on a violation of the Data Protection law.

It is interesting to note that all the foregoing approaches entail the application of the Data Protection Directive whenever personal data are processed in an online environment that is enjoyed by European users. This occurs even when it comes to applying the provisions under which the Directive itself limits the scope of its application. Therefore the question debated seems to be not *whether* such Directive rules have to be applied, but rather *how* they should be applied, namely to establish, for example, who is the data controller, what measures should be taken to protect data subjects, and so forth.

Likewise, in the Judgement the CJEU stated that the operation of

[29] Joined Cases C-236/08 and C-238/08 *Google* v *Louis Vuitton* (European Court of Justice Grand Chamber 23 March 2010) available at www.eur-lex.europa.eu: the question faced in this judgement concerns the liability of Google Inc. as a referencing service provider.

loading personal data onto an internet page must be considered to be a 'processing of personal data' within the meaning of Art 2(b) of Directive 95/46. In spite of the opinion delivered by the Advocate General, this is true even when the operation is carried out by a search engine provider that, in exploring the internet automatically, constantly and systematically in search of the information that is published there, 'collects' such data, which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers, and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results.[30] Furthermore, the Court has specified that this activity falls within the scope of the Directive whenever it is orientated towards the inhabitants of a Member State in which the provider has set up a branch or subsidiary through which it intends to promote and sell advertising space.[31]

The Judgement represents a real break with the past inasmuch as the CJEU focuses the rationale of its interpretation of the legal framework concerning the processing of personal data in the web context on the fundamental principles and values set out in the Nice Charter as well the current EU Treaties. Indeed, the Court remarks that the notion of 'establishment', within the meaning of Art 4(1)(a) of Directive 95/46, and of 'processing of personal data', within the meaning of Art 2(b), cannot be interpreted restrictively since such interpretation would be contrary not only to the clear wording of the Directive but also to its objective, which is to ensure, through a broad definition of those concepts, an effective and complete protection of data subjects. In brief, an interpretation which lets providers and users escape the obligations and guarantees laid down by Directive 95/46 would compromise the Directive's 'effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the Directive seeks to ensure'.[32]

[30] See paras 26-28 of the Judgement. Since 2006 the Italian *Garante* stressed that the indexing activity performed by a search engine service provider falls within the definition of 'processing' under Directive 95/46: see Autorità Garante per la Protezione dei Dati Personali, 18 January 2006, available at www.garanteprivacy.it (document web no 1242501).

[31] Ibid para 60.

[32] Ibid para 58. On the paramount importance of interpreting the law in the light of the fundamental principles and values enshrined by Constitution and the EU

Moreover, this principle has been both enshrined by the recent 'Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to human rights for Internet users', adopted on 16 April 2014 at the one-thousand one-hundred ninety-seventh meeting of the Ministers' Deputies within the Council of Europe, and implemented by the proposal for a 'General Data Protection Regulation' in the context of the ongoing revision of the European Data Protection Directive.[33]

IV. The Question of *How* the Data Protection Principles and Rules Should Be Applied in the Case at Issue and in the Wider Context of Internet Services: Who is the Controller?

In the light of the application of Directive 95/46, it is clear that the following question must be asked: 'Who is the controller, within the meaning of Art 2(d)?' In the foregoing paragraphs we have remarked that an 'intermediary service provider' (ie, for instance, a search engine provider or SNS provider) who processes user data falls within the scope of the definition of 'controller', and that, in cases of user-generated content that entail the publication of personal data on the web, both the 'intermediary service provider' and the user, ie the 'information provider', can play the role of

Treaties, see P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti* (Napoli: Edizioni Scientifiche Italiane, 3rd ed, 2006), 561 and 581.

[33] See recital 20 of the '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 - GDPR), COM(2012) 11 final.', (Bruxelles, 25 January 2012), and recital 20 of the General Data Protection Regulation (GDPR) adopted as a 'General Approach' by Ministers in the Council on 15 June 2015 available at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (last visited 20 October 2015), according to which the Regulation should be applied to 'the processing of personal data of data subjects residing in the Union by a controller not established in the Union' where 'the processing activities are related to the offering of goods or services to such data subjects irrespective of whether connected to a payment or not, which takes place in the Union'.

'controller' unless the user does not go beyond a purely personal or household activity.

It is interesting to note that, before the Judgement, the question debated was 'whether an intermediary should be considered to be the controller itself or a controller jointly with others with regard to a certain processing of personal data'.[34] From this perspective, the service provider should be considered as a simple 'processor' in cases where its activity is neutral, in the sense that its role is merely technical, automatic and passive, and as a 'controller' in cases where it plays an active role of such a kind as to give it knowledge of, or control over, the data stored. This means that the active provider falls within the scope of the definition of 'controller', alone or jointly with the 'information provider' or with other bodies that co-determine the purposes and means of the processing of the personal data in that online environment.

It is true that all concrete means of the intermediary activity and of the data processing must be taken into account in order to answer to the question at issue. Nevertheless, in the Judgement, the CJEU established an important criterion concerning the application of the Directive when it pointed out that 'the processing of personal data carried out in the context of the activity of a search engine *can be distinguished from* and *is additional to* that carried out by publishers of websites, consisting in loading those data on an internet page [...]. Inasmuch as the activity of a search engine is therefore liable to affect significantly, *and additionally compared with that of the publishers of websites*, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46'[35] (italics ours). In brief, it comes to differentiating the processing of personal data carried out by the publisher of a web site, ie the 'information provider', from that carried out by the 'intermediary service provider', because these can have different legal grounds, different

[34] See para 4.2.2 of Opinion 1/2008 on data protection issues related to search engines.

[35] See paras 35 and 38 of the Judgement.

purposes and different consequences for the fundamental rights of data subjects. This is a further break with the past.[36]

The case at issue is illustrative here. Indeed, according to the Court's remarks, 'the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Art 9 of Directive 95/46, from derogations from the requirements laid down by the Directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine'; furthermore 'it must be stated that not only does the ground, under Article 7 of Directive 95/46, justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, *the outcome of the weighing of the interests* at issue *to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the Directive may differ* according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, *the legitimate interests justifying the processing may be different* and, second, *the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same*'[37] (italics ours). This approach is very significant for an effective protection of data subjects' rights, insofar as the operator of a search engine can be obliged to remove, from the list of the results displayed following a search made on the basis of a person's name, links to web pages published by third parties and containing information relating to that person, even in a case in which that publication on the web is, in itself, lawful.[38]

Therefore, especially in the online environment, we have to distinguish between the various types of data processing, reserving to each of them a different treatment even in relation to the rights that

[36] See 'Guidelines on the implementation of the Court of Justice of the European Union Judgement on 'Google Spain and Inc. v. Agencia Española de Protección de Datos (Aepd) and Mario Costeja González' C-131/12' adopted by Working Party, Part I para A, n 1 above.

[37] See paras 85-86 of the Judgement.

[38] Ibid para 88.

can be exercised by data subjects. In other words, the types of data processing are becoming more diversified, as are the rules to be applied.

V. Focusing on the Application of Directive 95/46 to the 'Intermediary Service Provider': The Legal Grounds for a Lawful Processing of Personal Data

Given the foregoing, the application of Directive 95/46 to the processing of personal data carried out by an 'intermediary service provider' can give rise to further questions for analysis.

As the Court underlines in paras 71-74, all processing of personal data must meet a twofold legal test, which means that it must comply, first, with the principles relating to data quality set out in Art 6 of the Directive and, secondly, with one of the criteria for making data processing legitimate, listed in Art 7 of the Directive.

In detail, the controller has the task of ensuring that personal data are processed 'fairly and lawfully', that they are 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes', that they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed', that they are 'accurate and, where necessary, kept up to date' and, finally, that they are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'. In this context, the controller must take every reasonable step to ensure that data that do not meet those requirements are erased or rectified. It is clear that some of the listed obligations cannot be required to be fulfilled if they are interpreted as meaning that service providers would be responsible (or jointly responsible) for the lawfulness of data processing carried out by third parties such as users, publishers of web pages and advertisers. The provider cannot be made responsible (or jointly responsible) since it cannot reasonably control all user-generated content.[39] This could

[39] In the view of Advocate General Jääskinen, 'the internet search engine service provider cannot in law or in fact fulfil the obligations of controller provided in Arts 6, 7 and 8 of the Directive in relation to the personal data on source web pages

interfere with its role as intermediary in the information society without there being reasonable grounds. By contrast, the provider should ensure the compliance with the law of all data processing attached to its own role as intermediary. Therefore the Judgement is right to explain that the conditions required for the lawful processing of personal data that is carried out by a (search engine) provider must be assessed separately from the processing of such data by others.

More doubtful is the statement that a request for the removal or rectification of information must be addressed to the provider or the publisher of the website, depending on the role played by each one of them as data controller. From this point of view a criticism of the judgement at issue seems reasonable, inasmuch as such requests concerning data subjects' rights should be brought directly before the supervisory authority or the judicial authority, so that it can carry out the necessary checks and order the controller to take specific measures accordingly.[40] Otherwise there would be a risk that those who want to prevent the distribution of information about themselves would threaten to sue providers for privacy violations, and in so doing that they could induce the providers to censor the relevant content, even when it is lawful.[41] Moreover, providers do not have the professional ability to decide a huge number of issues involving the fundamental rights and freedoms of a huge number of data subjects.

On the other hand, the right to the protection of personal data is not an absolute right,[42] inasmuch as the processing of personal data

hosted on third-party servers'. See also M. Viola de Azevedo Cunha, L. Marin and G. Sartor, n 3 above, 66.

[40] For more details on such a critical observation, see S. Sica and V. D'Antonio, 'La procedura di de-indicizzazione', in G. Resta and V. Zeno Zencovich eds, n 1 above, 159-161; a different opinion is stressed by F. Pizzetti, 'Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il 'Velo di Maya' ', in G. Resta and V. Zeno Zenchovic eds, n 1 above, 271-272.

[41] M. Viola de Azevedo Cunha, L. Marin and G. Sartor, n 3 above, 66.

[42] See recital 3a of the proposed GDPR. On this point, cf Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert* v *Land Hessen* (European Court of Justice Grand Chamber 9 November 2010), available at www.curia.europa.eu, para 48. On the assumption mentioned, see also N. Witzleb, D. Lindsay et al, 'An Overview of Emerging Challenges in Privacy Law', n 6 above, 1.

can be legitimate pursuant to Art 7 of Directive 95/46, even where the data subject has not given his or her consent and even if the data subject has asked for the processing to cease.

As regards the provider when hosting user-generated content that includes personal data, the legal ground for making the processing of the data legitimate is covered by subpara (f) of that Article, which permits the processing of personal data where it is necessary for the purposes of legitimate interests that are being pursued by the controller or by third parties, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. In such cases, the application of data protection law necessitates a balancing of the opposing rights and interests involved, in the context of which account must be taken of the significance of the data subject's rights that arise from Arts 7 and 8 of the Nice Charter. For instance, the removal of information and links from the list of results generated by search engines in an online environment can be essential for protecting the privacy or dignity of a person, but could have effects upon the legitimate interests of internet users who may be interested in having access to that information. That balance may, however, depend in specific cases on the nature of the information in question and its sensitivity for the data subject's private life, and on the interest of the public in having that information, an interest that may vary, in particular, according to the role played by the data subject in public life.[43]

Moreover, as regards the provider when processing users' data, the legal ground required by Art 7 may be found in its subpara (b), which permits the processing of personal data if this is necessary for the performance of a contract to which the data subject is party. In such cases, the Directive prevents the controller from carrying out any data processing for further and different purposes, unless it has collected a specific data subject's consent, as required to give a legal

[43] See para 81 of the Judgement. For more details on the criteria to be taken into account for both making the balancing test and identifying the correct rule to be applied in a particular case, see 'Guidelines on the implementation of the Court of Justice of the European Union Judgement on 'Google Spain and Inc. v. Agencia Española de Protección de Datos (Aepd) and Mario Costeja González' C-131/12' adopted by Working Party, n 1 above, 'Part II: List of common criteria for the handling of complaints by European data protection authorities'.

ground for any further data processing, or alternatively can find another legal ground as provided for by Art 7.

VI. Users' Consent as a Legal Ground for Data Processing for the Purpose of Profiling Users: The Decision Adopted by the *Garante* against Google on 10 July 2014 Enhancing Users' Data Protection

In the light of the foregoing, during recent months the European data protection authorities have focused their attention on the activity of Google Inc. (hereinafter, Google) in EU Member States.

Having concluded an administrative proceeding in order to check the lawfulness and fairness of the processing operations performed by Google under its privacy policy, the Italian *Garante* adopted an important decision on 10 July 2014, setting out a number of measures that must be implemented by that company no later than the beginning of 2016.[44]

It is interesting to remark that in the course of this proceeding, the *Garante* found that Google had failed to request users' consent for the purpose of profiling them and in order to display customised behavioural ads and to analyse and monitor their navigation, and had failed to provide data subjects with information concerning the clarification of the particular purposes and the mechanisms relied upon in processing personal data. This means that Google will be violating Arts 7, 13, 23, 24 and 122 of the Italian Personal Data Protection Code (hereinafter: the Code) unless it implements the measures requested by the *Garante*. The decision at issue is consistent with the Judgement in one aspect, whilst the protection of data subjects seems to be stronger in another.

Indeed the above-mentioned approach set out by the Court of Justice towards the activity of a service provider, in the light of data

[44] See n 1 above. More precisely, the *Garante* has established that the measures set forth under its decision must be implemented no later than 18 months from the date of the decision itself. Furthermore, more recently, the *Garante* has adopted general guidelines on the processing of personal data for the online profiling of users: Autorità Garante per la Protezione dei Dati Personali 19 March 2015, available at www.garanteprivacy.it (document web no 3881513).

protection law, has been followed by the *Garante* when differentiating between the following three types of data processing whose purpose is to profile users: a) processing of personal data relating to authenticated users in connection with the emailing service called Gmail; b) matching the personal data collected in connection with the provision and use of several of the features made available to users; and c) using cookies and other identifiers as necessary to trace back specific actions or recurring behavioural patterns in the use of the available features to identified or identifiable entities. The *Garante* has analysed each of these types of data processing in order to assess their compliance with the law on a case-by-case basis, having regard to the individual features offered by the provider. This is an approach that can be used by other data protection authorities.

In its analysis, the *Garante* has emphasised the failure to request users' consent in all of the aforesaid cases of data processing carried out by Google.[45]

It is illustrative to look at the cases under a) and c) above regarding the emailing service and the use of cookies, in which Google performs processing of the personal data of authenticated users for multiple purposes. According to the *Garante*'s decision, some of these purposes (eg filtering spam; detecting viruses; enabling users to perform text searches) are purely technical in nature and are related directly to the provision of the service, so that the data processing 'falls under the scope of the derogation from consent obligations because it is performed to fulfill obligations arising out of the contract for the provision of emailing services'; as regards purposes that go beyond those mentioned, in particular in order to display, to authenticated users, customised ads based on behavioural advertising technology, 'it is conversely necessary for Google to obtain its users' prior informed consent'.

In fact, given that behavioural advertising is based on the use of identifiers that enable the creation of very detailed user profiles, providers are bound by Art 5(3) of Directive 2002/58/EC (ie the e-

[45] On this issue, see also the 'Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies' set out by the *Garante*: Autorità Garante per la Protezione dei Dati Personali 8 May 2014, available at www.garanteprivacy.it (document web no 3167654).

Privacy Directive, in its revised version), pursuant to which placing cookies or similar devices on users' terminal equipment or obtaining information through such devices is only allowed with the informed consent of the users.[46] In particular, the current wording of this Article is based on a distinction between at least two different scenarios. In the first of these, the storing of information is only allowed, 'on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46, inter alia about the purposes of the processing'. The second scenario is where the storing of information is considered as legitimate. This is the case where it only takes place for the transmission of an electronic communication or where it is necessary to provide a service requested by the user.[47]

The processing of personal data for technical purposes that are directly connected with the provision of the service requested by the data subject/user should therefore be legitimate on the ground provided for by Arts 7(b) of Directive 95/46 and 24(1)(b) of the Code, inasmuch as, in such cases, the processing is necessary for the performance of contractual obligations. Instead of this, the processing of personal data consisting in profiling authenticated users for further purposes, such as serving targeted advertising, should be based on the legitimate ground provided for by Arts 7(a) of Directive 95/46 and 23 of the Code, which means that, in such cases, Google would have to obtain the prior informed consent of authenticated users.

Such differentiation may be consistent with the ordinary context of market trading, in which both the request to collect and process personal data for purposes that go beyond the performance of contractual obligations, and the informed consent given by the data subject, give rise to a sort of negotiation that is additional to and

[46] See Data Protection Working Party (WP 29), Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 3. Art 5(3) of Directive 2002/58 has been amended by Art 2 of Directive 2009/136/EC of 25 November 2009. For more details on consent, see E. Kosta, *Consent in European Data Protection Law* (Leiden: Brill-Nijoff, 2013), 261-381.

[47] For more details on this provision, see P. Hustinx, 'Do not Track or Right on Track. The Privacy Implications of Online Behavioural Advertising', 7 July 2011,

outside of the scope of the contract. For precisely this reason, the data subject's consent may be freely given, as required by law.

By contrast, in the online environment, the above services and features are very frequently offered free to end-users. It follows that, in such cases, the request to collect and process personal data, for the purpose of displaying customised ads based on behavioural advertising technology to users, could be encompassed within the core business of the contract and accepted by the user as a compensation for the provision of the service that is offered free.

In this connection, it should be pointed out that if one accepts the offer of a free-of-charge service and the consideration consists in a given data processing operation, it would be unfair to require the data subject to give his or her consent to the processing – pursuant to Art 23 of the Code – inasmuch as such consent would not be freely given as required by the law.[48] In fact, the data subject's consent would be linked to the need to have access to a number of services such as emailing, social networking and online payment, which are more and more essential in our lives. In such cases, the only consent to be required would have to concern the conclusion of a contractual agreement; therefore, the processing of users' data for the purpose of profiling them through behavioural advertising technology should be grounded in Arts 7(b) of Directive 95/46 and 24(1)(b) of the Code, rather than in Arts 7(a) of Directive 95/46 and 23 of the Code.

It is interesting to remark that in its earlier decision of 12 October 2004, the *Garante* established, with regard to the offer of free-of-charge online services, that the 'consideration' could consist in 'lawful, fair as well as proportionate user profiling', providing that no additional consent was requested to process user data – as such consent would not have been freely given.[49]

In the afore-mentioned decision of 10 July 2014, the *Garante* looks beyond this problem and enhances the consumers' right to data

available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-07-07_Speech_Edinburgh_EN.pdf (last visited 20 October 2015).

[48] F.G. Viterbo, *Protezione dei dati personali e autonomia negoziale* (Napoli: Edizioni Scientifiche Italiane, 2008), 233.

[49] Autorità Garante per la Protezione dei Dati Personali, 12 October 2004, available at www.garanteprivacy.it (document web no 1108836). For further remarks see F.G. Viterbo, n 48 above, 230-233.

protection. As regards the activities performed in order to provide emailing services, it has been established that the processing of the data subject's information for purposes that are not directly and closely related to the provision of those specific services requires the data subject's prior informed consent, in particular when the purpose pursued by the service provider is to display, to its users, customised ads based on behavioural advertising technology. So, as pointed out by the *Garante* in the para 1 of its decision, since the company's business model is grounded first and foremost in its advertising revenues, the above services and features are offered free to end-users in the vast majority of cases. Nonetheless, it is necessary for the service provider to obtain its users' consent. Moreover, the *Garante* is even more explicit in the new '*vademecum*' called 'Up with Tips. Down with Spam. Privacy-Proof Marketing from Your Telephone to the Supermarket', which explains to consumers their rights and how to exercise them in order to prevent a company from violating their privacy.[50] In particular, the '*vademecum*' explains that the provision of a commodity or service cannot be bound to the consumer's consent to the processing of personal data for the purpose of sending ads. In such cases, both the editor of a website that does not permit consumers to enjoy a service and the operator of a supermarket that refuses to issue a loyalty card behave unfairly. In brief, the data subject cannot be compelled to give consent to the processing for marketing purposes.[51] The *Garante* has so ensured that consent should be given specifically and freely.

In other words, pursuant to the measures set out by the *Garante*, the processing of personal data for marketing and similar purposes must be outside the scope of freedom of contract, which means outside the contractual agreements between service providers and users, irrespective of whether the service is offered free-of-charge or for a fee. Namely, in such cases, the 'consideration' *could not* consist in 'lawful, fair as well as proportionate user profiling'. It follows that the information given to data subjects does not have to specify whether the provision of the requested personal data is obligatory or voluntary. This means that Google cannot establish that the consent

[50] Autorità Garante per la Protezione dei Dati Personali, 20 April 2015, available at www.garanteprivacy.it (document web no 3867816).

[51] See ibid 11.

to the use of cookies for the purposes of profiling the user and serving targeted advertising is an obligatory condition that must be met in order for the service to be provided without charge, meaning that if cookies are disabled, the service will not work.

This statement set out by the *Garante* seems to cover even the interpretation of Arts 5(3) of the e-Privacy Directive and 122 of the Code.[52] It follows that the user cannot be informed of the obligatory nature of allowing the cookie to be used for the purpose of profiling him/her, because the storing of information in the terminal equipment of the user is only allowed with his/her informed consent. This is not the case where the cookies are technically necessary in order for the service to be provided.

It is interesting to note that the storing of information or the accessing of information stored in the terminal equipment of the user is an operation which must be distinguished from the subsequent recording and elaboration of the collected personal data, even if both operations are aimed at the purpose of profiling the user. The former operation requires the user's consent under Arts 5(3) of the e-Privacy Directive and 122 of the Code; the latter (processing) operation requires the user's consent under Directive 95/46 and Art 23 of the Code. In both cases, the user must be provided with clear and comprehensive information in accordance with the Data Protection Directive before giving his or her consent. However, it can be argued that the consent required by the e-privacy Directive should be considered autonomously from the consent provided for by the data protection law. This approach can be supported by noting that, according to recital 24 of the 2002 version of the e-Privacy Directive and recital 65 of the revised version, the rationale of Art 5(3) is that the storing of information and the accessing of information stored in

[52] In order to support the above perspective, we have to emphasise para 3.II of the 'Working Document: Privacy on the Internet – An Integrated EU Approach to On-line Data Protection' adopted by the Data Protection Working Party on 21 November 2000, according to which the providers of free internet services would not fall outside the scope of application of the e-Privacy Directive since it has been made clear, in the jurisprudence of the European Court of Justice, that to make the e-Privacy Directive applicable 'the remuneration does not necessarily have to be paid by the recipient of the service; it can for instance also be paid by advertisers'; see Case C-109/92 *Wirth* v *Landeshauptstadt Hannover* (European Court of Justice Fifth Chamber 7 December 1993) available at www.eur-lex.europa.eu.

the user's terminal are considered to be an intrusion into the private sphere of the user, irrespective of whether the information is or is not personal data.[53] Moreover, as regards such a 'particular' regulation of consent, recital 66 refers to 'the methods of providing information and offering the right to refuse' which 'should be as user-friendly as possible'.

In this scenario, in which the user is informed of the voluntary nature of consenting to the use of the cookies for the purpose of profiling him/her, Google could obtain a unique prior consent to both operations. Such consent must be given in accordance with both the Data Protection Directive and the e-Privacy Directive so that it is given specifically and freely.

According to Opinion 2/2010 and Working Document 02/2013 adopted by the Data Protection Working Party, in order for browsers or any other applications to be able to 'deliver' a valid consent, by default, they should reject third-party cookies and require the data subject to engage in an affirmative action to accept both the setting of cookies and the continued transmission of information contained in cookies by specific web sites.[54] If browsers, by default, are configured to reject cookies, in each and every case, the user should be allowed to give his/her prior informed consent to the processing of personal data related to the use of cookies, in compliance with the opt-in rule.[55]

It is clear that, in certain cases, the obligation to request the data subject's consent is not a tool that can ensure the effective protection of individuals with respect to the processing of information related to them. An adequate protection of data subjects' rights may be ensured by virtue of all other principles and

[53] The rationale for Art 5(3) of Directive 2002/58 mentioned above has been underlined by P. Hustinx, n 47 above, 3.

[54] See para 4.1.1 of the 'Opinion 2/2010 on online behavioural advertising', n 46 above and para 3 of the 'Working Document 02/2013 providing guidance on obtaining consent for cookie – Adopted on 2 October 2013'. According to P. Hustinx, n 47 above, 5, since most current browsers accept cookies by default and most current users lack the skills to change browser settings, this scenario is too often not realistic at the moment. However, this could of course change in the future.

[55] A. Mantelero, 'Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies' *Diritto dell'Informazione e dell'Informatica*, 781-804 (2012).

rules binding the controller in light of the data protection law, ranging from the obligation to give clearly worded and easily accessible information to data subjects, pursuant to Art 13 of the Code, to discretion in selecting the methods for the processing of personal data under Art 4(1)(f) of the Code, ie the standards and measures ensuring that the processing of users' data for profiling purposes is compliant with the law.[56]

As regards the information to be given by the provider, the *Garante* has pointed to the adoption of a multi-layered approach to the information notice, in which a first layer requires that the notice should accommodate all the information of general import that is most relevant to users, and the second layer requires the notice to contain information that may be reserved for policies relating to the individual features, or for providing examples that clarify how personal data are processed.

As regards the methods for the processing of personal data, it is interesting to note that, in cases involving a high level of complexity for controllers and serious threats for data subjects, freedom of enterprise and discretion in selecting the measures that ensure the compliance of the data processing with the law are usually much more limited, inasmuch as they must meet the measures set forth by the *Garante*. Indeed, it is exactly from this viewpoint that Google must ensure that it is possible for users to exercise their rights fully, eg by refusing consent and/or changing their mind at any time, and in a user-friendly manner; for this purpose 'there must be a phase or moment, during the user's navigation experience, when he or she should be enabled to make a choice out of several options', according to what has been stated by the *Garante* in its decision.

[56] In this regard, see paras 2 and 4 of the decision which is discussed here (Autorità Garante per la Protezione dei Dati Personali, 10 July 2014). Furthermore, the Italian case law has established that, even in cases in which no consent is required for the processing of personal data (eg if the processing is necessary for the performance of obligations resulting from a contract), the other obligations under the data protection law should still be met, beginning with the information required to be given to the data subject pursuant to Art 13 of the Code: see Tribunale di Torino 21 October 2009, *Data bank online De Jure*.

VII. The Question of whether Personal Data May Be a Kind of (Online) Tradable Commodity. The Extent of Freedom of Contract within the Scope of Personal Data Protection

The question of *how* to apply data protection principles and rules includes the issue of the compatibility of the rules governing a data subject's consent and the processing of personal data with the rules governing negotiations and contracts; in particular, it must be clarified whether personal data can be negotiable goods.

It would seem that such problems could be solved on a case-by-case basis by considering the interest that the data subject intends to protect. This means that if personal data is considered to be similar to a commodity or to goods that may be destined to be appropriated or commercially exploited, then the protection and circulation regime proper to such goods would be applicable, being loanable from copyright law and contract law. Furthermore, in European law there are now regulations that expressly protect data as 'digital content', and give special treatment to the commercial use of data in sales law.[57] When, on the other hand, the protection of fundamental rights is at stake, the data protection law should apply, insofar as the forms of protection it establishes would be exclusively tailored to interests relating to the person and to personal rights.[58]

A similar approach, based on the hybrid nature of personal data protection, with rationales oriented towards both economic rights and human rights, has been argued by considering the choice that the European legislator would have made, in the European Charter on Fundamental Rights, to separate the provision setting out the right to

[57] See Directive 2011/83/EU in relation to the rights of the consumer, which expressly protects 'digital content' according to its definition as 'data which are produced and supplied in digital form' (see Art 2, n 11). See also Arts 2(j) and 5(b) of the Draft Common European Sales Law (CESL): COM (2011) 635 final, backed by the European Parliament on 26 February 2014, in which digital data are treated as tradable goods in the same manner as other goods.

[58] This problem is discussed by C. Kuner, F.H. Cate et al, 'Privacy – an Elusive Concept' 3 *International Data Privacy Law*, 141 (2011): 'one of the most important things protected by privacy law is personal data, which has become a valuable commercial commodity. And it is here that we observe the tension between the dual nature of privacy as a human right and a subject of commercial interest'.

respect for private and family life pursuant to Art 7 from the right to protection of personal data pursuant to Art 8: namely that these provisions have evolved into two highly distinct concepts because of which personal data have nothing to do with fundamental freedoms but have to be protected only for their market value.[59] Indeed, Art 1(2) of Directive 95/46 prohibits any restriction on the free flow of personal data between Member States. Furthermore, the basic assumption that underlies this utilitarian approach towards personal data protection is given by an empirical observation of present day practice in the marketplace and social life, especially in the online world. It has been pointed out that on the internet individuals often make deals for the disclosure, collection, use and reuse of their personal data, in certain situations receive some form of compensation, and thus 'exploit' and 'sell' their habits, customer/user-profile and even sensitive personal data.

Nevertheless such an interpretation seems to be unsatisfactory because the concept of personal data protection is ill-suited to a definition in terms of exchange for a value as well of ownership.[60] In

[59] On this point, see C. Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity', in L. Guibault and P.B. Hugenholtz eds, *The Future of the Public Domain* (Netherlands: Kluwer Law International, 2006), 244.

[60] This approach has particularly been proposed by scholars in the United States: R.A. Posner, 'The Right of Privacy' 12 *Georgia Law Review*, 393 (1978); J. Litman, 'Information Privacy/Information Property' 52 *Stanford Law Review*, 1283 (2000); A. Bartow, 'Our Data, Ourselves: Privacy, Propertization, and Gender' 34 *University of San Francisco Law Review*, 633 (2000); L. Lessig, 'Privacy as Property' 69 *Social Research*, 247 (2002); P.M. Schwartz, 'Property, Privacy and Personal Data' 7 *Harvard Law Review*, 2056 (2004); in Italy see V. Zeno Zencovich, 'Profili negoziali degli attributi della personalità' *Diritto dell'informazione e dell'informatica*, 547 (1993). In the European debate, see Y. Poullet, 'Data Protection between Property and Liberties. A Civil Law Approach', in H.W.K. Kaspersen and A. Oskamp eds, *Amongst Friends in Computers and Law. A Collection of Essays in Remembrance of Guy Vandenberghe* (The Hague: Kluwer Law International, 1990), 160; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), 120; N. Purtova, *Property Rights in Personal Data: a European Perspective* (The Hague: Kluwer Law International, 2011), 1; T. Hoeren, 'Dateneigentum – Versuch einer Anwendung von § STGB § 303a StGB im Zivilrecht' *Multimedia und Recht*, 486 (2013); G. Spindler, 'Datenschutz – und Persönlichkeitsrechte im Internet – der Rahmen für Forschungsaufgaben und Reformbedarf' *Gewerblicher Rechtsschutz und Urheberrecht*, 996 (2013).

truth, it is very difficult to find a general notion concerning the right to property in the most important civil codes enacted in the European Member States within the last century. However, a recent attempt to formulate such a notion may be found in the experience of the 'codification' of the principles and general rules of the main private law areas in the EU context which have given rise to the DCFR, under Art VIII-1:202: '«Ownership» is the most comprehensive right a person, the owner, can have over property, including the exclusive right, so far as consistent with applicable laws or rights granted by the owner, to use, enjoy, modify, destroy, dispose of and recover the property'.[61] Within the meaning of this definition and of the subsequent definition of 'co-ownership' under Art VIII-1:203, we can argue that personal data cannot be vested with rights in property.[62] On the other hand, the commercial exploitation of personal data cannot be detached from those aspects concerning the vulnerability and the human personality of the data subject, so that it is not possible for these two facets to be considered and regulated separately. In other words, the problem is that the disciplines to be applied to these different aspects can interfere with each other: eg the creation and selling on the market of a big databank, obtained through the profiling of a large number of citizens and even processing their sensitive data, may appear lawful from the sole perspectives of copyright law and contract law, but such an operation can lead to the infringement of data protection rules having a mandatory character, which can make the contract – or some of its terms – void and unenforceable.[63]

[61] DCFR stands for 'Draft Common Frame of Reference'. It contains 'Principles, Definitions and Model Rules of European Private Law' and its Articles and Comments were prepared by the Study Group on a European Civil Code and the European Research Group on Existing EC Private Law (the 'Acquis Group'): C. von Bar et al, *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR)* (Munich: Sellier European Law Publishers, 2009), 422.

[62] In Book VIII of the DCFR, 'co-ownership' means 'two or more co-owners own undivided shares in the whole goods and each co-owner can dispose of that co-owner's share by acting alone, unless otherwise provided by the parties'.

[63] F.G. Viterbo, n 48 above, 235-242. For more details on the contractual nature of agreements between (social network) service providers and users, see F. Astone, 'Il rapporto tra gestore e singolo utente: questioni generali' *Annali italiani del diritto*

Even if some believe that it is possible to sell personal data, this opinion leads to a false perspective. Personal data are not simply pieces of information. They are pieces of information about a particular, identified or identifiable natural person and can be capable of revealing some of the most intimate and delicate aspects of that individual's personality, such as his/her state of health or sex life, for example. Their significance is not linked to the economic and quantitative criterion of marketability but, rather, to a rationale based on the protection of human rights and values.[64] This argument may be inferred from the law that is expressly devoted to guaranteeing the protection of personal data, irrespective of whether it is possible to attach an economic value to them: indeed, in the personal data protection laws there is no provision for a specific contract that would allow the transfer or assignment of personal data by the data subject or the data controller to another data controller. It is precisely in this respect that personal data seem to differ from all other goods in the Italian and EU legal order. On the one hand, they pose as elements creating the data subject's personal identity. On the other hand, personal data possess a capacity to be an important resource that may be the object, not of appropriation but, rather, of *access*; neither for enjoyment nor for consumption but, rather, for *processing* – by third parties for specific and worthy purposes.[65] Therefore personal data may be deemed to be intangible goods that are *not transferable*, within the meaning given to this term by the most important civil codes enacted in the EU context. The only transferable goods can be the benefits and (pecuniary) utilities that the data controller receives *through* and *after* the processing of personal data that is carried out in full compliance with personal data protection law. From this perspective, when referring to personal data, the concept of processing not only embraces all those

d'autore, della cultura e dello spettacolo, 107 (2011); and C. Perlingieri, 'Gli accordi tra i siti di *social networks* e gli utenti' *Rassegna di Diritto civile*, 120 (2015), who stresses that these contracts are not considered to be free, but are commutative and involve the issue of the 'marketability' of the attributes of the human person. For an analysis of the checks that can be carried out on contracts in the light of the fundamental principles and values of the legal system, see P. Perlingieri, 'Il principio di legalità nel diritto civile' *Rassegna di diritto civile*, 187 (2010).

[64] F.G. Viterbo, n 48 above, 149-152.

[65] Ibid 153-155.

operations that result in the movement of the data but also implies that a special set of rules is applied to all matters regarding personal data. This regime is wholly autonomous, and is different from the rules of the *ius commune* concerning the transfer of ownership and intellectual property.[66]

Therefore, by way of consideration for the supply of a free online service, the user is not able to sell his/her personal data, but can allow personal data to be processed by the provider for specified and lawful purposes and in compliance with data protection law. In other words, at the time of entering into the contractual agreements, the data subject cannot waive the protection of his/her personal data and the consequent rights that are conferred for this purpose, such as the rights to be informed that processing is taking place, to be aware of each specific purpose for which personal data are processed, to consult the data, to request corrections and even to object to processing in certain circumstances, and so forth.

A different conclusion would lead to the infringement of the data subject's fundamental rights. Given the high level of protection for human dignity, personality and fundamental rights guaranteed by both the Charter of Fundamental Rights of the EU and the ECHR, and given the fundamental principles and rules provided in the Italian Constitution and the constitutions of the other EU Member States, individuals are not able to waive the protection of their fundamental rights by means of a contract.[67]

[66] Ibid 156-158.

[67] See M. Hartlev, 'The Concept of Privacy: An Analysis of the EU Directive on the Protection of Personal Data', in D. Beyleveld, D. Townend et al eds, *The Data Protection Directive and Medical Research Across Europe* (Aldershot: Ashgate, 2004), 29, who remarks that Art 6 of the Directive, together with Arts 10-12 and Art 17, emphasise the importance attached to the individual's right to an inviolate personality so that 'it is not possible to derogate from these provisions, even with the consent of the data subject'; L. Bergkamp, *European Community Law for the New Economy* (Antwerp: Intersentia, 2003), 123, who argues: 'even if an individual wants to give up some or all of his privacy rights (eg to obtain a lower price for a product or service), EU law will not let him do so. The EU privacy rights cannot be waived in any matter'. For a wider perspective, see J. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' 113 *The Yale Law Journal*, 1153-1190 (2004); P. Perlingieri, 'L'incidenza dell'interesse pubblico sulla negoziazione privata' *Rassegna di Diritto civile*, 933 (1986), and Id, *Il diritto dei contratti fra persona e mercato* (Napoli: Edizioni Scientifiche Italiane, 2003), 60.

The fundamental rights of the persons to whom data refer (ie the right to respect for private and family life and the rights to the protection of dignity and personal identity, above all) constitute the axiological parameter for selecting and evaluating the arrangements for processing information. This parameter is integrated with the 'purpose specification principle', which gives relevance to the transparency of the purpose of the processing, as well with the 'data minimisation principle' and the other criteria for the lawfulness and fairness of the processing, as specified in Art 6(1) of the Directive.[68] All these criteria, parameters and principles express the idea of and demand for proportionality.[69] They can be considered 'mandatory' not only for natural and legal persons but even for the EU and national legislators and authorities that are responsible for tackling issues in the Area of Freedom, Security and Justice (AFSJ). Because of an infringement of those principles, the Court of Justice of the EU has declared Directive 2006/24/EC (the Data Retention Directive) to be invalid.[70]

[68] The above-mentioned principles refer to all types of personal data processing, even if Art 3 of the Italian Code seems to give them a more restricted significance, stating that 'Information systems and software shall be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity': for more details on this provision see G. Buttarelli, 'Articolo 3', in C.M. Bianca and F.D. Busnelli eds, *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196*, I (Padova: Cedam, 2007), 34; R. D'Orazio, 'Il principio di necessità nel trattamento dei dati personali', in R. D'Orazio, V. Cuffaro and V. Ricciuto eds, *Il Codice del trattamento dei dati personali* (Torino: Giappichelli, 2007), 21.

[69] In the 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector', adopted on 27 February 2014, the 'Article 29 Data Protection Working Party' has emphasised these linked criteria and principles: 'The principle of purpose limitation is about understanding *why* certain personal data is being processed. This means being as specific as possible about the purposes for which a proposed measure might warrant collection and processing of personal data. By doing so it should also lead to better compliance with the data minimisation principle. The data minimisation principle exists to ensure that only the minimum amount of personal data is processed to achieve the purpose set out. These data protection principles link very closely with the concept of proportionality in a privacy context' (para 5.7).

[70] See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* v *The*

Freedom of contract, within the scope of personal data protection, does not seem to be cancelled by virtue of the mandatory character of the aforesaid fundamental principles and rules of data protection law, nor by the conclusion that personal data are not negotiable goods. Indeed, one can imagine clauses or agreements directed at establishing the adoption, during processing, of particular security measures extending beyond the minimum standards provided for by law, as well as of a particular 'retention policy' and 'deletion policy',[71] or at distinguishing (in the constitution of an association) the data that may be processed for online communication to the public from the remaining data that has been collected for membership purposes, or at prohibiting the assignment of data to third parties, even when the conditions laid down by the law can be satisfied. Recently, the *Garante* has suggested the performance of a contract by both the manager of a website ('publisher') and the manager of another website that installs the cookies by way of the former ('third party'), in order to ensure that the 'third party' shall not cross the information contained in 'technical cookies' with other data that it already processes.

By contrast, the freedom of contract seems to be ruled out in the area of marketing and behavioural advertising by virtue of the measures adopted by the Italian supervisory authority, according to which the processing of personal data for marketing purposes cannot have the performance of a contract as its legal ground. As a mandatory rule, such data processing cannot be bound to the

Minister for Communications et al (European Court of Justice Grand Chamber 8 April 2014) available at http://curia.europa.eu/. In the previous judgement of 2 March 2010 the German Federal Constitutional Court abrogated the national implementation of the Data Retention Directive, basing its analysis on a 'privacy test', similar to the one developed by the ECtHR under the criteria contained in Art 8(2) of the ECHR. The German Court followed this scheme and made a check of three requirements (legality, legitimacy and proportionality): for more details see K. de Vries, R. Bellanova et al, 'The German Constitutional Court Judgement on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It)', in S. Gutwirth, Y. Poullet et al eds, *Computers, Privacy and Data Protection: an Element of Choice* (London-New York: Springer, 2011), 4-23.

[71] The 'retention policy' concerns the maximum retention period of users' personal information. The 'deletion policy' sets out the conditions under which a data subject can request the deletion of the personal data related to him/her.

performance of a contract and should be grounded on the data subject's prior (free and informed) consent.

Thus, applying the measures set forth by the supervisory authorities along with negotiating the data protection policy to be adopted by the controller are very important tools by which individuals can strengthen the protection of their fundamental rights and freedoms from the threats derived from the necessary processing/movement of their personal data.[72]

[72] F.G. Viterbo, n 48 above, 167-168.