EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

The (in)adequacy of the law to new technologies: the example of the Google/CNIL and Facebook cases before the Court of Justice of the European Union

ALDO IANNOTTI DELLA VALLE
Ph.D. Candidate in Researcher 'Humanities and Technologies' at University Suor Orsola Benincasa of Naples
Lawyer in Naples

Abstract

The paper starts with the analysis of the two recent decisions of the Court of Justice of the European Union on the Google/CNIL and Facebook cases, also in the light of the GDPR.

The digital revolution is giving one of the greatest transformations to the world since the era of the industrial revolution and is equally aware that we must be ready for the ever-greater penetration of new technologies into our lives. With specific regard to the right to be forgotten, the real problem lies in the fact that personal data become substantially indelible once they have been published online and the only possibility is to think about a possible balance between innovation and the protection of fundamental rights.

For this reason, this paper highlights how both the legislator and the Courts do not pay the due attention to the new technologies behind the law, suggesting a technological approach to law as a way to better protect fundamental rights in the digital age.

Keywords: Right to be forgotten - Data Protection Law - GDPR - Technology - Internet - Search engines

Summary: 1. New technology law and GDPR: the right to be forgotten has been forgotten? – 2. Lack of a technological analysis of the law and weakening of the protection of rights: the Google/CNIL case. – 3. What the Google/CNIL and the Facebook cases have in common: The Court does not care about the technology underlying the application of the law. – 4. The protection of fundamental rights needs a technological approach to law.

1. New technologies law and GDPR: the right to be forgotten has been forgotten?

The Internet revolution has affected every sector of social life and, consequently, has also profoundly changed the face of the legislation, which must inevitably react to these changes to preserve its effectiveness and social utility.

It is, therefore, crucial to reflect on the adequacy of the law with respect to the technology it intends to regulate. In fact, in the 21st century, the development of new technologies is so fast that it requires a constant interaction of legal experts with specialists from other branches of knowledge, who are involved in studying technologies from a technical point of view. Only by being aware of the technical world that is about to regulate, lawmakers and judges will be able to try to keep pace with the development of new technologies and, if possible, to anticipate them. Furthermore, only thorough a knowledge of the technology involved in laws and decisions it is possible to critically analyze[1] them, as we will try to do in this paper.

[1] *See* L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Pol. Dir., 339.

It seems appropriate to start reflections on the topic of the adequacy of the law to new technologies from the analysis of laws and decisions regarding the right to be forgotten, being one of the rights that have become central in the digital age. It changed its skin, becoming even more important, and it never loosed its connotation of inviolable law.[2] The right to be forgotten, traditionally, was linked to the concept of printed paper; the new right to be forgotten, which we may refer as a right to be forgotten 'online', is linked to the world wide web and needs to be properly distinguished from the first even on a systematic level.

The difference between the two conceptions of right to be forgotten emerges, in evidence, thinking about the same structure of the Internet in which the storage of data and information knows no boundaries and knows no obsolescence, especially if indexed in a search engine like Google, making it much more difficult, or in certain cases impossible, to 'be forgotten'.

As for the legislation, it seems necessary to start from the analysis of the aforementioned Article 17 of the GDPR to try to explain, very briefly, why this is disappointing compared to the ambitious objectives that arise.

Two years after the entry into force of the GDPR, applicable in all Member States since 25th May 2018, replacing the Data Protection Directive (Directive 95/46/EC), the new regulation seems to be for many aspects a disappointment, in terms of the adequacy of the law to the demands of European society and ultimately to new technologies.[3] One of these aspects is undoubtedly the discipline of the right to be forgotten which seems to have been forgotten by the same GDPR, Article 17, which claims to regulate it.

After the groundbreaking 2014 decision of the Court of Justice of the European Union in the Google Spain case (C-131/12), it was reasonable to expect an exhaustive discipline of the right to be forgotten by the European legislator: the new discipline should have taken into account the intense debate of the last few years and should have attempted to bring order and clarity.

Therefore, the GDPR would have really constituted the perfect opportunity to finally dictate a uniform discipline on the territory of the European Union also regarding the right to be forgotten, an occasion that unfortunately seems to have been wasted.

In fact, the aforementioned Article 17, paragraph 1, only establish the principle according to which the interested party, under certain conditions, has the right to request the cancellation of personal data concerning him (therefore not de-referencing personal data from the search engine as the Court of Justice claimed in the Google Spain decision). Referring only to the cancellation it is not clear if the GDPR intends to refer this duty to proceed with the cancellation also to the search engines or not.

Definitely, the content of paragraph 1 does not have an original content, if compared with the previous Directive 95/46, Article 12.

Therefore, the right to erasure, as well as the discipline of notification to third parties, was already contained in the previous discipline: the regulation, therefore, only specifies the content of a right already guaranteed on the basis of the previous rules, namely the right to

---

[2] Being forgotten assumes a fundamental importance for the individual who, also if he has committed a fact, has the right not to be remembered for that fact for life, ignoring all his subsequent human and social growth, as well as his eventual reintegration following the expiation of a penalty. In the digital age, being forgotten has become even more difficult, since the web knows no obsolescence. *See* TE Frosini, *Liberté Egalité Internet* (2015) Napoli, 117.

[3] *See* MC Gaeta, 'Hard law and soft law on data protection: what a DPO should know to better perform his or her tasks in compliance with the GDPR' (2019) 1 EJPLT, 61 ff., according to which 'The data protection regulation was adopted in response to the maximum extension of the processing of personal data and to the development of ever more pervasive technologies, strengthening the main EU data protection regime to the point to entail a real reform on data protection'.

erasure, nothing saying about the right to be forgotten, understood, starting from the Google Spain judgment, mainly as the right to de-referencing. Indeed, despite of the heading, the right to be forgotten is neither defined nor disciplined.

However, the same heading of the article, referring to the right to be forgotten, is less ambitious than it would appear, relegating the right to be forgotten in brackets, almost as a subset of the right to erasure. In this way, however, we end up forgetting that the right to be forgotten, if anything, could include the (old) right to erasure, together with the (new) right to de-referencing deriving from the Google Spain judgment. Anyway, the provision seems not to be aware of this, being confused about what erasure is and what oblivion is.

Furthermore, the repeated reference to the element of consent, which certainly constitutes one of the legal bases for the lawful processing of personal data, does not appear at all conclusive[4], especially concerning the search engines and the issue of de-referencing: as a matter of fact, referencing is independent of consent. A regulation based on consent, therefore, will not be able to solve the problems related to the referencing of data which is what really matters when we talk about the right to be forgotten. This aspect, which is now ignored by the GDPR, was correctly understood by the Court of Justice in the Google Spain judgment: it is the presence of those data on a search engine, in fact, to make them truly public on the web, certainly not the presence on an anonymous site lost in the galaxy of the Internet, untraceable for anyone in the absence of an index.

Since it is unlikely that the EU lawmaker would have taken a similar step back from the pronouncements of the Court of Justice, the right to be forgotten, and therefore to de-referencing, would be included in the broader right to erasure. And in fact, consider the right to de-referencing included within the right to erasure is the only way to ensure that the uncertain wording of the GDPR does not weaken the right to be forgotten as emerged in the Google Spain case.

In any case, the answers to these questions will only be confirmed by jurisprudence and, in fact, it is already possible to identify elements by reading the most recent pronouncements of the Court of Justice.

Concluding this brief reconstruction about GDPR, Article 17, the wording of paragraph 2 is appreciated where it expressly mentions the need to take into account the 'available technology', demonstrating to keep in mind the 'technological' approach which should characterize the legislation in these topics. It is very simple, indeed, to impose obligations, if the technology behind it is not taken into account. This type of approach, therefore, should more often be used by the legislator when dealing with topics that, due to their intrinsic characteristics, need a comparison with the technology behind it.

2. Lack of a technological analysis of the law and weakening of the protection of rights: the Google/CNIL case.

[4] About the ineffectiveness of the instrument of consent in order to the processing of personal data see L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale' (n 1), 340 ff.; IA Caggiano, 'Il consenso al trattamento dei dati personali', (2017) 1 DIMT (online), 1 ff.; MC Gaeta, 'Data protection and self-driving cars: the consent to the processing of personal data in compliance with GDPR' (2019) 1 Communications Law, 15 ff.; MC Gaeta, 'La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi' (2018) 1 Dir. Inf., 171 ff.; A Mantelero, 'The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics' (2014) 30 Computer Law & Security Review, 643 ff.; A Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale* (2019) Napoli; J Míšek, 'Consent to personal data processing – The panacea or the dead end?' (2014) 8 Masaryk University Journal of Law and Technology, 69 ff.; DJ Solove, 'Privacy self-management and the Consent Dilemma' (2013) 126 Harv. Law Rev., 1880 ff.

As for jurisprudence, the analysis will start from the recent Google/CNIL judgment[5] of the Court of Justice of the European Union to highlight how this decision neglects to consider the new technologies at the basis of the right to be forgotten. The decision will be then compared with the also recent decision of the Court of Justice in the Facebook case[6], not specifically concerning the right to be forgotten. Indeed, both decisions have in common the lack of adequacy to the technologies they intend to deal with.

Compared to the Google Spain decision, the 2019 Google/CNIL decision certainly represents a step backwards in the protection of the right to be forgotten and a 'good news' for the Mountain View[7] search engine.

The new decision, in fact, territorially delimits the right to be forgotten, limiting the obligation to de-reference to the search engine versions corresponding to all Member States and no longer in all versions of the search engine.

It is appropriate to briefly summarize the terms of the dispute. Already in the aftermath of the Google Spain judgment, Google has considered it a priority to assign a European and non-global value to the right to be forgotten.

Google's approach to the issue of de-referencing was aimed, in essence, to contain 'the damage' to the company resulting from the 2014 decision, recognizing the existence of a de-referencing obligation only with reference to the versions of the search engine whose domain name corresponds to a Member State.

This approach was not shared by the *Commission Nationale de l'Informatique et des Libertés* (CNIL), an independent administrative authority responsible for the protection of personal data in France, which, by the decision of 21st May 2015, has ordered Google to proceed with the cancellation of certain links from the list of results in all versions of its search engine.

In a 2015 document published by Google itself, signed by its Global Privacy Counsel Peter Fleischer and significantly titled 'Implementing a European, not global, right to be forgotten', the search engine had publicly taken a position clearly contrary to the approach made by CNIL. Google even went so far as to say that CNIL's position would make the web the least free place in the world[8].

In support of its thesis, Google stated that the introduction of a generalized de-referencing obligation was disproportionate and unnecessary compared to the purpose, since, according to the data updated to 2015 in the possession of the search engine, about 97% of French users only referred to the local version google.fr, ignoring the others.

---

[5] CJEU, Grand Chamber, 24th September 2019, C-507/17 (Google/CNIL). *See* A Iannotti della Valle, 'Il diritto all'oblio "preso meno sul serio" alla luce della sentenza Google/CNIL della Corte di Giustizia dell'Unione europea' (2020) 2 Rivista AIC, 495 ff.; O Pollicino, 'L"autunno caldo' della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale' (2019) 19 Federalismi.it; G Bevilacqua, 'La dimensione territoriale dell'oblio in uno spazio globale e universale' (2019) 23 Federalismi.it; F Balducci Romano, 'La Corte di Giustizia 'resetta' il diritto all'oblio' (2020) 3 Federalismi.it, 2020, 31 ff.; M Orefice, 'Diritto alla deindicizzazione: dimensione digitale e sovranità territoriale' (2020) 1 Rivista AIC, 2020, 653 ff.

[6] CJEU, Grand Chamber, 3rd October 2019, C-18/18 (Facebook).

[7] P Fleischer, 'Implementing a European, not global, right to be forgotten' [2015], in https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html.

[8] *See* P Fleischer, 'Implementing a European' (no. 7): 'if the CNIL's proposed approach were to be embraced as the standard for Internet regulation, we would find ourselves in a race to the bottom. In the end, the Internet would only be as free as the world's least free place. We believe that no one country should have the authority to control what content someone in a second country can access'. About Google's statement see G Cintra Guimarães, *Global technology and legal theory. Transnational constitutionalism, Google and the European Union* (2019) New York, 155, which observes: 'after all, most companies, Google included, apply worldwide restrictions when they limit access to content that allegedly violates intellectual property rights. If property is enforced globally, so should privacy be'.

Taking note of Google's refusal to comply with the decision taken, the CNIL had therefore imposed a penalty of 100,000.00 euros on Google, with a resolution of 10th March 2016.

Following the CNIL's decision, unfavorable to Google, the search engine manager requested its cancellation by the Council of State of the French Republic (*Conseil d'État*), which had finally referred three related preliminary rulings of interpretation to the Court of Justice of European Union.

With a first preliminary ruling, the *Conseil d'État* asked if the right to de-referencing, as established by Google Spain judgement, should be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive 95/46.

In the event that Question 1 is answered in the negative, the *Conseil d'État* asked if the right to de-referencing should be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester's name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States.

Moreover, in addition to the obligation mentioned in Question 2, the *Conseil d'État* asked if the right to de-referencing should be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the 'geo-blocking' technique, from searches conducted on the basis of the requester's name from an IP address deemed to be located in the State of residence of the person benefiting from the 'right to de-referencing', or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive 95/46, regardless of the domain name used by the internet user searching.

This third question, which undoubtedly would have required a 'technological' analysis by the Court, had been prompted by a proposal by Google itself to the CNIL.

As anticipated, the Court of Justice of the European Union, with the sentence of September 24th, 2019 (case C-507/17), stated that there is no obligation to de-reference in all versions of the search engine[9]. The chosen position, however, was intermediate, since it was considered that this obligation of de-referencing still exists in the domains referable to all Member States (google.fr, google.it, etc.) and not only in the domain referable to the Member State where the request had been made.

The argumentative path followed, and the result achieved by the Court, cannot be free from criticism, since they ignore the advocate general's concerns about technology. [10]

---

[9] The decision is made in relation to a dispute to which the old directive 95/46 was still applicable, repealed with effect from 25th May 2018, but is expressly made also pursuant to regulation 2016/679 (GDPR), whose regulation on the subject of oblivion, as we have seen, cannot however be considered particularly innovative.

[10] The advocate general, in fact, paid wide attention to the resolution of the third preliminary question, relating to the use of the 'geo-blocking' technique to prevent a person from remaining free to search on another version of the search engine. A technique that, it should be remembered, had been proposed by Google itself in the proceedings before the CNIL and which would in any case be circumvented with the use of a proxy server. In any event, despite the attention paid by the advocate general to the technological aspect, the Court does not devote particular space to the resolution of the third question referred or, more generally, to the underlying technological problem. *See* CJEU, 'Opinion of advocate general Maciej Szpunar about case C-507/17', 10th January 2019, in http://curia.europa.eu: '69. On the other hand, if the first question is answered in the negative,

The 2014 decision in the Google Spain case was unfavorable to Google since it guaranteed a right to be forgotten without adequately considering the opposing rights, also entrusting Google with the unwanted role of 'judge' on requests about the right to be forgotten. On the other side, the 2019 decision undoubtedly favors Google's interests, territorially delimiting the protection of the right to be forgotten.

Unfortunately, the decision exposes itself to even greater criticisms than the previous one, not considering that technological developments easily allow to circumvent the scope of the pronunciation and not to take the right to be forgotten 'seriously'.

It is crucial, however, that decisions affecting the digital economy take into account existing technological tools and their adequacy to guarantee the effectiveness of the decision.

Indeed, the Court shows awareness that the de-referencing carried out on all the versions of a search engine constitutes the most suitable way to protect the right to be forgotten. This is because the Internet is 'a global network without borders and search engines render the information and links contained in a list of results displayed following a search conducted on the basis of an individual's name ubiquitous' and that 'in a globalized world, internet users' access — including those outside the Union — to the referencing of a link referring to information regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself'.

The Court, therefore, shows that it is aware of how large the Internet phenomenon is and that deindexing in one version of the search engine cannot, in fact, offer full protection.

In this sense, the decision seems to act almost as an implicit invitation to the EU lawmaker to better regulate the right to be forgotten, since it is stated that 'currently, there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject, as the case may be, following an injunction from a supervisory or judicial authority of a Member State, to carry out such a de-referencing on all the versions of its search engine'.

Although there is awareness of the weakening that the decision will impose on the protection of the right to be forgotten, on the basis of other arguments, the Court states that the operator of a search engine cannot be required to proceed with a de-referencing in all versions of its engine.

The arguments behind the decision essentially relate to the fact that many States outside the Union do not recognize the right to de-referencing or otherwise adopt a different approach for this right: the reference, not too veiled, is to the United States, where the Google Spain judgment received a not too enthusiastic reception.[11] The Court therefore

---

as I propose it should be, such a link is no longer inevitable. As the referring court itself observes, it remains open to a person to search on any domain name of the search engine. For example, the extension google.fr is not limited to searches carried out from France. 70. That possibility may nonetheless be limited by what is known as 'geo-blocking' technology. 71. Geo-blocking is a technique that limits access to internet content depending on the geographic location of the user. In a system of geo-blocking, the user's location is determined with the help of geolocation techniques, such as verification of the user's IP address. Geo-blocking, which is a form of censorship, is deemed to be unjustified in the law of the EU internal market, where it is the subject, in particular, of a regulation designed to prevent professionals carrying out their activities in one Member State from blocking or limiting access by customers from the other Member States wishing to carry out cross-border transactions on their online interfaces. 72. Once geo-blocking is accepted, the domain name of the operator of the search engine used is immaterial. I, therefore, propose to address the third question before the second question'.

[11] For this reason, the Google Spain ruling received a very negative reception in the nation of Google, the United States of America, even on a media level. *See* J Zittrain, 'Don't force Google to "forget"', (2014) The New York Times, 14th May 2014, also online at www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html, according to which: 'This is a form of censorship, one that would most likely be unconstitutional if attempted in the United States'. *See* also G Cintra Guimarães, *Global technology* (n 8), 170, which observes: 'the

affirms that the right to data protection must be considered in the light of its social function and balanced with other fundamental rights. At this purpose, the Court especially emphasizes that 'the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world', also considering that the GDPR, Article 17, has never intended to make any balances regarding the scope of de-referencing outside the Union (not regulating the de-referencing at all).

In fact, through a literal interpretation of both letter b) of the Article 12, and letter a) of the Article 14, paragraph 1, of the previous Directive 95/46, and of Article 17 of the GDPR, the Court clarifies how the EU lawmaker did not intend at all to extend the right to erasure (and therefore the right to be forgotten) outside the borders of the Member States.

In the Court's opinion, currently, the absence of an obligation for the operator of a search engine that accepts a request for de-referencing to carry out such de-referencing on all versions of its engine.

The obligation, however, is to be considered to exist on the domains referable to all Member States, since the European legislator clearly intended to extend, in a uniform way, the discipline regarding the protection of personal data with the choice of the regulatory instrument of the regulation and therefore of a source directly applicable in the Member States: it is precisely the GDPR, therefore, that allows the Court to affirm that de-referencing is to be carried out for all Member States.

However, if some of the Court's considerations appear to be acceptable, making a balance with other fundamental rights, the decision can be criticized in other aspects.

In fact, just like the Google Spain decision, the Google/CNIL decision does not adequately take into account the technological profile and it cannot be considered sufficient, in this regard, to leave Google entirely the burdensome task of taking 'sufficiently effective measures',[12] being totally disinterested in the technical feasibility of protecting the right to be forgotten thus configured and not taking into consideration the easy circumvention that could derive from it.

The Court's idiosyncrasy for the more technical aspects can be seen, first of all, from the substantial failure to answer the third question, not bothering the Court to clarify whether or not the so-called 'geo-block' technique should be used and if this is sufficient to guarantee protection, limiting itself only to imposing on Google the adoption of 'effective' measures.

What matters most, however, even regardless of the application of the aforementioned 'geo-block' technique, is that the territorial delimitation of the de-referencing obligation creates a huge vulnerability in the protection of the right to be forgotten because of a lack of technological analysis of the decision to be made by the Court.

Now, it is true that typing google.com.br or google.co.jp will not be enough to display the results that would appear from Brazil or Japan, thus circumventing the limits imposed by territoriality. However, even if it is not enough to directly enter the URL of a different version of Google, with the use of a proxy server[13] it is still very easy to view a site from Italy as if

---

right to be forgotten […] is a European invention. It does not necessarily match international human rights standards, not to mention the multiple national constitutional standards of different nation states outside Europe'.

[12] Indeed, the Court states that 'it is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Those measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name'.

[13] For the definition of proxy *see* A Luotenen, K Altis, 'World-Wide Web Proxies', in http://courses.cs.vt.edu/~cs4244/spring.09/documents/Proxies.pdf, 1, according to which: 'The primary use

we were in Brazil or Japan, hypotheses that it has been possible to verify personally managing in a few minutes to view Google 'from abroad' while remaining in Italy.

This means that it will always be possible, for those who are really interested in carrying out a 360-degree search on a person, to also trace the results for which the right to be forgotten has been recognized, thus making the (geographically delimited) implementation of that right vain.

The protection would remain effective, therefore, only in front of the average user and not so interested at all in the search for information, which will make only a quick search on his local version of the search engine, without further deepening. On the other hand, the right to be forgotten would be ineffective for all those really interested in finding out who they are dealing with.

The question at this point is: has the Court of Justice actually intended to restrict the scope of the right to be forgotten? Or is the decision only the result of technological inaccuracy?

The Court, on the one hand, showed that she is aware the extent of the Internet phenomenon; on the other hand, however, the worst risk seems to be considered that a person, who is physically located outside the European Union, may view information relating to a person whose center of interest is located within the Union.

These considerations suggest that the Court ignores the real risk inherent in the decision: in fact, as already said, a person, physically located in a Member State of the Union, may display every information for which oblivion has been recognized, through the use of a proxy server, a methodology within everyone's reach with a simple Google search.

3. What the Google/CNIL and the Facebook cases have in common: The Court does not care about the technology underlying the application of the law.

The Google/CNIL decision may be compared with another very recent decision by the Court of Justice of the European Union concerning Facebook (case C-18/18), dated 3rd October 2019, oriented towards completely opposite criteria but that with the pronunciation analyzed above has in common the lack of attention to the technology underlying the application of the judgment.

The present case concerned the sharing, by a Facebook user, on his social network page and without limitation of visibility, of a news published by an online information site. The 'post' included the photo of a member of the Chamber of representatives of the Austrian Parliament and an own comment with contents considered defamatory by Austrian Courts at first and second degree.

Finally, the Austrian Supreme Court decided to raise three questions for a preliminary ruling to the Court of Justice of the European Union, essentially asking if there's a duty on a hosting provider such as Facebook to remove the content of information which is identical to the content of information previously declared to be illegal, or to block access to that information, irrespective of who requested the storage of that information; to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be illegal, or to block access to that information, and to extend the effects of that injunction worldwide.

The Facebook judgement confirms the substantial indifference of the Court of Justice to technological issues, already seen in the Google/CNIL decision, but in a different way. With the decision in C-18/18, in fact, the Court imposes over Facebook an obligation to remove

---

of proxies is to allow access to the Web from within a firewall […]. A proxy is a special HTTP [HTTP] server that typically runs on a firewall machine. The proxy waits for a request from inside the firewall, for- wards the request to the remote server outside the firewall, reads the response and then sends it back to the client'.

contents identical and/or equivalent to those declared illegal, worldwide and regardless of the technical feasibility of what is imposed.

The removal, in this case, would take place all over the world and not only in the Member States, differentiating in this way from the approach followed for the Google/CNIL decision.

In fact, despite the assonances of the issue treated with the right to be forgotten, the 'method' used by the Court to reach the decision appears to be based on different parameters compared to the Google/CNIL judgment, perhaps not adequately justified by the 'silences' of the GDPR about the right to be forgotten and the not too 'richer' wording of Directive 2000/31/EC, applicable to the present case.[14]

It is indeed likely that the Court of Justice wanted to react to the establishment of Facebook's Oversight Board,[15] an own 'Court' on whose effective independence it is legitimate to doubt. The Court is supposed to review content and issue reasoned and binding decisions regarding the contents published on the social network, strengthening a model of private jurisdiction to the detriment of public jurisdiction. Without going further on this aspect, which has already been the topic of specific studies,[16] it seems appropriate to make some observations, in relation to the Facebook case, from the technological point of view. In fact, in the Facebook case, the Court does not care about the technological limitations that would prevent the enforcement of European Union law outside the borders of the European Union, effectively obliging Facebook to implement the codification of very complicated algorithms to ensure implementation in all the world of this principle of law. These algorithms are made even more complicated by the need to find messages with 'the content of which remains essentially unchanged': in fact, how could the algorithm identify those posts that the Court defines as those 'whose content remains, in essence, unchanged' and in 'the content of which, whilst essentially conveying the same message, is worded slightly differently'? Although the Court recognizes that, based on Article 15, Directive 2000/31/EC,[17] there cannot realistically be a monitoring obligation on Facebook,[18] actually it is not clear which algorithm can guarantee an automatic evaluation that has an acceptable margin of error and that does not end up overwhelming activities that constitute a free expression of thought, such as satire.

Ultimately, the Court requires Facebook to use undoubtedly complex technologies whose existence it essentially ignores (nor it seems to worry about them). In this way, it exposes Facebook to the risk of an inadequacy of the existing technology for the law. Therefore, a probable technological inadequacy which however conceals a much safer inadequacy of law compared to the world of new technologies.

In conclusion, undoubtedly the matter dealt with in the Facebook judgment is partially different from that of the Google/CNIL judgment, just as the regulatory framework is

---

[14] *See* Art. 18, para. 1, Dir. 2000/31/EC: 'Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved'.

[15] *See* O Pollicino, 'L''autunno caldo", 10 ff.

[16] *See* A Iannotti della Valle, 'A Facebook Court is born: towards the 'jurisdiction' of the future? (2020) 1 EJPLT, 98 ff.

[17] Art. 15, para. 1, Dir. 2000/31/EC: 'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity'.

[18] In fact, the Court states: 'Differences in the wording of that equivalent content, compared with the content, which was declared to be illegal, must not, in any event, be such as to require the hosting provider concerned to carry out an independent assessment of that content'.

different, but this does not justify such a diversity of approach compared to the Google/CNIL judgment.

The only common aspect, which really links the two pronouncements made after a few days, is the substantial absence of attention to the technology 'behind' the law, beyond the style formulas used here and there.

As a matter of fact, the absence of real attention to the technology underlying the legal statements seems to be the leitmotif of all the pronouncements analyzed, from Google Spain to the most recent Google/CNIL and Facebook pronunciations.

4. The protection of fundamental rights needs a technological approach to law.

As has been shown, what the two relevant pronouncements analyzed above have in common is the lack of real attention to the technology underlying the application of the law.

The European Union is well aware that the digital revolution is giving one of the greatest transformations to the world since the era of the industrial revolution and is equally aware that we must be ready for the ever greater penetration of new technologies into our lives:[19] this, obviously, with the instruments available to the Union itself, and therefore with the law. On the one hand, the reference is to soft law which, in the matter of new technologies, often precedes hard law and tends to occupy its spaces in an almost uncontrollable way;[20] on the other hand, however, there is the awareness that the more serious problems posed by new technologies will require the intervention of hard law.

With specific regard to the right to be forgotten, the real problem lies in the fact that

---

[19] *See* European Commission, 'Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All', COM (2017) 228, in https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM:2017:228:FIN, where there is a strong awareness of the need for legal intervention in the digital world: 'Successive waves of technological change have transformed human societies and economies, with long-term benefits for both economic growth and quality of life. The current digital revolution has the power to do so again. […] The completion of the EU Single Digital Market also needs a clear and stable legal environment to stimulate innovation, tackle market fragmentation and allow all players to tap into the new market dynamics under fair and balanced conditions. This will provide the bedrock of trust that is essential for business and consumer confidence. […] It is critical for all parties to ensure that the measures are adopted, fully implemented and effectively enforced in a timeframe that is coherent with the fast development of a digital economy. The Commission will bring to bear the full range of policy instruments and funding opportunities to help make this happen, but the full support of Member States, the European Parliament, the Council and stakeholders is essential; otherwise the Digital Single Market will simply not become a reality'. For some initial attempts to implement the European Commission's proposals, see, for example, the proposal for a regulation concerning respect for privacy and the protection of personal data in electronic communications, intended to replace Directive 2002/58/EC with a regulation directly applicable, on the model of the GDPR. *See* European Commission, 'Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', 10th January 2017.

[20] As far as the European Union is concerned, the reference is evidently to a soft law which is still of European Union origin, such as the guidelines of the European Data Protection Board (EDPB). Precisely on the subject of the right to be forgotten, a consultation was held until 5 February 2020 as part of the procedure for approving the new guidelines, the draft of which is already available online. *See* EDPB, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR', in https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_it. Still on the subject of the right to be forgotten, while remaining at the soft law level, see also the guidelines WP29, 'Guidelines on the implementation of the judgment of the Court of Justice of the European Union judgment in the case "Google Spain and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González" (C-131/12)', 26th November 2014, in https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=667236. With regard to the soft law relating to the protection of personal data, see the aforementioned paper MC Gaeta, 'Hard law and soft law on data protection' (n 1).

personal data become substantially indelible once they have been published online. For example, consider the hypothesis in which personal data is put on the Internet and, at a later time, the same is deleted in the application of the GDPR, Article 17: this does not exclude that someone has already saved the web page that contained personal data on their device. However, that personal data will never be erased.

This is why the Google Spain decision had identified the true form of protection, in terms of the right to be forgotten online, precisely in de-referencing: this is because, even if a personal data still 'exists' on the web and is in fact indelible, it will no longer exist for almost all the web audience, if not (more) traceable through a search engine.

But the delicacy of the issue of right to be forgotten is even more evident with a technological analysis of law. In fact, a technological reading of the aforementioned decisions highlights a considerable vulnerability in the protection of the right to be forgotten, not adequately taken into consideration by the Court of Justice: as has been shown, indeed, it is still possible to access from Italy or from another part of the world to a different version of the search engine where the news has not been de-referenced through the use of a proxy server, a methodology accessible to all and identifiable with a simple Google search.

Therefore, it is crucial to think about a possible balance between innovation and the protection of fundamental rights. At this purpose, the study carried out so far leads to the identification of a method for the protection of fundamental rights in the digital age, based on a serious technological analysis, which should be carried out both by the legislator and by the jurisprudence: it will be possible to provide the fundamental rights in the digital age of a more effective protection only if the functioning of information and communication technologies is really be taken seriously.

More specifically, a technological analysis of law should be based on a hybridization of knowledge.[21] The continuous technological advances of our days require that lawyers interact more and more with technical specialists who are experts in the new technologies that the law should regulate and are aware of the mechanisms underlying their functioning and development. Therefore, taking into account the concrete functioning of the technologies, also interacting with engineers and mathematicians, is sometimes the only way to really verify whether the law has achieved its purpose.

[21] L Gatt, R Montanari, IA Caggiano (eds), *Privacy and Consent. A Legal and UX&HMI Approach* (forthcoming), marks an evolution of the authors' thesis compared to the already innovative perspective of L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale' (no. 1).