BRILL

THE ITALIAN REVIEW OF INTERNATIONAL AND COMPARATIVE LAW 1 (2021) 277–310

The Italian Review of International and Comparative Law

brill.com/iric

The Transatlantic Dimension of the Judicial Protection of Fundamental Rights Online

Oreste Pollicino
Full Professor of Constitutional Law, Bocconi University, Milan, Italy
oreste.pollicino@unibocconi.it

Abstract

This article underlines the role of courts in ensuring the protection of fundamental rights in the digital environment. In particular, the focus will be on the European and the US judicial dimension, looking at the right of freedom of expression and data protection. Section 2 underlines how judges rely on metaphors to address digital matters. Sections 3 and 4 respectively look at the role of courts in shaping the protection of freedom of expression and of privacy and personal data across the Atlantic. Section 5 provides two examples of the role of European courts in extending values across the Atlantic.

Keywords

judicial protection – fundamental rights online – US – EU – privacy and data protection

1 Introduction

Against a backdrop of uncertainty triggered by the COVID-19 pandemic, judicial globalization has increasingly placed courts in a privileged position to identify risks of potential collisions between interconnected legal regimes in terms of the protection of fundamental rights.[1] Cooperation between courts

1 As observed by Slaughter, this is a "process of judicial interaction across, above, and below borders, exchanging ideas and cooperating in cases involving national as much as international law". SLAUGHTER, "Judicial Globalization", Virginia Journal of International Law, 2000, p. 1103 ff., p. 1104.

 | DOI:10.1163/27725650-01020004

forges closer bonds between different yet interacting orders,[2] while contributing to the adaptation of legal systems to the new global challenges. This dynamic – and, more generally, the role and the impact of judicial activity – is even more important within the digital domain.

The increase in the role of judges in the information society can be explained in different ways. The main (substantive) reason for this increase focuses on the traditional gap between law and technology that occurs when the law lags behind technological advances. The burden of making up for this inevitable legislative inertia – both at a national and supranational level – falls heavily on the shoulders of the courts. The new factual and legal context created by the Internet has further widened this gap, thus highlighting the lack of judicial expertise to deal with new scenarios that have emerged alongside new technologies. In this context, political inertia (which is not always forced, since power is sometimes delegated to courts with a view to avoiding difficult choices) has fostered judicial imagination – along with the resulting use of metaphors and frames for legal systems – within the digital era.[3]

However, it is worth observing that the general increase in judicial momentum has contributed to an imbalance between judicial and political actors struggling to find new solutions for new challenges associated with the protection of fundamental rights online. In the current era of legal and economic globalization, it is notable that traditional constitutional governance is altering the characteristics that marked the process of its development in previous centuries. Post-modern constitutionalism is characterized by a process of fragmentation in terms of sovereignty, followed by a parallel process of reconfiguration within a multilevel and polycentric system.[4] Within this context, it is

2 Beside the amplification of judicial momentum, there is also a parallel and more worrying process of privatization of digital justice. More precisely, on the one hand the major social networks are implementing rules related to the institution of last instance appeal bodies such as the so-called Facebook Supreme Court (see KLONICK, "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression", Yale Law Journal, 2020, pp. 2418 ff.) and, on the other hand, as recently written by the President of European Court of Human Rights Robert Spano, an issue emerges related to "the ongoing concern with the question of remedies and review mechanism for disputes online and the increasing tendency to privatize or outsource to the platforms the final determination of the scope and the content of free speech and privacy online". SPANO, "Summary of the Issues Discussed during the Seminar: An Aerial View", in BRATZA et al. (eds.), *Human Rights Challenges in the Digital Age: Judicial Perspectives*, Strasbourg, 2020, p. 201 ff., p. 209.

3 STONEBRIDGE, *The Judicial Imagination: Writing After Nuremberg*, Edinburgh, 2011. See also DEL MAR, *Artefacts of Legal Inquiry: The Value of Imagination in Adjudication*, Oxford, 2020.

4 TEUBNER, "Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory?", in JOERGES, SAND and TEUBNER (eds.), *Constitutionalism and Transnational Governance*, Oxford, 2004, p. 3 ff.

essential to establish the correct and most direct interconnections between the different constitutional centers that frame the new polycentric global order at a national, supranational and international level. It is a commonly held opinion that the multilevel network of judicial decisions provides the best pathway for interconnections.[5]

The "road to juristocracy" is thus one of the main trends within post-modern constitutionalism in the era of judicial globalization.[6] In other (more convincing) words, judicial power has moved from being the "weak ring" of the chain to becoming the strong one.[7] Judge-made law seems to offer more flexible and pragmatic solutions than legislative or administrative acts, in addressing the challenges of legal systems as they become increasingly interdependent, subject to constant and unforeseen transformation. To put it simply, global governance seems to prefer the language of the "law in action" rather than the ink of the "law in the books".[8]

If this is true, before returning to the value that digital technologies add to the language of the law in action in a globalized information society, it is important to make one point of clarification regarding a stereotype that emerges in the discourse surrounding judicial globalization and the relationship between the European legal framework and the national constitutional dimension.[9] Indeed, in order to avoid the mistake made by those who, when

5 L'HEUREUX-DUBE, "The International Judicial Dialogue: When Domestic Constitutional Courts Join the Conversation", Harvard Law Review, 2001, p. 2049 ff.; SLAUGHTER, "A Global Community of Courts", Harvard International Law Journal, 2003, p. 191 ff.; SLAUGHTER, *A New World Order*, Princeton, 2004; CHOUDRY, "Globalization in Search of Justification: towards a Theory of Comparative Constitutional Interpretation", Indiana Law Journal, 1999, p. 821 ff.; MCCRUDDEN, "A Common Law of Human Rights?: Transnational Judicial Conversations on Constitutional Rights", Oxford Journal of Legal Studies, 2000, p. 499 ff.; SHAPIRO and STONE SWEET, *On Law, Politics and Judicialization*, Oxford, 2002; STONE SWEET, *Governing with Judges: Constitutional Politics in Europe*, Oxford, 2000.

6 SLAUGHTER, *cit. supra* note 1, p. 1104 ff.; HIRSCHL, *Towards Juristocracy: The Origins and Consequences of the New Constitutionalism*, Cambridge (MA), 2004; TATE and VALLINDER (eds.), *The Global Expansion of the Judicial Power*, New York, 1995.

7 DAHRENDORF, *Dopo la democrazia*, Roma-Bari, 2003, p. 65.

8 The dichotomy between "law in action" and "law in the book" was originally underlined by POUND, "Law in Books and Law in Action", American Law Review, 1910, p. 12 ff.

9 ORUCU, *Judicial Comparativism in Human Rights Cases*, London, 2003; FRANCIONI, "International Law as a Common Language for National Courts", Texas International Law Journal, 2001, p. 587 ff.; SKOURIS, "The Position of the European Court of Justice in the EU Legal Order and its Relationship with National Constitutional Courts", Zeitshrift fur Offentliches Recht, 2005, p. 323 ff.; STONE SWEET, "Constitutional Dialogue in the European Community", in SLAUGHTER, STONE SWEET and WEILER (eds.), *The European Court and National Courts. Doctrine and Jurisprudence: Legal Change in its Social Context*, Oxford, 2004, p. 304 ff.

looking at a finger pointing at the moon, focus on the finger and not on the moon, it should be noted that the notion of judicial dialogue is nothing more than a sign of the presence of something else behind it, which is often particularly problematic.[10]

Therefore, the need to maintain a symmetrical balance between judicial and political powers in the digital era may not come from court-based hyper-activism or legislator-based inertia, but from the judicial ability to promptly react. Since judges appear to be best placed to identify the possible collisions between fundamental rights online and, consequently, to be the bodies best equipped to provide initial answers for these collisions, the systemic answer (but not the final answer, which is always left to the Constitutional Court) should come from the legislative branch that has the power to respond *lato sensu* and codify the relevant case law. In other words, if, as it has been said, the new round of judicial globalization constitutes a response to a pre-existing problem involving a possible conflict between fundamental rights, the legislature should offer a further response, after the initial judicial response.

Within this framework, this article underlines the role of courts in ensuring the protection of fundamental rights in the digital environment. In particular, the focus will be on the European and the US judicial dimension, looking at the right of freedom of expression and data protection. Section 2 underlines how judges rely on metaphors to address digital matters. Sections 3 and 4 respectively look at the role of courts in shaping the protection of freedom of expression and of privacy and personal data across the Atlantic. Section 5 provides two examples of the role of European courts in extending values across the Atlantic.

10 It is perhaps worth making clear that the term "judicial dialogue" is used here in a twofold way. Firstly, it refers to judicial relations between "vertically" interconnected legal orders situated at different, not hierarchically based, levels (national, European, and international); secondly, it refers to the direct relationship between courts rather than the broader situation of constitutional cross-fertilization and judicial borrowing between legal systems in which the judges generally conduct a form of dialogue through mutual citations. See JACOBS, "Judicial Dialogue and the Cross Fertilization of Legal System: The European Court of Justice", Texas International Law Journal, 2003, p. 547 ff.; ROSAS, "The European Court of Justice in the Context: Forms and Pattern of Judicial Dialogue", European Journal of Legal Studies, 2007, p. 1 ff.

2 Judges and Metaphors

One of the principal consequences of the enhanced role of the judiciary in the digital age is that the courts now have broader room for manoeuvre when using metaphorical language and judicial frames related to the balancing of fundamental rights. In other words, as mentioned above, the difficult task of adapting "traditional" legal rules to new technological paradigms is increasingly dependent upon judicial imagination.

In order to fully understand the relevance of metaphors and frames in the new technological context, it is necessary to take a step back to consider the theoretical background. As far as metaphorical language is concerned,[11] the shift from a conception of the metaphor as exclusively linguistic to a conception involving a cognitive process and framework comes from Lakoff's and Johnson's 1980 publication of the text, *Metaphors We Live By*.[12] This study marked a genuine, paradigmatic shift in research on the role of metaphors within a wide variety of fields (from politics to religion, from economics to the law, etc.). Researchers proposed two central theses on modern cognitive linguistics: the idea that language is not independent from other human cognitive activities such as perceiving, reasoning, etc., and the close link between meanings and concepts.

Therefore, Lakoff's and Johnson's fundamental theoretical assumption is that a metaphor is more a fact of thinking than language.[13] According to this view, every metaphor has a "source domain," a "target domain," and "source-to-target mapping."[14] Theorists go on to claim that the metaphorical processes developed through the shift from one domain to another reflect the cognitive structures that condition human understanding.

Metaphorical language performs an irreplaceable role within the law. In fact, many legal categories and institutes have been constructed through metaphorical processes. Within that ambit, metaphors perform a constitutive function of legal reality itself. Consider, for instance, the categories of "legal person" or "sovereignty" in all of its manifestations (State, national, popular, etc.). As Blavin and Cohen write "[m]etaphors structure the way lawyers conceptualize legal events as they infiltrate, consciously and unconsciously, legal discourse".[15]

---

11 MORELLI and POLLICINO, "Metaphors, Judicial Frames and Fundamental Right in Cyberspace", American Journal of Comparative Law, 2020, p. 616 ff.

12 LAKOFF and JOHNSON, *Metaphors We Live By*, Chicago, 1980.

13 CONTINI, "La forza cognitiva della metafora", I castelli di Yale online, 2016, p. 14 ff.

14 LAKOFF, *Women, Fire, and Dangerous Things. What Categories Reveal about the Mind*, Chicago, 1987, p. 276.

15 See BLAVIN and COHEN, "Gore, Gibson, and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary", Harvard Journal of Law & Technology, 2002, p. 265 ff.,

These scholars have analysed three different ways of describing the Internet in metaphorical terms: "the information superhighway", "cyberspace", and the Internet as a "real space". They have shown how these conceptual metaphors influence the solution to legal problems involving the Internet.[16] However, this aspect is not always fully appreciated and metaphorical language has not always been viewed favorably within arguments deployed by legal practitioners (above all in those used by courts). Thus, for example, within the US debate, Posner has asserted that analogies cannot always resolve legal disputes since "[t]o say that something is in some respects like something else is to pose questions rather than answer them".[17]

And before Posner, Cardozo argued – wearing his judge's hat – that "metaphors in law are to be narrowly watched, for starting as devices to liberate thought, they end often by enslaving it".[18] It is of singular significance that, in condemning metaphors in this manner, Cardozo did so on the basis of a dual metaphor, namely the liberation of thought and its reduction to slavery. More generally, various US scholars have viewed the creation of new fictions by the courts with suspicion, arguing that such activity jeopardizes the "judicial candor" that ought to characterize the decision-making processes of both judges and courts.[19]

Based on the conceptual and cognitive paradigm of the metaphor, theorists offer another paradigm as a means of studying issues that have arisen in relation to judicial protection for fundamental rights in the digital environment: the frame. More specifically, particular attention must be dedicated to the interactive conception and the theory of conceptual metaphors. The interactive conception, which theorists (above all Black) developed during the 1950s,[20] considers the metaphor to be the result of a process of semantic

---

p. 266; JOO, "Contract, Property, and the Role of Metaphor in Corporations Law", University of California – Davis Law Review, 2001, p. 779 ff. See also HUNTER, "Cyberspace as Place and the Tragedy of the Digital Anticommons", California Law Review, 2003, p. 439 ff.

16 The same idea is behind the book written by Larsson that uses conceptual metaphor theory "to strengthen the awareness of the strong metaphoricity in contemporary understandings of the Internet". LARSSON, *Conceptions in the Code. How Metaphors Explain Legal Challenges in Digital Times*, Oxford, 2017.

17 POSNER, *How Judges Think*, Cambridge (MA), 2008, p. 181.

18 Court of Appeals of the State of New York (USA), *Berkey v. Third Avenue Railway Co.*, Judgment of 31 December 1926, 244 N.Y. 84 (NY 1926), para. 95, available at: <https://casetext.com/case/berkey-v-third-avenue-railway-co-1>.

19 SHAPIRO, "In Defense of Judicial Candor", Harvard Law Review, 1986–1987, p. 731 ff.; SMITH, "New Legal Fictions", Georgetown Law Journal, 2006–2007, p. 1484 ff.

20 BLACK, *Models and Metaphors. Studies in Languages and Philosophy*, Ithaca, 1962, p. 25; BLACK, "Metaphor", Proceedings of the Aristotelian Society, 1954, p. 273 ff.; RICHARDS, *The Philosophy of Rhetoric*, Oxford, 1936.

interaction or, more specifically, the product of the combination of an expression used metaphorically (the "focus") and the enunciative structure within which the expression is framed (the "frame"). The conceptual and cognitive paradigm of the metaphor presupposes the fundamental concept of "frame". Within the specific context of legal argumentation, a "judicial frame" is the expressive structure and, more broadly, the reference context for the reasoning set out in the judgment.

As shown in this article, the particular judicial frame chosen by a court can result in differently balanced and/or divergent solutions even in cases that are essentially similar or identical. In other words, the notion of frame must be shifted from cognitive studies to the theory of interpretation and argumentation. As Sajó and Ryan point out, "translation of a technology and its consequences into the legal frame is not automatic".[21] This is where courts play an important role through the judicial process of translating something new into the language of past legal models by means of the judicial framing technique.[22]

It is important to stress how this activity – based on a "conceptual transfer" from the world of atoms to the world of bits – is not neutral but is rather based on the frame of values on which it is founded. This explains why, for instance, digital privacy gained more protection compared to the non-digital world, most notably in the Court of Justice of the European Union's ("CJEU") case law. In particular, we must focus on the impact of the balance struck by the court and, consequently, on the level of protection for the rights at stake. Within this context, Lakoff's concept of frame helps us to identify a constitutive use of metaphors. The notion of the "frame" is evident in this context. By transferring this concept from the field of language theory and cognitive science to the theories of interpretation and argumentation, and, subsequently, by identifying judicial frame as a subcategory of the frame, we can define the court's value options within a specific judicial balancing operation.

However, in any case, those in charge of interpreting the law, and in particular the courts, cannot refrain from exercising – in the words of White – their "legal imagination",[23] whether this involves reconsidering existing rules based on changes in technological circumstances, or a shift from the material to the intangible. The specific solution that is chosen does not change the role of the courts, especially constitutional (or supreme) courts in performing

21 SAJÓ and RYAN, "Judicial Reasoning and New Technologies: Framing, Newness, Fundamental Rights and the Internet", in POLLICINO and ROMEO (eds.), *The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe*, London, 2016, p. 3 ff., p. 7.

22 *Ibid.,* p. 8.

23 WHITE, *The Legal Imagination*, Chicago, 1985.

a highly delicate role as they are required to choose between constitutional "translation" and constitutional caution.[24] It is for courts to decide whether to translate the values behind the original constitutional principles in order to cover the new technological framework, or to adopt an approach characterized by self-restraint, leaving this task to policy-makers. In other words, it is necessary to understand whether judicial deference or judicial activism would be the most appropriate approach in such cases, while considering the important question regarding the relationship between political and judicial power within the context of Internet law.

Although the scenario is much more nuanced, it is possible to identify two alternative options for courts when confronted with new technologies: re-contextualizing the relevant parameters by creating new frames in the light of the technological environment, or adopting a position of judicial deference towards political choices. The latter is a solution supported, for example, by Lessig: "My sense is that, knowing nothing, or at least not very much, terrified by the threats of which they don't know, these judges will defer to democratic authority".[25]

Still, there is a problem: courts are required to adjudicate on the cases that come before them. They do not have much choice regarding this matter. In this regard, Justice Kennedy's dissenting opinion in *Denver Area Educational Telecommunications Consortium* on the regulation of cable television is emblematic.[26] When considering the technological aspects of the case, which were new at the time, he said, "we don't know yet, but here's the best we can".[27] Doubt and caution may be reasons for the US Supreme Court's reluctance to take a case, but when the Court does take a case, it may be difficult to accept the Court's position of undecidedness.[28] This is why metaphors and analogies to other areas of First Amendment case law become a responsibility, rather than the luxury that the plurality considers them to be. In other words, a decision has to be reached in each case and the technological factor has to be dealt with in some way. Hence, the frame – which linguistic scientists construe by as a cognitive structure that facilitates comprehension – becomes a judicial

24 SUNSTEIN, "Constitutional Caution the Law of Cyberspace", University of Chicago Legal Forum, 1996, p. 361 ff.

25 LESSIG, "Reading the Constitution in Cyberspace", Emory Law Journal, 1996, p. 869 ff., p. 874.

26 Supreme Court of the United States (USA), *Denver Area Educational Telecommunications Consortium v. FCC*, Judgment of 28 June 1996, 518 U.S. 727 (1996), available at: <https://supreme.justia.com/cases/federal/us/518/727/>.

27 PRICE, *Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power*, Cambridge (MA), 2002, p. 152.

28 *Ibid.*

frame; as such, it is an argumentative technique that can be used to persuade either by metaphors or by analogy, that is by shifting from the familiar archetype to the new technological context.

It is therefore possible to draw a distinction between a frame of resistance to technology on the one hand and a frame of openness to technology on the other hand. These value frames can be encapsulated in the courts' propensity to either recognize or reject the technological factor in question. In any case, whichever frame is chosen between continuity and discontinuity within the pre-existing technological framework, the operation will never be neutral as it is conditioned by one other important factor, which many legal practitioners do not account for in this field. This is specifically the possibility that the juxtaposition between the Hartian external and internal point[29] of view is framed in the more incisive understanding of MacCormick. Consequently, courts may adopt either a perspective that is internal to the new technology, or one that is external to it.[30]

Before the advent of the Internet, the *Olmstead* judgment made the juxtaposition between the external and internal points of view vis-à-vis technological developments clear, particularly regarding the dissenting opinion of Justice Brandeis.[31] According to the majority opinion, the use as evidence in a trial of telephone conversations intercepted by federal agents without having previously obtained a court order did not violate the Fourth Amendment because listening to a private telephone conversation does not require a physical search or entry into a person's private space.[32] By contrast, Brandeis used a different judicial frame in stating his dissenting opinion on the basis of what he perceived as technological discontinuity between the new technology (at that time) and the *status quo*. He proposed a teleological interpretation of search and seizure based on the Fourth Amendment.

One might ask why the judges sitting at the same time on the same court were so diametrically opposed in their approaches. The answer can be found by distinguishing between the internal perspective of the "player" and the external perspective of the "outsider". Whilst the majority in *Olmstead* adopted an external perspective with regard to the person whose telephone conversation was tapped, Brandeis adopted his own judicial frame as an internal

29 HART, *The Concept of Law*, Oxford, 1961.

30 MACCORMICK, *Legal Reasoning and Legal Theory*, Oxford, 1978.

31 Supreme Court of the United States (USA), *Olmstead v. United States*, Judgment of 4 June 1928, 277 U.S. 438 (1928), available at: <https://supreme.justia.com/cases/federal/us/277/438/>.

32 *Ibid*.

player (and not as an outsider). He considered the new technology at that time from a perspective that was internal, conceptualizing the telephone network as a privileged means for creating a virtual closet in which secrets could be whispered.[33] On the basis of this value frame, which was structurally different from the frame adopted by the majority, Brandeis did not have any difficulty in concluding that intrusion (albeit not physical but nonetheless an intrusion) had occurred within the private sphere of the person whose conversation was tapped, thereby violating the Fourth Amendment.

Whilst the possible juxtaposition between the external perspective and the internal perspective vis-à-vis the identification of technological developments might have been clear even before the advent of the Internet, the invention of the web has resulted in the fertile soil in which the dialectic between openness and resistance to new technologies has flourished. This should come as no surprise, especially considering that the Internet is the only medium equipped with its own constitutive spatial metaphor: "cyberspace". This is because, in contrast to other technologies, the context, or the frame of reference, is so constitutive and self-sufficient in nature that it competes with physical reality and pushes any court to choose the perspective that best characterizes their judicial frame when addressing Internet law.

Recalling the two quotations cited above, the Italian *Corte di Cassazione* seemed to adopt an internal perspective by privileging the "figurative meaning over the technical meaning", whereby it considers the intangible reality as a space in which the court could reconsider traditional categories. Meanwhile, Easterbrook's[34] ironic and provocative reference to the "law of horses" is closer to an external perspective that takes the analogue realm as a point of reference for the application of certain rules. In this view, the digital realm is a mere accessory, to which it is possible, and indeed advisable, to transfer traditional legal categories *sic et simpliciter*.

The cases mentioned above point towards the role played by judicial frames in the shift from atoms to bits and the resulting increase in judicial momentum. The focus on the judicial protection of freedom of expression, privacy, and personal data across the Atlantic can provide examples of this trend.

33 *Olmstead v. United States* case, *cit. supra* note 31.

34 EASTERBROOK, "Cyberspace and the Law of the Horse," University of Chicago Legal Forum, 1996, p. 207 ff., p. 208.

3 Judicial Protection of Freedom of Expression Online

European courts have played a critical role in shaping the protection of the right to freedom of expression in the digital era. When called upon to rule on alleged violations of freedom of expression on the Internet, the European Court of Human Rights ("ECtHR") has shown an attitude to reshape the expansive scope that previously characterized its case law on the application of Article 10 within the analogue world. This reining in of the scope and reach of freedom of expression on the web appears to be rooted in the assumption that the use of digital technologies entails a greater degree of offensiveness compared to other interests that intersect with the freedom of expression. Whilst it must be noted that the "relative" status of the fundamental rights protected under the European Convention on Human Rights ("ECHR") and their potentially subsidiary status within balancing operations is certainly nothing new, this aspect appears to have been heightened within the case law concerning the Internet.

A precursor to this "narrow" reading, as it were, may be found in the ruling *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* from 2011,[35] in which the Court underlined that the capacity of the Internet to pose harm to the exercising of human rights, "particularly the right to respect for private life, is certainly higher than that posed by the press". Therefore, the Court added that "the policies governing reproduction of material from the printed media and the Internet may differ".

In contrast to the US Supreme Court which immediately identified how a potential expansion of the web (defined as "phenomenal") could also expand the space within which freedom of expression could be exercised (as will be seen below in the 1997 case *Reno v. ACLU*),[36] the ECtHR appeared to be primarily concerned with the critical aspects of the use of the Internet as well as the risks associated with a more significant violation of other fundamental rights that were likely to clash with the freedom of expression and information.

It must be recalled that the ECtHR has always considered freedom of expression, and in particular freedom of the press, a kind of touchstone (the "canary in the mine") for the democratic nature of a legal system. It would appear that the extent of this protection as consolidated within the case law of the ECtHR

35 *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, Application No. 33014/05, Judgment of 5 May 2011.

36 Supreme Court of the United States (USA), *Reno v. American Civil Liberties Union*, Judgment of 4 June 1928, 521 U.S. 844 (1997), available at: <https://supreme.justia.com/cases/federal/us/521/844/>.

has changed. First, in the judgment *Stoll v. Switzerland* of 2007,[37] the Court appeared to endorse the imposition of more stringent obligations on online journalists compared to those working with the printed press. Furthermore, the court upheld a similar view in another case in 2008. More specifically, in *KU v. Finland*, the Court observed that, although freedom of expression and confidentiality of communications are primary considerations, such guarantees cannot be absolute and must yield, on occasion, to other legitimate imperatives, such as the prevention of disorder or crime, or the protection of the rights and freedoms of others.[38]

Naturally, it must not be forgotten that the decisions of the ECtHR are largely based on specific circumstances that gave rise to the application in the specific individual cases. This means that the reach of apparently radical judgments must be scaled back, or in any case not overstated. This applies, for example, to the case of *Delfi AS v. Estonia,*[39] a 2015 decision in which the Grand Chamber confirmed the trend more open to possible restrictions on online freedom of expression. In particular, the Court stated that: "defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online".

The Court held that the imposition on the operator of an online information portal of the obligation to pay a fee, albeit minimal (in that case, EUR 320), as compensation for the harm suffered by a person as a consequence of certain defamatory comments that had remained accessible for around six weeks at the bottom of an article published online did not constitute a disproportionate restriction on freedom of expression in view of the need to strike a balance with the protection of the personality rights (such as honour and reputation) of the person who had been defamed.

It should be pointed out that the same case would most likely have been decided differently by the CJEU, whose power of scrutiny would however have been based on criteria different than those adopted by a human rights court such as the ECtHR, being rooted, by contrast, in the issue of the potential liability of the operator of the online portal under Directive 2000/31/EC. The judgment in question is undoubtedly problematic and difficult to reconcile with EU law: leaving aside the need to adopt a perspective of inquiry that is not misleading (the *thema decidendum* here was whether the requirement for monetary compensation could constitute an unjustified violation of Article 10 of

37 *Stoll v. Switzerland,* Application No. 69698/01, Judgment of 10 December 2007.

38 *KU v. Finland,* Application No. 2872/02, Judgment of 2 December 2008.

39 *Delfi AS v. Estonia,* Application No. 64569/09, Judgment of 16 June 2015.

the European Convention, and not the compatibility of such an outcome with Directive 2000/31/EC), the judgment leaves the door open to the possibility of finding the editor of a portal liable under certain circumstances for unlawful content published by third parties.

These indications are most telling when comparing the scope of the *Delfi* judgment with the judgment issued several months later in which the ECtHR once again stated its position in relation to a similar case, albeit with a different outcome, in *MTE v. Hungary.*[40] The case did not involve any substantial differences, as the applicant sought a review of the compatibility with Article 10 ECHR of a ruling against an operator of an information portal due to defamatory comments left anonymously by third parties (i.e., using pseudonyms) in a news article published in a newspaper. As noted above, the ECtHR reached the opposite conclusion, finding that Article 10 had been violated, and thus departing from its precedent in *Delfi*. According to the Court, the two cases may be distinguished due to the nature of the offensive comments and their differing harm; in *Delfi*, in fact, the content posted by third parties was particularly offensive in nature, so much so that the Court argued that it amounted to a form of hate speech that constituted an incitement to acts of violence. This aspect of inciting violence, which the Court suggests makes it more attractive to users, was by contrast absent in *MTE* and it is precisely this absence of manifest unlawfulness that the Court used to justify the difference in the treatment of the Internet service provider.

The ECtHR thus revisited its previous position. Moreover, the case did not involve – as in *Delfi* – a delay in the removal of comments (as this had been done promptly), but rather involved the platform operator's own responsibility for offensive comments published by third parties. In this sense, the Court appears to have attempted to draw closer to EU law as compared to the *Delfi* case and to the principles on the responsibility of Internet service providers.

Moving to Luxembourg, a preliminary question would focus on how the CJEU would have addressed the digital challenges mentioned above. This question allows us to compare the EU standard of protection concerning freedom of expression with the background of the ECHR.

As already clarified, in examining cases involving freedom of expression, the ECtHR decides whether the conducts of domestic authorities comply with the standard of protection established by Article 10 ECHR. In other words, the ECtHR addresses cases as a constitutional court in the context of the Council of Europe. However, it is necessary to stress that such a parameter was

40 *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt v. Hungary,* Application No. 22947/13, Judgment of 2 February 2016.

established when the Convention entered into force in 1950. Therefore, when dealing with applications where the use of new technologies is at issue, the Strasbourg Court grounds its assessment in parameters drafted during the analogical era.

Differently, the CJEU delivers its decisions in the context of preliminary proceedings. In this case, domestic courts play a crucial role in referring questions to the CJEU. Such a difference leads the Luxembourg Court to play de facto a role as fundamental rights adjudicator.[41] Taking as an example the *Delfi* case, the CJEU would have relied on the application of the e-Commerce Directive regime which, at first glance, could fit better the online challenges rather than Article 10 ECHR. Indeed, the CJEU delivers preliminary rulings based on more specific parameters. For instance, the e-Commerce Directive regulates the liability of internet service providers ("ISP s") for illegal content with specific regard to the Internet.

In the *Delfi* case, the CJEU would thus have relied on those rules rather than exclusively reviewing whether Estonian law had complied with the standard of protection established by Article 11 of the Charter of Fundamental Rights of the European Union. Indeed, in this case, the CJEU would most likely have adjudicated on the basis of the liability exemptions. The CJEU would have likely assessed the lack of control over third-party conducts rather than focusing exclusively on the interference with freedom of expression. However, the focus of the CJEU on ISP liability regime does not imply that the EU Court would not have applied the standard of protection established by Article 11 of the Charter.

These preliminary observations highlight how the two European courts have adjudicated the cases involving the protection of free speech in the online environment. Nevertheless, this does not mean that freedom of expression has not been seriously taken into account in the judgments of the CJEU. Indeed, by focusing on CJEU case law, it is possible to evaluate how the right to free speech has been balanced with other fundamental rights that enjoy protection in the EU framework. More specifically, the case law in the field of copyright protection reveals the crucial role of freedom of expression in the CJEU's reasoning. Copyright is enshrined as a fundamental right in the Charter, which expressly protects intellectual property pursuant to Article 17(2). As a result, the recognition of such a right in the Charter means that intellectual property

41 On this point, and with respect to the impact of the Charter of Fundamental Rights of the European Union, see DE BÚRCA, "After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?", Maastricht Journal of European & Competition Law, 2013, p. 168 ff.

is a competing interest which needs to be taken into consideration when balancing it with other rights such as freedom of expression.

Whereas, in the past, free speech was considered an individual fundamental right far from conflicting with property rights (such as copyright), the scenario nowadays has completely changed, so that economic interests are put in the same position as individual interests. The advent of the Internet has fostered a clash between copyright and freedom of expression as represented in the case law of the CJEU. Indeed, in the (similar) cases *Scarlet v. SABAM* and *SABAM v. Netlog*,[42] the main question was whether the domestic judicial authority could impose on ISPs an obligation to adopt a filtering system in order to detect potential copyright infringements.[43] More specifically, in both cases, the Court was required to assess the compatibility of national measures with EU law, namely with: users' freedom of expression; users' right to data protection; ISPs' freedom to carry out economic activity.

It is necessary to emphasize that, although the CJEU expressly took into consideration the right to freedom of expression in its decision-making, it considered the interference with such a fundamental right only residually. Indeed, the CJEU focused its assessment on data protection and freedom to conduct business. The result of such an approach led the CJEU to consider the adoption of the above-mentioned filtering system not proportionate in order to protect the fundamental right of intellectual property. First, the Court observed that the national measure was disproportionate because it hindered the ISP's right to carry out economic activity pursuant to Article 16 of the Charter. Second, as an ancillary consideration, the Court observed that the system also constituted a violation of Articles 8 and 11 of the Charter that expressly referred to the right to data protection and freedom of expression.

Similar considerations can be extended to other cases addressed by the CJEU in the field of copyright protection.[44] These decisions downgraded the role of freedom of expression which enjoys in fact the same status of the freedom of economic activity. The lack of any prominence could be explained by considering the unaccomplished emancipation of the EU from a prevalent economic dimension. As a result, it can be observed that the CJEU's approach to freedom of expression could be considered less accurate than that of the Strasbourg Court since the former has not shown a full emancipation from the

42 Case C-70/10, *Scarlet Extended SA v. SABAM*, 2011; Case C-360/10, *SABAM v. Netlog NV*, 2012.

43 For a comment, see KULK and BORGESIUS, "Filtering for copyright enforcement in Europe after the SABAM cases", European Intellectual Property Review, 2012, p. 54 ff.

44 Case C-314/12, *Telekabel*, 2014; and Case C-484/14, *Mc Fadden*, 2016.

EU economic dimension in order to grant protection to fundamental rights in a similar manner to the latter.

Broadly, this approach is also the result of the lack of any content regulation at the EU level since Member States maintain their discretion in deciding what should or should not circulate. The e-Commerce Directive is the sole common framework adopted by the EU. However, this Directive addresses ISP liability without providing any content regulation. Indeed, the Directive establishes that ISPs which do not perform any editorial control over content cannot be considered responsible for any unlawful conduct performed by third parties.[45]

Therefore, the advent of the Internet has likely led to a low level of protection for freedom of expression. This assumption is also confirmed by the fact that, in the EU context, the existing framework in the field of the Internet is based on the e-Commerce Directive which expressly refers to economic services.

The United States, by contrast, stands out as a bastion of freedom of expression also within the new digital ecosystem.[46] This approach is the result of the broader constitutional protection afforded by the First Amendment of the US Constitution. Indeed, according to Petkova, "the two main theories of interpreting the First Amendment in the US are revolving around the libertarian notion of a 'marketplace of ideas' and the republican one of 'self-government'".[47]

This stance is apparent from the value frame adopted by the Supreme Court, which has been inclined to exalt the unprecedented libertarian dimension of the Internet since its very first judgments in this area. From the outset, in the eyes of the US Supreme Court, the Internet has offered new fora and spaces in which users can exercise the freedom of expression, which must be viewed through different lenses and with reference to different categories from those applied to traditional media. In *Reno v. ACLU*,[48] this difference constituted the basis for the Court's decision to borrow the metaphor of the "free marketplace

45 On the challenges deriving from the role of ISPs in the management of content see in more detail WISCHMEYER, "Making social media an instrument of democracy", European Law Journal, 2019, p. 169 ff., and BASSINI, "Fundamental rights and private enforcement in the digital age", European Law Journal, 2019, p. 182 ff. See also SUSI, "The internet balancing formula", European Law Journal, 2019, p. 192 ff., and ALEXY, "Mart Susi's internet balancing formula', European Law Journal, 2019, p. 213 ff.

46 See BOLLINGER, *The Tolerant Society. Freedom of Speech and Extremist Speech in America*, Oxford, 1986. See also ABRAMS, *The Soul of the First Amendment: Why Freedom of Speech Matters*, New Haven (CT), 2017.

47 PETKOVA, "Privacy as Europe's First Amendment", European Law Journal, 2019, p. 140 ff.

48 *Reno v. ACLU* case, *cit. supra* note 36.

of ideas" from the renowned dissenting opinion of Justice Holmes,[49] the enduring relevance of which could be called into question in the light of the changes to the Internet over the early years of its existence. The Supreme Court embraced the metaphor of the free marketplace of ideas, and in fact exalted it by identifying the Internet as a special domain in which this free exchange could be considerably expanded.

Turning to the reasoning given for the judgment, there is a clear link between the recognition of technological discontinuity and the new developments which the Internet entails, and the internal perspective which – as mentioned above – is characteristic of the point of view of an internal player as opposed to an outsider. The nine justices on the Supreme Court resisted the temptation to extend the case law on radio and television broadcasting to the web, and hence to impose a frame of resistance on the (then) new technology and the resulting continuity with the previous technological framework. With reference to this aspect, the justices stressed the specific reasons why the regulatory regime for radio and television could not be transferred *sic et simpliciter* to the Internet, starting from the specific problem of television as a scarce resource (at that time) that required public regulation, as well as the fact that, with specific reference to the protection of minors, whereas on Internet they would have to take "affirmative steps" (in 1997) to access obscene material, had they been watching television they would by contrast have been passively exposed to such material simply by watching.

Following the Supreme Court's judgment in *Reno v. ACLU*, the US authorities made further attempts to regulate the circulation of content considered to be harmful to minors. However, none of these attempts successfully passed muster before the Supreme Court. 1998 saw the enactment of the Child Online Protection Act, which took account of some of the indications provided in *Reno*. However, according to the Supreme Court, the definition of "material that is harmful to minors", which was based on a generic reference to the standards of the reference community, did not comply with the criteria necessary in order to place legitimate restrictions on freedom of expression.[50]

The outcome was similar in the battle between the US Government and the Supreme Court concerning the prohibition of obscene Internet content that

49 Supreme Court of the United States (USA), *Abrams v. United States*, Judgment of 10 November 1919, 250 U.S. 616 (1919), dissenting opinion of Justice Holmes, available at: <https://supreme.justia.com/cases/federal/us/250/616/>.

50 Supreme Court of the United States (USA), *Ashcroft v. American Civil Liberties Union*, Judgment of 13 May 2002, 535 U.S. 564 (2002), available at: <https://supreme.justia.com/cases/federal/us/535/564/>.

was harmful to minors in the Child Pornography Prevention Act.[51] According to the Supreme Court in this case, the restrictions introduced to prohibit the dissemination of pictures of children depicted engaging in sexual acts or in a manner evocative of sexual acts also proved to be excessive and to lack the required proportionality. In the view of the Court, the scope of the conduct covered by these rules was much broader than that which the legislature could have legitimately regulated in order to achieve the objective of protecting minors.

These rulings are indicative of a clear attitude to safeguard the exercise of free speech through an instrument considered capable of extraordinary expansion in the extent of its use. In other words, the Supreme Court did not make any effort to "downgrade" its sensitivity to this issue specifically by focusing on the possible critical implications of the usage of the Internet, but confirmed, on the contrary, its own liberal vision, even recognizing scope for an expansion in freedom of speech in the light of the characteristics of an entirely new instrument. It is emblematic that the three "strikes" of the Supreme Court have been applied to rules enacted in order to protect a particularly sensitive interest, namely the protection of minors, which is, more than others, capable of legitimizing highly invasive encroachments on freedom of expression.

This is accordingly indicative of a judicial frame that is in general terms opposed to that followed by the European courts which, rather than endorsing the Internet as the driving force for freedom of expression, have perceived and considered above all its critical significance for the exercise of competing rights.

More recently, in *Packingham v. North Carolina*,[52] the Supreme Court addressed another case involving the relationship between the digital dimension and free speech. In this case, the petitioner was convicted based on a Facebook post in which he celebrated the dismissal of a traffic ticket. The US Supreme Court was then required to answer "whether, under this Court's First Amendment precedents, such a law is permissible, both on its face and as applied to the petitioner." The US Supreme Court determined the law in question unconstitutional by adopting an approach of trust in relation to digital technologies, underlining how "[t]he forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what

51 Supreme Court of the United States (USA), *Ashcroft v. Free Speech Coalition*, Judgment of 16 April 2002, 535 U.S. 234 (2002), available at: <https://supreme.justia.com/cases/federal/us/535/234/>.

52 Supreme Court of the United States (USA), *Packingham v. North Carolina*, Judgment of 19 June 2017, 582 U.S. ___ (2017), available at: <https://supreme.justia.com/cases/federal/us/582/15–1194/>.

they say today might be obsolete tomorrow". In other words, the Court should assess such a matter with consideration of the risks of limiting the application of the First Amendment to the Internet.[53]

4 Judicial Protection of Privacy and Data Protection

The increasing judicial momentum that has resulted from the shift from the world of atoms to the world of bits is not specific to the judicial transatlantic narrative surrounding the protection of the freedom of expression. The crucial role played by judicial frames (and, more broadly, judicial imagination), as well as the relevance of the jurisdictional issue, have also emerged within the transatlantic judicial practice of privacy and data protection. In this case, courts across the Atlantic have also played a key role in adapting, or rather interpreting, the protection of rights and freedoms in the transition from atoms to bits. While the right to privacy was initially considered only in its negative dimension, the scenario first changed due to the rise of welfare states and more recently to the rise of the information society.

In the European framework, the ECHR was the first document to introduce a right to private and family life at the European level. However, this document is not directly applicable by the CJEU, even though the principles contained in it have undoubtedly exerted an important influence on its arguments and on the results of its rulings, including in the guise of general principles of EU law. Furthermore, given the lack of clear codification within the constitutions of European countries, it is clear that the right to privacy enjoys a privileged status.[54] Although Article 8 of the ECHR refers exclusively to the right to private and family life, the ECtHR has contributed to the evolution of this parameter. The transition from a static to a dynamic dimension as well as a certain manipulative approach have followed the evolution of new technologies. By interpreting Article 8 of the ECHR (which protects the right to private and family life as an obligation of non-interference by public authorities) in a positive

53 *Ibid.*

54 Taking Italy as an example, Article 117 of the Italian Constitution, as interpreted by the Italian Constitutional Court, requires the legislator to comply with the restrictions deriving from international and EU law, thus making the provisions of the European Convention on Human Rights, as well as those contained in other documents in force at the international level and the European Union, an interposed parameter of constitutional legitimacy. See *Corte Costituzionale*, 22 October 2007, No. 348, and *Corte Costituzionale*, 22 October 2007, No. 349.

way, it was possible for the court to adopt a dynamic standpoint vis-à-vis the emergence of the right to data protection.

The first technological case that stimulated the ECtHR's creativity occurred at the end of the 1980s. In *Klass and Others v. Germany*,[55] the ECtHR acknowledged that telephone conversations fall within the scope of Article 8 of the ECHR. As technology evolved over the next decade and computers became ubiquitous (albeit offline computers), the European Court of Human Rights was encouraged to interpret this provision as inclusive of the collection of personal data. This happened for the first time in 1987, when the ECtHR clarified that the collection and processing of personal data must be included within the scope of Article 8 ECHR.[56]

Among the relevant decisions, in the case of *S and Marper v. UK*,[57] the Grand Chamber of the ECtHR recognized that the protection of personal data is of fundamental importance for an individual in order to fully enjoy the right to respect for private and family life. In this case, the ECtHR made broad references to a set of principles of EU law. Thus, in a case that originated from the retention of fingerprints, tissue samples and DNA profiles of the applicant for an indefinite period of time after a criminal trial, which was concluded with the applicant's acquittal, the ECtHR held that Article 8 of the ECHR had been violated on the grounds that a disproportionate interference had occurred with the right to private and family life that was not necessary in a democratic society. In particular, the ECtHR referred to the need for a balance to be struck between the public interest and individual rights, although also to those principles that allow for the storage of personal data, provided that this storage is relevant and not excessive compared to the purposes for which the data were collected.[58]

Within this framework, the processing of personal data for judicial purposes has been privileged terrain for the ECtHR, which has had the opportunity to rule on violations of Article 8 of the ECHR on several occasions, as it did with regard to an excessive duration of data collection related to an applicant's criminal record in the case of *MM v. UK*.[59]

As previously observed in relation to judicial protection for freedom of expression, the Strasbourg court interpreted the new digital scenario as

55 *Klass and Others v. Germany*, Application No. 5029/71, Judgment of 6 September 1978.

56 *Leander v. Sweden*, Application No. 9248/81, Judgment of 26 March 1987, para. 48.

57 *S and Marper v. The United Kingdom*, Applications No. 30562/04 and No. 30566/04, Judgment of 4 December 2008.

58 *Ibid.*, para 67.

59 *MM v. The United Kingdom*, Application No. 24029/07, Judgment of 29 April 2013.

a source of greater danger, even in consideration of the rights protected by Article 8 ECHR. This interpretation has resulted in the adoption of an approach that reinforces the dimension of confidentiality and the protection of personal data in comparison with other rights, as in the case of *Editorial Board of Pravoye Delo and Shtekel v Ukraine*.[60]

The frame of distrust in new technologies has also led the ECtHR to not only hold States responsible for violating the fundamental rights at stake, but to hold them responsible for failing to implement adequate safeguards to protect the right to privacy. While respecting the margin of appreciation of Contracting States,[61] the reliance on the doctrine of positive obligations that require States to ensure the protection of fundamental rights has increasingly shifted the attention from the relationship between States and individuals (i.e. vertical relations) to the relationship between private actors (i.e. horizontal relations).[62] This step is critical when considering the digital environment since it leads network operators, who are private subjects, to become involved in the protection of privacy and data through the legal measures that States are required to implement in order to safeguard these fundamental rights. This evolution is apparent in *KU v Finland*.[63] In *Copland v UK*,[64] the Strasbourg Court held that Article 8 ECHR had been violated by an employer who monitored telephone calls, emails, and websites visited by an employee.

The role of the ECtHR is just one aspect of the evolution of the right to privacy and data protection in Europe. If the European Convention and the ECtHR case law could be considered as the first steps towards protecting the right to privacy and personal data in Europe, the role of the EU, and especially the CJEU, in the last few years has resulted in the consolidation and adaptation of these fundamental rights within the digital domain. The judicial activism of the CJEU case law has paved the way for the creation of the European personal data fortress.

60 *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* case, *cit. supra* note 35.

61 SPANO, "Universality or Diversity of Human Rights? Strasbourg in the Age of Subsidiarity", Human Rights Law Review, 2014, p. 487 ff.

62 KUMM and FERRERES COMELLA, "What Is So Special about Constitutional Rights in Private Litigation? A Comparative Analysis of the Function of State Action Requirements and Indirect Horizontal Effect", in SAJÓ and UITZ (eds.), *The Constitution in Private Relations: Expanding Constitutionalism*, Den Haag, 2005, p. 241 ff.; KNOX, "Horizontal Human Rights Law", American Journal of International Law, 2008, p. 1 ff.

63 *KU v. Finland* case, *cit. supra* note 38.

64 *Copland v. The United Kingdom*, Application No. 62617/00, Judgment of 3 April 2007.

Among the first cases involving the digital dimension and the application of the Data Protection Directive, it is worth mentioning the *Lindqvist* decision.[65] The case arose out of a Swedish citizen's online publication in which she disclosed the personal data of certain parishioners, along with details of their private and family lives, without having acquired their consent. The individual received a criminal conviction on the grounds that her conduct constituted unlawful data processing. In particular, the CJEU observed that this conduct constituted a processing of personal data with no scope for doubt.[66]

Additionally, in *Promusicae*,[67] a collecting society representing producers and publishers of musical and audiovisual recordings asked their access provider, Telefónica, to disclose the personal data relating to its users due to alleged access to the IP-protected works of the collecting society's clients without the prior authorisation of the rights holders. The question referred to the CJEU sought to determine whether an access provider could be obliged to provide this information to the collecting society. The CJEU held that Member States are not obliged to impose an obligation requiring intermediaries to disclose personal data in order to ensure the effective protection of copyright within the context of civil proceedings. Even more importantly, in this case, the CJEU paved the way for a shift in the paradigm of an autonomous concept of data protection, albeit still inherently linked to the right to privacy.[68]

These were only the first steps. The path towards the constitutionalization of the protection of personal data has been closely linked to the evolution of the EU's own identity in more recent times. As noted above, in the last decade, the European Union has been progressively yet decisively emancipated from the economic vocation that characterized the first fifty years of its life, thanks to the proclamation of the EU Charter of Fundamental Rights in 2000 and its entry into force in 2009. At the same time, the Treaty of Lisbon revolutionized the EU architecture as a precursor to its adherence to the European Convention on Human Rights, thus bringing the EU closer to a "constitutional-like" system.

This was particularly emphasized in a case involving digital privacy. As will be illustrated below in the case *Digital Rights Ireland,*[69] the CJEU invalidated the EU Directive on the retention of data on the grounds that it violated certain provisions of the Charter of Fundamental Rights of the European Union.[70]

65 Case C-101/01, *Bodil Lindqvist*, 2003.

66 *Ibid.* para 27.

67 Case C-275/06, *Productores de Música de España* (*Promusicae*), 2008.

68 *Ibid.* paras. 62–3.

69 Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, 2014.

70 For some comments on the decision, see BOEHM and COLE, "Data retention after the Judgement of the Court of Justice of the European Union", Report commissioned by

In *Google Spain,*[71] the CJEU held that, under certain conditions, Internet search engine service providers are under an obligation, following a complaint by the data subject, to remove links to websites containing information that could harm the applicant's right to be forgotten,[72] where personal data have been available for a significant period of time on the Internet. In *Schrems,*[73] the Court invalidated the Safe Harbour due to the lack of an adequate, or rather equivalent, level of protection of the right to privacy and personal data in the US.

These decisions, and in particular the approach taken by the CJEU in both cases, reveal a judicial frame that is focused on modelling a new right to privacy and data protection that emerges from the legal implications of the Internet. In fact, this dynamic is backed up by a complex process of deterritorialization, denationalization and dematerialization that reflects, *inter alia*, the jurisdictional issue that characterizes the digital revolution.

Moreover, both decisions show the common approach the CJEU has adopted in exploring the impact of technological changes on the level of protection of fundamental rights. The crucial aspect in this respect is not whether limitations are legitimate. Rather, these decisions deal with how new technology affects fundamental rights across jurisdictions. The new right to digital privacy is the result of the CJEU's attempt to adopt a judicial frame that is capable of protecting fundamental rights in the world of bits.

Under these circumstances, it is possible to identify a clash between the US and European perspectives. When looking at privacy and data protection, the approach followed by the US Supreme Court has been quite different. It has been characterized by the so-called "third-party doctrine" by which any person who gives information voluntarily to third parties, including Internet service providers, has no reasonable expectation of privacy. Additionally, it is the Federal Trade Commission ("FTC")[74] – not the US Supreme Court – that is primarily responsible for protecting users' data in the US.

Greens/EFA, European Parliament, 2014, available at: <www.janalbrecht.eu>; FABBRINI, "The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.", Harvard Human Rights Journal, 2014, p. 65 ff.

71 Case C-131/12, *Google Spain*, 2014.

72 For additional commentary, see (among others), LYNSKEY, "Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order", International & Comparative Law Quarterly, 2014, p. 569 ff.; POLLICINO and BASSINI, "Reconciling Right to Be Forgotten and Freedom of Information: Past and Future of Personal Data Protection in Europe", Diritto pubblico comparato ed europeo, 2014, p. 641 ff.

73 Case C-362/14, *Schrems*, 2015.

74 HARTZOG and SOLOVE, "The Scope and Potential of FTC Data Protection," George Washington Law Review, 2015, p. 2230 ff.

This paradigm has only been partially challenged in the last few years. In *United States v. Jones*,[75] the case involved an arrest for drug possession after the police had used a tracker without judicial approval for one month. The primary question was therefore whether the warrantless use of a tracking device to monitor the defendant's movements on public streets violated the Fourth Amendment. The US Supreme Court rejected the Government's argument concerning the lack of a reasonable expectation of privacy and upheld the judgment of the lower court, holding that the use of a GPS tracking device on the defendant's vehicle without a warrant constituted an unlawful search under the Fourth Amendment. More importantly, in this case, Justice Sotomayor stressed the need to reconsider the premise that an individual has no reasonable expectation of privacy in relation to information voluntarily disclosed to third parties. In particular, Justice Sotomayor observed that this approach does not fit with the digital age "in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks".[76]

Even more importantly, this decision has led to the development of the so-called "mosaic theory".[77] The approach adopted in this case results in a focus on governmental activity as collective or aggregate behaviour when reviewing compliance with the Fourth Amendment safeguards. In other words, when small pieces of information are collected, there should not be any problem as a warrant should only be required for bulk surveillance. Any given piece within a mosaic cannot reveal the overall picture without adding the other tiles. It is only the aggregation of the tiles that enables the full picture to be established.

Some years later, it became possible to enshrine this framework in law in one of the most important steps in the field of digital privacy in the US. In *Carpenter v. United States*,[78] after the police arrested four men for a series of armed robberies, the FBI accessed transactional records, including geo-location, from the telephone of one of them. Based on these records, they discovered that the defendant was responsible for aiding and abetting a robbery that affected interstate commerce. The defendant claimed a violation of his Fourth Amendment rights due to the FBI's failure to obtain a warrant. Therefore, the question was

75 Supreme Court of the United States (USA), *United States v. Jones*, Judgment of 23 January 2012, 565 U. S. 400 (2012), available at: <https://supreme.justia.com/cases/federal/us/565/400/>.

76 *Ibid.*, concurring opinion of Justice Sotomayor, p. 417.

77 KERR, "The Mosaic Theory of the Fourth Amendment", Michigan Law Review, 2012, p. 311 ff.

78 Supreme Court of the United States (USA), *Carpenter v. United States*, Judgment of 21 June 2018, 585 U.S. ___ (2018), available at: <https://supreme.justia.com/cases/federal/us/585/16–402/>.

whether a warrantless search and seizure of mobile telephone records violates the Fourth Amendment.

A majority ruled that, in order for the police to access cell site location information or "tower dumps" without infringing Fourth Amendment rights, it is necessary to obtain a search warrant. This is perhaps one of the rare decisions in which the US Supreme Court applied an internal perspective. In particular, the Court underlined that there is a difference in the collection of personal data by wireless carriers, as opposed to that previously reviewed by the Court under the third-party doctrine. Indeed, "there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information".[79] However, the US Supreme Court stressed that it amounted to a "narrow decision", which did not affect other aspects of the third-party doctrine.[80]

It is clear that in the US, privacy and data protection are locked in a judicial frame of full trust in digital technologies. Indeed, aside from the exceptions mentioned above, there are no concerns regarding the new challenges raised by new digital technologies. This also applies to the digital world and, based on the considerable differences in the paradigm for the mutual balancing of fundamental rights" with data collection, it may even result in some of them being considered as fundamental rights.

The US Supreme Court did not subject the use of data and the infringement of privacy to safeguards since the system is still based on a narrow notion of the reasonable expectation of privacy. Such a liberal judicial approach to digital privacy is evident in the field of free speech. This is a general trend, which entails a decision to favour economic freedoms over fundamental rights, or better yet, to focus only on the vertical dimension of fundamental rights in the digital world rather than on the horizontal one.

79 *Ibid.* p. 15.

80 "Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security". *ibid.* p. 17.

5 Judicial Protection of Speech and Data Across Borders

The amplification of judicial momentum in the transition from the world of atoms to the world of bits has affected fundamental rights, as the case law of US and European courts has shown.

Territory and sovereignty still matter in the digital world. The European data protection fortress for its residents is founded on two pillars: European law and the EU "territory". Against this background, the digital territory seems to be the most critical element: the transnational nature of the Internet appears to be irreconcilable with attempts at regionalising data protection online. Therefore, Articles 7 and 8 EUCFR have become trump cards for ensuring greater protection and for extending the "territorial scope" of EU law online.

Within this framework, the cases of *Google v. CNIL*.[81] and *Glawischnig-Piesczek*[82] are paradigms of the CJEU's approach to constitutional values on a global scale at the intersection between speech and privacy.[83] Both decisions show how the CJEU's judicial frame seeking to adapt protection for fundamental rights in line with global challenges where the jurisdictional issue is now a matter of digital sovereignty rather than the attribution of judicial power within a certain territory. Whereas this relationship was more traditionally limited to striking a balance between these rights as conflicting interests, as in *Google Spain*, it is now possible to observe a new interconnection between the two "faces of the same coin". The above-mentioned decisions opened up a new route for this path: a judicial linkage between the regimes governing these two rights in the digital environment.

Within this framework, in *Google v. CNIL*, the CJEU considered a preliminary reference concerning the territorial scope of the right to be forgotten online. The case arose from a formal notice in which the President of the French *Commission Nationale de l'Informatique et des Libertés* ("CNIL") ordered Google to delist information concerning data subjects from all of its domain name extensions. Despite Google's proposal to adopt geo-blocking measures, the CNIL nevertheless decided to sanction Google for a failure to comply with the order. Before the *Conseil d'État*, Google raised a concern regarding the vagueness as to the territorial scope of application of the delisting decision as held by the CJEU in the *Google Spain* case, which led the administrative court

81 Case C-507/17, *Google v. CNIL*, 2019.

82 Case C-18/18, *Glawischnig-Piesczek*, 2019.

83 On the connection between these judgments see DE GREGORIO, "Google v. CNIL and Glawischnig-Piesczek v. Facebook: content and data in the algorithmic society", Rivista di diritto dei media, 2020, p. 249 ff.

to send a preliminary reference to the CJEU concerning the scope of search engine delisting obligations.

Starting from Advocate General Szpunar's opinion in *Google v. CNIL*, it is possible to observe an approach characterized by self-restraint. According to Szpunar, neither EU law nor the CJEU case law engaged with the territoriality of de-referencing within the context of protection of rights outlined in Articles 7 and 8 EUCFR.[84] In other words, neither EU lawmakers nor the EU courts provided any answers for dealing with the results of searches made outside of the EU physical borders.

From this point of view, Advocate General Szpunar argued that there should be no potential expansion of the territorial scope of fundamental rights beyond the EU borders. Indeed, he both rejected the argument that the EU Charter of Fundamental Rights has extraterritorial effects and asserted that the right to be forgotten did not have the status of a super-right (that is, a right exempt from the balancing process), signifying an approach of self-restraint in relation to the jurisdictional issue. This point concerns not only the "invasion" of third countries' sovereignty in striking their own balances between fundamental rights, but also the increasing risk of triggering a counter-response.[85]

This is why Advocate General Szpunar's proposal was more focused on geo-blocking technologies applied within the EU. Having once again asserted that EU law applies to the activities of search engines, and having noting that the CNIL had rejected Google's proposed geo-blocking formulation, the CJEU analysed the questions proposed for a preliminary ruling: whether according to Articles 12(b) and 14 of the Data Protection Directive and Article 17(1) of the GDPR, de-referencing is due either on all the versions of the search engine, or only on the versions of that search engine corresponding to all the Member States, or even only on the version corresponding to the Member State where the de-referencing was requested. The global nature of the Internet and the claims of the right to digital privacy and data protection seemed to open the door on a new phase in the extraterritoriality saga.[86]

However, in contrast to what happened in the *Google Spain* case, by embracing Advocate General Szpunar's views, the CJEU highlighted a different approach to the right to privacy and data protection in other legal systems as well as the relative nature of this fundamental right. Two of the pillars underlying the extraterritoriality effect seemed to have fallen; on the one hand, the court recognized the limited digital sovereignty of the EU or rather recognized

84 *Google v. CNIL* case, *cit. supra* note 81, Opinion of AG Szpunar, para. 45.

85 *Ibid.*, para 61.

86 *Google v. CNIL* case, *cit. supra* note 81, para 58.

the presence of different sovereignties within the digital world. On the other hand, the trump card of the absolute right to data protection and privacy online appears, in part, to have become less powerful. As a result, even if, in light of the precedents, the coherent solution would have been to extend the right to be forgotten to a global scale, the CJEU, motivated by the risk of a kind of European legal colonisation in the name of cultural hegemony, opted for an approach of self-restraint.

However, this decision seems to be more a tactical retreat than a surrender to criticism against the Europeanization of Internet regulation. It appears that the judiciary primarily exhibited self-restraint, pending further decision-making by politicians. Aside from these considerations, the obligation to delist seems to be restricted to the EU Member States,[87] while national authorities may be free to require global removal.

In this sense, it is notable that the CJEU is also engaging in dialogue with Member States' courts, as indicated by the German Constitutional Court's last two decisions on the right to be forgotten.[88] The two decisions concern partially and fully-harmonized areas of EU law. In the first case, the right to privacy had to be balanced against freedom of the press,[89] and in this field, the *Bundesverfassungsgericht* reasserted its right to apply national fundamental rights. In the second case however,[90] the German Constitutional Court claimed that it could have the power to review a hypothetical infringement of EU fundamental rights.[91] The most significant aspects of these decisions are, first of all, the attention given to the technological dimensions of the case and, secondly, the German Constitutional Court's more careful balancing between

87 "The EU legislature has now chosen to lay down the rules concerning data protection by way of a regulation, which is directly applicable in all the Member States, which has been done, as is emphasized by recital 10 of Regulation 2016/679, in order to ensure a consistent and high level of protection throughout the European Union and to remove the obstacles to flows of personal data within the Union, that the de-referencing in question is, in principle, supposed to be carried out in respect of all the Member States". *Ibid*. para. 66.

88 *Bundesverfassungsgericht*, Judgment of 6 November 2019, 1 BvR 16/13, available at: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr001613en.html>, and *Bundesverfassungsgericht*, Judgment of 6 November 2019, 1 BvR 276/17, available at: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr027617en.html>. See also HERZOG, "Dialogue and Diversity. The "Right to be forgotten" – decisions of the Federal Constitutional Court", Rivista di diritto dei media, 2020, p. 285 ff.

89 BvR 16/13 case, *cit. supra* note 88, para. 45.

90 BvR 276/17 case, *cit. supra* note 88, para. 50.

91 See, on this point, Burchardt, "Backlash against the Court of Justice of the EU? The Recent Jurisprudence of the German Constitutional Court on EU Fundamental Rights as a Standard of Review", German Law Journal, 2020, p. 1 ff.

the right to be forgotten and freedom of speech.[92] The German Constitutional Court stressed that conflicting fundamental rights must be weighed up equally, and there is no presumption that the right to personality must prevail in all cases.[93]

From the first point of view, the technological dimension played an important role in the German Constitutional Court's considerations, showing how courts are being continuously called upon to update their reasoning in line with technological evolution.[94] From the second point of view, the first case showed careful consideration for freedom of the press,[95] whilst the second did not appear to consider search engines' freedom of expression, but rather limited the analysis to their economic interests by holding that a search engine operator cannot invoke freedom of the press and freedom of opinion and media prerogatives in general.[96] However, the important point in this case is that the nature of the right to digital privacy was considered less absolute.[97]

A similar approach can be discerned in relation to freedom of expression. Specifically, in *Glawischnig-Piesczek*, the CJEU addressed the territorial scope

92 BvR 276/17 case, *cit. supra* note 88, para. 120.

93 *Ibid.*, para. 121.

94 "The conflicting fundamental rights must be balanced against one another. Such a balancing requires a determination of their respective guaranteed contents. In this regard, particular consideration must be given to the realities of Internet communication.". BvR 16/13 case, *cit. supra* note 90, para. 96. But above all the Bundesverfassungsgericht claimed "Given that technical developments are ongoing and that they entail uncertainties regarding how and to what extent content providers can influence the dissemination of their articles on the Internet in interaction with search engines, it will fall to the ordinary courts to continue to shape effective and reasonable protective measures. Where reasonable, the courts, which have a considerable margin of appreciation in respect of all these measures, can also require the actors to develop new instruments.". *Ibid.*, para. 142.

95 "Online archives do not merely serve the interests of media outlets, but are also in the public interest.". *Ibid.*, para. 113.

96 The *Bundesverfassungsgericht* has stressed that search engines cannot be considered as the press. BvR 276/17 case, *cit. supra* note 88, para. 9. Additionally, search engines are not guaranteed an independent and autonomous right to freedom of expression. *Ibid.*, para. 105.

97 Even recognising that "insofar as the Charter of Fundamental Rights of the European Union is applicable, the wording chosen by the European Court of Justice in the Google Spain decision that the rights of the data subject (as protected by artt. 7 and 8) generally outweigh the interest of Internet users, is not generalizable beyond the case decided at the time. Such a predisposition to data protection instead of an open balance of fundamental rights would be in clear contrast with the case law of the Federal Constitutional Court, but also of the European Court of Human Rights and the European Court of Justice itself. The facts decided by the Higher Regional Court and the facts underlying the decision Google Spain of the European Court of Justice showed factual differences. It should also be considered to what extent media freedoms should be taken into account in such cases." (translation by the author). *Ibid.*, para. 21.

of national orders concerning the removal of content, thus configuring the impact of EU law, especially the freedom of expression, on a global scale. In contrast to the previous case, this case did not concern a non-harmonized framework of EU law,[98] as Advocate General Szpunar stressed in the previous case.[99]

Freedom of expression is not regulated by a harmonized set of provisions at a supranational level, such as those contained in the GDPR. Nonetheless, even though the matter is not fully harmonized and Member States grant different degrees of protection to freedom of expression, it is worth emphasising how the EU has intervened in the area of freedom of expression.[100] The willingness of the EU institutions to create a *droit acquis communautaire* in relation to the freedom of expression may be due to various factors such as furthering the political integration of the EU or responding to populist challenges. The EU's actions in the area of freedom of expression have also recently included measures such as the amendments to the Audiovisual Media Service Directive or the Copyright Directive.[101] Additionally, it is worth mentioning here also the Code of Conduct on Countering Illegal Hate Speech Online,[102] which seeks to combat hate speech online, as well as the Code of Practice on Disinformation,[103] which enshrined the first attempt to regulate online platforms with reference to disinformation and misinformation[104].

98 *Glawischnig-Piesczek* case, *cit. supra* note 82, Opinion of AG Szpunar, para. 79.

99 *Ibid.*

100 See for instance, Directive (EU) 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography; Directive (EU) 2017/541 on combating terrorism; Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online C/2018/1177; Proposal for a Regulation of The European Parliament and of the Council on preventing the dissemination of terrorist content online, COM/2018/640 final.

101 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities; Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

102 Code of Conduct on Countering Illegal Hate Speech Online (2016), available at: <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en>.

103 Code of Practice on Disinformation (2018), available at: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

104 Even if – as some authors argue – this soft legal instrument can be ascribed to a logic that delegates the balancing process of fundamental rights to private powers, which entails some risks of the privatisation of the censorship. See MONTI, "The EU Code of Practice

As in the case relating to digital privacy, fundamental rights are balanced quite differently in Europe and in the US.[105] Whereas in the US legal system the doctrine of the free marketplace of ideas considers State intervention within public discourse to be inconsistent with the First Amendment, Europe has embraced a different balancing process for establishing the limits of free speech. Under Article 10 of the ECHR and Article 11 of the EUCFR, not all forms of speech enjoy the same standard of protection, and this is particularly evident in the fields of hate speech and fake news. Consequently, another clash of digital sovereignties could potentially break out online. In this regard, it must be stressed that judicial protection for freedom of expression in Europe has not been particularly broad. On the other hand, the rise of new technologies has led European courts to narrow down the protection of freedom of expression in order to protect other conflicting interests online.

In this context, the decision in *Glawischnig-Piesczek* considered the compatibility with the e-Commerce Directive (most notably with the absence of a general obligation to monitor) of the removal of defamatory content from Facebook. In this case, a former Member of the Austrian Parliament complained that her honour had been impugned following the publication of defamatory content, which was accessible to all Facebook users. Nonetheless, the social network refused to remove the comments. In view of the conflicting views adopted by the domestic courts, the Austrian Supreme Court of Justice decided to refer some questions to the CJEU, asking whether Facebook should be required to remove expressions that are identical and equivalent to hosted content as ordered by the national courts, as well as the territorial reach of such an order.

The challenges raised by this new decision are already apparent from the CJEU's choice not to limit removal to identical content but also to equivalent content, thus broadening content-based control over the information disseminated. This seems to be the first problematic aspect of the decision. To allow the removal of more content that is considered to be equivalent in nature to banned content could increase the likelihood of a different balance of rights being struck in a third country with regard to expressions not covered by free speech clauses. For instance, the clash between the balancing processes is

on Disinformation and the Risk of the Privatisation of Censorship", in GIUSTI and PIRAS (eds.), *Democracy and Fake News – Information Manipulation and Post-Truth Politics*, Abingdon, 2021, p. 214 ff.

105 See SCHAUER, "Freedom of Expression Adjudication in Europe and America: A Case Study in Comparative Constitutional Architecture", in NOLTE (ed.), *European and US Constitutionalism*, Cambridge, p. 49 ff.

evident in weighing the balance struck by the US Supreme Court in the defamatory cases with the Austrian court's position.[106]

Furthermore, as in *CNIL v. Google*, Advocate General Szpunar proposed geographical limits to the application of national law in the digital world. Once again, the problem concerned other States' digital sovereignty. Indeed, as the Advocate General observed, the imposition in one Member State of an obligation consisting in removing certain information worldwide, for all users of an electronic platform, because of the illegality of that information established under an applicable law, would have the consequence that the finding of its illegality would have effects in other States.[107] This is particularly relevant in relation to the principle of international comity. As underlined by Advocate General Szpunar, a "court should, as far as possible, limit the extraterritorial effects of its junctions concerning harm to private life and personality rights. The implementation of a removal obligation should not go beyond what is necessary to achieve the protection of the injured person".[108] On this point the CJEU recognized that no EU provisions impose a territorial limitation in this area.[109]

As in *CNIL v. Google*, the CJEU decision could be read as a green light for national courts to impose a global reach to their decisions on the removal of online content.[110] Indeed, in *Glawischnig-Piesczek v. Facebook*, the CJEU did not deny the possibility that EU Member States' laws might have extraterritorial effects. Its approach sought to leave the issue of the extraterritorial scope of EU law open. Besides, the Belgian Constitutional Court's recent request for a preliminary ruling – including ten preliminary questions on the obligation to transfer passenger information – could allow the CJEU to clarify the issue of the third country's digital sovereignty.[111]

In light of the European approach to fundamental rights on a global scale resulting from these decisions, and in light of the growing convergence of the

106 About the *probatio diabolica* of the 'actual malice' in the US legal system, see HO YOUM, "'Actual Malice' in U.S. Defamation Law: The Minority of One Doctrine in the World?", Journal of International & Entertainment Law, 2011, p. 1 ff.

107 *Google v. CNIL* case, *cit. supra* note 81, Opinion of AG Szpunar, para. 80.

108 *Ibid.*, para. 100.

109 *Glawischnig-Piesczek* case, *cit. supra* note 82, para. 51.

110 As stressed by Thomas Hughes, Executive Director of Article 19, in "CJEU judgment in Facebook Ireland case is threat to online free speech", Article 19, 3 October 2019, available at: <https://www.article19.org/resources/cjeu-judgment-in-facebook-ireland-case-is-threat-to-online-free-speech/>.

111 Constitutional Court (Belgium), *Ligue des Droits de l'Homme*, Judgment of 10 October 2019, No. 135, available at: <https://www.const-court.be/public/f/2019/2019-135f.pdf>.

principles regulating freedom of expression and data protection online,[112] it is possible to discern a broader trend: the Europeanization of Internet regulation as an expression of digital sovereignty through judicial power. In addition, it has to be stressed that a "sword of Damocles" is hanging over the CJEU's apparently self-restrained approach. By not excluding the possibility that the territorial reach of EU fundamental rights may be global, the CJEU leaves room for politicians to make decisions on the territorial scope of EU law.

The European Union's path towards digital privacy is peculiar but it is not the only approach to digital sovereignty in the information society. When moving to other side of the Atlantic, it is worth observing the lack of a tendency towards judicial activism but towards stagnation.

6 Conclusions

The amplification of judicial power is also the result of procedural and substantial issues in the digital age, which are related to the obvious yet somehow trivialized notion that legal reforms tend to lag behind technological advances. The newness of technologies has encouraged courts to respond to new challenges in order to ensure protection of fundamental rights in the context of new technology.

The rise of the Internet has led courts to face new challenges, which have affected the judicial protection of the freedom of expression, privacy, and data protection. However, this is more evident in Europe where judicial interpretation of the relevant provisions has shifted towards judicial manipulation. The European Court of Human Rights and the US Supreme Court have been able to update judicial protection for free speech and privacy in line with technological developments, whilst relying on provisions written decades (in the former case) or centuries (in the latter case) ago. With specific reference to the US framework, the US Supreme Court has adopted a different approach to the protection of free speech and privacy. Nonetheless, this does not mean that Internet technologies have not affected judicial protection for fundamental rights. On the contrary, the Internet has highlighted different judicial frames and approaches to the territorial boundaries that underscore constitutional differences across the Atlantic.

112 DE GREGORIO, "The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?", Robert Schuman Centre for Advanced Studies, Research Paper No. RSCAS 2019/36, 2019.

There is no doubt that courts today are the best-equipped institutions to identify the risk of a constitutional collision. However, this does not mean that judges should act in isolation. The fact that they are the best-placed institutions does not mean that they are the only institutions to identify these risks. Moreover, the comparative analysis carried out above has made it clear how the specific individual judicial frame can have a crucial impact on a court's final decision, not only between different courts but also within the same court at different times and comprised of different judges. The rise of the Internet has resulted in an increasing protection of the right to free speech in the US, while leading to the consolidation and emancipation of the right to data protection in the EU. At the same time, the extended protection over these fundamental rights has led to a rolling back of protection of other constitutional interests. Additionally, this approach clearly entails a fragmentation of existing protections, and the unpredictable nature of the relevant case law, thus causing clear harm for the principle of legitimate expectations and legal certainty. However, those are not the only reasons why (especially European) courts' activism is needed in order to compensate the legislator's inertia and lack of political will.

The analysis of judicial frames across the Atlantic has shown how courts have adapted constitutional values to new technologies. As far as digital technologies are concerned, courts have proven to be the primary actors in bridging the gap between law and technology. This does not mean that the role of courts will be rebalanced by the emergence of political power in the technological domain. On the contrary, it is likely that the courts will continue to adapt protection for fundamental rights in the information society in line with new technology. Whilst there is no doubt that technology clearly develops much more quickly than the law, it is important to point out that judicial activism is not exclusively the result of the legislator's inability to keep pace with technological evolution. Indeed, sometimes legislative inertia is simply a political choice. More specifically, courts have often been given the responsibility for balancing contrasting fundamental rights in the digital era.