The Legal Side of Digital Technologies: Challenges and New Paradigms

Marco Bassini and Oreste Pollicino

Abstract

The chapter aims to provide an overview of the relationship between law and the rise of digital technologies. It focuses on two of the most challenging issues that have come up in cyberspace, namely, the role of online platforms in the context of content moderation and the protection of personal data. It highlights the role played by courts in safeguarding the rule of law principle also in the digital sphere, in light of the emergence of new "private powers" that more and more are capable of influencing the degree of protection of human rights (such as freedom of expression and the right to privacy).

1 Enforcing the Rule of Law in the Algorithmic Society

New technologies have always challenged, if not disrupted, the social, economic, legal, and to an extent, the ideological *status quo*. The development of data collection, mining, and algorithmic analysis, resulting in predictive profiling, is playing a disruptive role. Society is increasingly digitized, and the way in which values are perceived and interpreted is inevitably shaped by the consolidation of the information society. The pandemic season has not only broadened the technological challenges, as in the case of contact tracing, but it has also shown the role of private actors in acting as essential infrastructures or digital utilities. Facebook, Amazon, and Zoom are just three examples of actors that have allowed people to study, work, and maintain social relationships.

M. Bassini (✉) · O. Pollicino
Bocconi University – Department of Legal Studies, Milan, Italy
e-mail: marco.bassini@unibocconi.it; oreste.pollicino@unibocconi.it

G. Castelli et al. (eds.), *The Post-Digital Enterprise*, Future of Business and Finance,
https://doi.org/10.1007/978-3-030-94837-5_8

The rule of law has not been spared in this process of framing (but not transforming) traditional categories in light of technological dynamics.[1] The newness of (algorithmic) technology is a natural challenge for the principles of the rule of law.[2] However, technology also represents an opportunity to foster this principle, since it can provide better systems of enforcement for public policies, as well as a clear and reliable framework to compensate for inefficiencies *de facto* undermining legal certainty.[3]

Within this framework between innovation and risk, the key question to be addressed by regulators is whether algorithmic technologies can encourage the exercise of arbitrary powers.[4] The principle of the rule of law is a precondition for ensuring equal treatment before the law, protecting human rights, preventing abuse of power by public authorities, and holding decision-making bodies to account.[5] The rule of law is primarily considered as the opposite of arbitrary public power. Therefore, it is a constitutional bastion limiting the exercise of authorities outside any constitutional limit and ensuring that these limits answer to a common constitutional scheme. In the information society, this principle is a primary safeguard to ensure that when public actors implement digital technologies to increase their efficiency, provide better services, or improve the performance of public tasks, the exercise of these activities is not discretionary but based on clear and proportionate provisions. At the same time, the lack of expertise of public authorities and the rise of gatekeepers online have led the public sector to increasingly rely on private actors to ensure the enforcement of public policies online.[6]

Nonetheless, in the lack of regulation or horizontal translation of constitutional values, the principle of the rule of law does not limit the freedom that private entities enjoy in performing their activities, including their right to free speech or freedom to conduct business. In a global digital environment, the threats to the principle of the rule of law do not just come from the implementation of algorithmic technologies by public actors, but also, and primarily, from the ability of transnational private actors to develop and enforce private standards that compete with public values. This is evident when focusing on how information flows online and the characteristics of the public sphere, which is increasingly personalized rather than plural.[7] Likewise, the

[1] See Oreste Pollicino and Giovanni De Gregorio, "Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics," *MediaLaws.eu,* 11 November 2021.

[2] Monroe E. Price, "The Newness of Technology" (2001) 22 *Cardozo Law Review* 1885.

[3] Steven Malby, "Strengthening The Rule of Law through Technology" (2017) 43 *Commonwealth Law Bulletin* 307.

[4] Mireille Hildebrandt, "The Artificial Intelligence of European Union Law" (2020) 21 *German Law Journal* 74.

[5] Jeremy Waldron, "The Concept and the Rule of Law" (2008) 43(1) *Georgia Law Review* 1.

[6] Michael D. Birnhack and Niva Elkin-Koren, "The Invisible Handshake: The Reemergence of the State in the Digital Environment" (2003) 8 *Virginia Journal of Law & Technology* 1.

[7] Giovanni De Gregorio, "Democratising Content Moderation: A Constitutional Framework" (2020) 36 *Computer Law & Security Law Review* 105374.

field of data is even more compelling, due to the ability of private actors to affect users' rights to privacy and data protection by implementing technologies whose transparency and accountability cannot be ensured.[8]

The technological factor makes an already troubled situation increasingly serious, in which the rule of law seems to be under siege. Within this framework, it is worth wondering what the role of law in the algorithmic society is. How do particular states deal with the emerging private powers that bring new threats to the principle of the rule of law? How should states address the challenges generated by the spread on a larger and larger scale of digital technologies that increasingly play an essential role in a variety of human activities and process large amount of personal data?

Before exploring the most recent stances taken by the European Union regulators, it is worth noting that such a scenario, whereby private powers have arisen and created unprecedented challenges for the protection of a plurality of human rights, finds it roots in the initial desire to maintain their immunity to strict regulation in different respects. The absence of particular constraints that could, in a way, place some restrictions on digital platforms' freedom to conduct business was intended to avoid measures that could undermine the flourishing of services deemed to be of key importance. But if such an approach made sense at the time of the origins of the Internet (when the apparently free-of-charge nature of these services made it possible for the most important platforms to collect large amounts of data), whether the lack of more in-depth regulation is still beneficial overall can now be questioned.

This chapter will try to answer these questions, addressing the two most important pillars when it comes to exploring the relationship between technology and regulation, namely, content and data. Both perspectives provide interesting insights into the current challenges to be dealt with in the algorithmic society and into the role of regulation in preserving protection of fundamental rights against this background.

In the specific domain of the protection of personal data, the digital revolution made it necessary, at the level of the European Union, to shift from a more flexible and open-ended legal framework (namely, Directive 95/46/EC), drafted in the age that preceded the rise of the Internet and its spread on a massive scale, to a more detailed and stricter piece of regulation, which came into force in 2016 (the General Data Protection Regulation). This dynamic clarified the influence of the emerging technologies on the effectiveness of the existing legal measures and brought to light the need to revisit some of the pillars of the legal framework in order to not deprive individuals from the essence of their fundamental rights.

The key question is then, in view of the new challenges surrounding the role of digital platforms, can a similar process take place before it is too late?

[8] Serge Gutwirth and Paul De Hert, "Regulating Profiling in a Democratic Constitutional States," in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* 271 (2006).

2 Reforming the Legal Regime Applicable to Internet Service Providers: When Content Regulation Passes Through Services Regulation

The dispute that recently arose between the social network Twitter and the now former president of the United States Donald Trump has brought to light a long-debated topic of recent years, regarding which the institutions of the European Union, through the Digital Services Act package, have recently advanced an important proposal for reforming a legal regime that was drafted in 2000,[9] when many of the current digital platforms did not even exist.[10]

Concerning the status of Internet service providers, in fact, this is a legal issue that has often been at the heart of the attention of commentators and has given rise to several courts' decisions (both at national level and at the supranational level, in the EU legal system and in the Council of Europe),[11] without leading lawmakers to ultimately change the rules of the game.

The hesitation shown so far by the European Union institutions, which for some time have been quite reluctant to consider the option of shaping a new legal framework, should not, however, come as a surprise, especially if one bears in mind the legal, economic, and cultural conditions behind the adoption, both in the United States and in Europe, of the first rules on this subject.

It is not even a coincidence, perhaps, that before the aforementioned proposal for a regulation under the Digital Services Act came into play in Europe, even in the United States, attempts were made to shed some new light on the subject, albeit in the context of a strongly personal opposition between Donald Trump and some social networks, Twitter above all, in the context of the 2020 US general election.

In the United States, Internet service providers have benefited from a very favorable regime, based on the provision of Section 230 of the Communications Decency Act (CDA),[12] the first act regulating the Internet passed by Congress in 1996 with a view to prevent cyberspace from becoming a free zone where conduct prohibited in the real world could nevertheless occur.

[9] Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Brussels, 15.12.2020, COM(2020) 825 final, 2020/0361(COD).

[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").

[11] For an overview, see Marco Bassini, "Mambo Italiano: the perilous Italian way to ISP liability," in Bilyana Petkova and Tuomas Ojanen, *Fundamental Rights Protection Online. The Future Regulation of Intermediaries* (Cheltenham-Northampton 2020), 84. For an in-depth focus on the implications on freedom of expression of the role of Internet service providers, see Ernesto Apa and Oreste Pollicino, *Modeling the Liability of Internet Service Provider. Google vs. Vivi Down: A Constitutional Perspective* (Milan 2014).

[12] 47 U.S.C. § 230.

According to the Good Samaritan clause enshrined in Section 230 CDA, Internet service providers enjoy a broad immunity in relation to any content moderation activities carried out "in good faith." This provision was of the utmost importance for the rise and expansion of the Internet as we know it today,[13] allowing service providers to escape from possible negative consequences (i.e., incurring liability) related to any act of content moderation, except for a limited set of derogations. Congress passed this provision with the primary goal of avoiding courts being able to analogize service providers to publishers and thus make them subject to the same legal regime based on direct liability. Indeed, an American court had already made this point in 1991, in the *CompuServe* case,[14] in which the court found that Internet service providers are comparable to book stores, public libraries, and newsstands, and as such merely act as distributors of third-party content. Nonetheless, in 1995 the Supreme Court of the State of New York delivered an opposite decision in *Prodigy*,[15] subjecting a service provider to the standard of liability applicable to publishers. In the latter judgment, the judges argued that the presence of a team of moderators and some guidelines intended for users of the platform made it possible to qualify the operator as a publisher and not a mere distributor of third-party content. The intervention of Congress in 1996 aimed to clarify this possible misunderstanding, avoiding any content moderation activity conducted in good faith being qualification as an index of editorial responsibility.[16] Of course, this provision dates back to an era when the Internet was not yet populated, as it is today, by the so-called web giants, and when therefore the absence of concentrations of power in the hands of a few subjects led to the presumption that it could fulfill the ambition of a free market of ideas, that is, the digital declination of that "marketplace" theorized by Justice Holmes in 1919 in his famous dissenting opinion in the *Abrams v. United States* judgment.[17] It is no coincidence that this provision has been at the center of numerous debates among American commentators, some of which have emphasized that the attitude of greater openness cultivated by the legislator at the beginning of the digital age has ended up placing a very important market power in the hands of a few operators. Nor is it a coincidence that for some types of infringements, the exemption from liability based on Section 230 CDA has been mitigated through the provision of notice and take down mechanisms, as in the case of copyright infringement, which falls under the provisions of the Digital Millennium Copyright Act.[18]

[13] A recent volume by Jeff Kosseff not surprisingly renamed this provision as "The Twenty-Six Words That Created the Internet" (see Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Ithaca-London 2019).

[14] *Cubby, Inc. v. CompuServe Inc*., 776 F. Supp. 135 (S.D.N.Y. 1991).

[15] *Stratton Oakmont, Inc. v. Prodigy Services Co*., 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

[16] "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

[17] *Abrams v. United States,* 250 U.S. 616 (1919).

[18] 17 U.S.C. §§ 512.

These rules seemed, at the time, most suitable to give substance to the spirit of American constitutionalism with respect to the First Amendment, portrayed in its digital declination by the landmark *Reno* case delivered by the Supreme Court in 1997.[19]

In Europe, where the protection of freedom of expression is subject to a more balanced standard, it is not by coincidence that regulators took inspiration from the second model, based on the notice and take down mechanism, introducing it in the E-Commerce Directive in 2000. While this act has somehow prevented Europe from being an "easy land of conquest" for the American tech giants raised in Silicon Valley, it has nevertheless proved inadequate to capture the more and more complex nature of these services and of the relevant business models.

This brief overview of the origins of Internet service providers' liability should suffice to explain which reasons prompted the European Union institutions, also by virtue of all-but-enthusiastic results of the various self-regulation and co-regulation mechanisms undertaken so far, to plan a new regulatory intervention for this matter. A guiding factor of the new package of reforms is the awareness of the obsolescence of the rules on the liability of service providers, which no longer mirror the complexity and sophistication in the role of Internet service providers.

Recent events show the sensitive nature of content moderation and thus provide further justifications for the ongoing debate on possible reforms of the rules enshrined in the E-Commerce Directive. More and more, as noted above, digital platforms act as private powers, therefore competing, in a way, with public authorities in which governmental functions are traditionally and exclusively vested. The recent "battle" between Donald Trump and Twitter sheds light on the importance of the role of social networks at the intersection between power and democracy.[20] On one hand, social networks still qualify as private platforms run by operators that pursue their business, seeking maximization of the revenues they collect. One may thus shape the relationship between these service providers and the relevant users as a purely private one governed by the contractual terms and conditions both parties agree to abide by. On the other hand, however, the same relationship could be framed according to a different understanding, to the extent social networks constitute the main (and sometimes the only) avenue for individuals to express ideas and opinions, so that the deprivation of their use (for instance, because of the suspension or block of users' account) may be deemed to interfere with individuals' freedom of expression.[21] This problem has come into play most notably with respect to the role of content moderation, which may lead to the removal from digital platforms of pieces of content that do not necessarily amount

[19] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

[20] See most notably *Knight First Amendment Inst. at Columbia Univ. v. Trump,* 928 F.3d 226 (2d Cir. 2019), now *Joseph R. Biden, Jr. President of the United States, et al., v Knight First Amendment Institute at Columbia University, et al.*, 593 U. S. ____ (2021).

[21] On these profiles see Giovanni De Gregorio, *Expressions on Platforms: Freedom of Expression and ISP Liability in the European Digital Single Market,* (2018) 3(2) *European Competition and Regulatory Law Review* 203.

to illegal conduct. If such removal can be justified on the basis of the terms and conditions entered into by the parties, a different conclusion may be reached assuming that digital platforms operate as public fora and constitute quasi-public services. In the latter scenario, in fact, service providers would be subject to the same obligations applicable to state actors (i.e., public authorities) for protecting freedom of expression. Content moderation, thus, would not be possible for pieces of content that public authorities have no right to censor or prohibit. Especially when cases like that of the opposition between Trump and Twitter arise, the removal of a post, the deletion of a comment, or the blocking of an account, even if legitimized on the basis of the terms and conditions of use of the service, probably no longer represent only choices made in the context of one's private autonomy from a private subject but become determinations with significant legal implications because of their effects on the digital public sphere.

In strictly legal terms, the key question concerns the possible equalization between the Internet (and social networks) and what in American jurisprudence is usually defined as a public forum, a "place" naturally designated for the exchange of ideas and opinions between individuals and therefore subject to only very limited restrictions. Admitting this equation would lead to a very significant reduction of the room for "private" content moderation, thus aligning the statute of freedom of expression on digital platforms with that in force outside this ecosystem. This option would pave the way for the application of freedom of expression with horizontal effects, as users could therefore enforce their right to free speech vis-à-vis the relevant service providers.

These legal issues already arose in the case law of the US Supreme Court, which precisely on the generalized prohibition, provided for by a North Carolina law, of accessing social networks for persons who had reported convictions for particular crimes, found a violation of the First Amendment in the 2017 landmark *Packingham* case.[22]

Other American courts have also had the opportunity to take the floor on this issue, but limited to cases that had to do with the use of social networks by institutional figures (including Trump) and which were therefore characterized by qualification of the account as a public forum used by a state actor. In another case in which no public figure was at stake (*PragerU v. YouTube*),[23] the Ninth Circuit Court of Appeals stated that an operator such as YouTube does not perform functions traditionally attributable to public actors, thus excluding a possible equalization.

Taken from this angle, the reform that the institutions of the European Union aim to implement in the field of digital services (but also markets) reveals the complexity of the various profiles behind it.

It is no coincidence, as already mentioned, that even in the United States, with a much-discussed Executive Order,[24] Donald Trump had tried to shift away the role of

[22] *Packingham v. North Carolina*, 582 U.S. ___.

[23] No. 18-15712. D.C. No. 5:17-cv-06064.

[24] Executive Order 13925 of May 28, 2020. Preventing Online Censorship.

intermediaries from that enshrined in the legal paradigm of Section 230 CDA. It is also no coincidence that before this attempt, the institutions of the European Union had tried to work "alongside" this legal framework, proceeding with a sectoral approach: First with the reform of the discipline on audiovisual media services (the so-called SMAV Directive 2010/13/EU),[25] and then with the more recent and much debated Copyright Directive (Directive (EU) 790/2019).[26] What both moves had in common was the attempt to shape a specific categorization of the platforms, going beyond the legal paradigm enshrined in the E-Commerce Directive and carving out special rules related to the peculiarity of the sector. The time to evaluate the profitability of this approach is not yet ripe, but perhaps it will be later, with the debate on the Digital Services Act in full swing.

3 Personal Data Protection: A New Paradigm for Regulating Digital Technologies

The reform that has taken place in the field of personal data protection, which resulted in the entry into force of the GDPR, shows a very close link that binds the revision of the EU legislation on personal data and the reform of the Digital Single Market.

In this regard, it should be recalled that the second pillar of this strategy, launched in 2015, corresponds to the creation of a favorable context for the development of digital networks and services. This objective could not be achieved in the absence of an adequate regulatory framework addressing the criticalities that the digital economy brings forward for personal data.

The European Union has been dealing with the protection of personal data since 1995, the year in which Directive 95/46/EC, the first act intended to harmonize the laws of Member States on the subject, entered into force. But this degree of harmonization, in the light of the peculiarities of digital technologies that are now implemented on a large scale, was no longer sufficient to ensure adequate protection of personal data in Europe. Hence the choice to replace the directive with a regulation which, being an act with general efficacy (applicable as such in every Member State of the EU), reaches the result of a uniform law applicable in each legal system.[27]

[25] Directive 2010/13/EU of the European Parliament and of the Council of March 10, 2010, 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).

[26] Directive (EU) 2019/790 of the European Parliament and of the Council of April 17, 2019, on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

[27] See for an overview Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means" (2019) 28(1) *Information & Communications Technology Law* 65.

However, this change does not exclusively concern the type of regulatory act, but also the substance of the underlying legal paradigm. In fact, a new regulatory approach is inherent to the GDPR, the so-called risk-based approach, which marks the emancipation from a mostly "paternalistic," albeit justified, attitude that was behind Directive 95/46.[28] In a nutshell, the principle of accountability is the driving factor of the new legal framework; it makes data controllers not only liable but also accountable and thus responsible for the processing of personal data, drawing an important shift from a purely formal understanding of legal compliance to a more reputational and business-sensitive consideration of the value of personal data (that enjoy protection as fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union). In view of this innovative approach, it is up to data controllers to implement the technical and organizational measures that are necessary to adequately protect personal data depending on the specific level of risk of the relevant processing operations.

This shift of paradigm can be understood in light of the historical and legal context: at the time of Directive 95/46/CE, the goal of the EU institutions was to establish a first set of safeguards for the protection of personal data in order to facilitate their free circulation across the Member States without unnecessary legal barriers. Personal data were, however, still subject to a predominantly economic understanding. Their free circulation required the implementation of a framework of safeguards such as that modeled by Directive 95/46, which not by chance embodied a quite paternalistic approach.

By virtue of the evolution of technologies over the last 20 years, which is mirrored by the important judgments delivered by the Court of Justice of the European Union to enforce the provisions of Directive 95/46/EC in the age of the Internet,[29] legal compliance has acquired a new and more deeper meaning. Compliance with the GDPR, in fact, stands out as a reputational factor that allows data controllers to make visible the efforts they have made to "take care" of personal data and of the protection of the rights and freedoms of individuals. GPDR compliance has thus become an opportunity for companies to act as more responsible business actors.

The rationale behind the risk-based approach encapsulated in the GDPR is well-described by one of its key provisions, namely, Article 25, named "Data protection

[28] See Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford 2015).

[29] See among others *Digital Rights Ireland et al,* joined cases C-293/12 and C-594/12 [2014]; *Google Spain,* case C-131/12 [2014]; *Maximillian Schrems v. Data Protection Commissioner,* C-362/14. See also Oreste Pollicino and Marco Bassini, "Bridge is Down, Data Truck Can't Get Through… A Critical View of the Schrems Judgment in the Context of European Constitutionalism," in Giuliana Ziccardi Capaldo (ed.), *The Global Community Yearbook of International Law and Jurisprudence 2016* (Oxford 2017) 245; Oreste Pollicino and Marco Bassini, *The Luxembourg Sense of the Internet: Towards a Right to Digital Privacy?*, in Giuliana Ziccardi Capaldo (ed., "Global Community Yearbook of International Law & Jurisprudence 2014" (Oxford 2015) 223.

by design and by default."[30] The principle of data protection by design requires that, taking into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, *both at the time of the determination of the means for processing and at the time of the processing itself*, implement appropriate technical and organizational measures. These measures (such as pseudonymization) implement data-protection principles (such as data minimization) in an effective manner and integrate the necessary safeguards into the processing of personal data. On the other—complementary—hand, the principle of data protection by default requires data controllers to implement appropriate technical and organizational measures to ensure that, *by default*, only personal data necessary for each specific purpose of processing are processed. This obligation applies to the various aspects of the processing of personal data, such as the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, these measures shall ensure that *by default* personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Against this background, the GPDR nevertheless shows some continuity with the pre-existing legal framework, where it more clearly differentiates itself from Directive 95/46/CE when outlining the obligations applicable to data controllers and data processors.

The processing of personal data can legitimately occur when one of the legal grounds provided by Article 6 is met. This catalogue reflects the same conditions that were embodied in Directive 95/46/EC, allowing for the processing of personal data, e.g., when the data subject has given consent to it, or when the processing is necessary for the performance of a contract to which the data subject is party, or for compliance with a legal obligation to which the controller is subject. Also, the processing is lawful when is necessary for the purposes of the legitimate interest pursued by the controller or by a third party (provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data). These legal grounds were already established by Directive 95/46/CE, thus adopting a merely formal approach one could correctly argue that nothing has changed in this respect. If this holds true on a purely formal basis, it is worth noting that in light of the risk-based approach, the legal basis offered by the pursuit of a legitimate interest of the controller may find a broader scope of application and constitute the condition that makes the processing of personal data lawful more frequently. Once again, the focus is on the ability of data controllers to conduct an evaluation of the circumstances of each case and assess whether, striking a balance, his/her/its legitimate interest justifies the processing of personal data of the data subjects. This explains why, even when the

[30] See also European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,* 20 October 2020.

legal rules are still the same, the rise of a new paradigm of compliance may result in different outcomes.

A remarkably important novelty of the GDPR, which the Court of Justice of the EU had already outlined in the *Google Spain* case, concerns its territorial scope of application, which is now extended to the processing of personal data of data subjects who are in the EU carried out by controllers and processors not established in the EU, when they meet one of the following conditions: The processing of personal data is related to the offering of goods or services to data subjects in the Union; the processing of personal data occurs in the context of the monitoring of the behavior of data subjects that takes place within the EU. This provision, enshrined in Article 3, para. 2, marks a turning point that has significant implications, also in the context of the debate on digital sovereignty.[31] The Court of Justice had already made clear, albeit by interpreting a different legal provision, the rationale behind the extension of the territorial reach of EU law: if entities not based in the EU wish to take advantage of their ability to target European residents, thanks to the use of digital technologies, they cannot expect that this results in the deprivation of the rights that individuals enjoy under EU law. The Latin phrase *ubi commoda, ibi et incommoda* seems to capture the essence of this novelty: the non-EU entities wishing to process data of European residents for the purposes outlined in Article 3, para. 2, cannot escape the obligations under the GDPR. This is one of the reasons why the GDPR seems to be a more universal law governing the processing of personal information worldwide, with effects and consequences not limited to European Union Member States.[32]

In addition to that, evidence of the new digital context behind the GDPR emerges particularly in connection with the catalogue of data subjects' rights and data controllers' and processors' obligations.

With respect to the rights of data subjects, the GDPR confirms to a large extent the legal situations that individuals were entitled to under Directive 95/46/EC. However, the GDPR also establishes some new rights for data subjects, namely, the right to data portability and the right to not be subject to automated individual decision-making. These rights reflect the predominantly digital context of the processing of personal data. The right to data portability consists of the right of data subjects to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format and to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. This right can be enforced when the processing is carried out by automated means and shall include the right to

[31] See the judgments of the Court of Justice in the *Schrems I* (C-362/14 [2015], *supra*) and *Schrems II* (*Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, C-311/18 [2020]) cases. See also the *Google v. CNIL* judgment on the territorial reach of the right to be forgotten: *Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*, case C-507/17 [2019].

[32] See also European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, Version 2.1., 12 November 2019.

have the personal data transmitted directly from one controller to another, where technically feasible.

The second legal situation created by the GDPR consists in the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly and significantly affects him or her. This provision does not apply when the processing is (a) necessary for the entering into, or performance of, a contract between the data subject and a data controller; (b) authorized by EU or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) based on the data subject's explicit consent.

In the cases under (a) and (c), the data controller shall nonetheless implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision.

Article 22 of the GDPR carves out a very debated provision, whose scope of application may perhaps go beyond the sole domain of data protection and thus encompass a variety of legal situations, including those where no processing of personal data actually occurs. This provision, in fact, may be interpreted as establishing some general constraints with respect to the implementation of algorithms and techniques that are likely to significantly affect individuals in a variety of situations, including the aforementioned case of content moderation (thus, with an influence on the right to freedom of expression). The rationale behind it can be better understood by looking at recital 71, which outlines a more elaborated definition of the rights that individuals may claim vis-à-vis the processing of data based on automated decision-making: the processing should be subject to suitable safeguards, which should include information specific to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment, and to challenge the decision. The actual existence of a right to obtain an explanation is by no coincidence one of the most disputed legal issues in the current debate on the large-scale implementation of algorithms, focused on how individuals may not be deprived of control of the processing of information and content.[33]

The most significant changes introduced by the GDPR, however, are placed on the side of compliance, as a consequence of the new paradigm based on the adherence to the so-called risk-based approach. The GDPR establishes a set of obligations applicable without distinction to data controllers and processors, also providing for a series of additional obligations in the presence of personal data

[33] See, e.g., Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," [2017] 7(2) *International Data Privacy Law* 76; Margot E. Kaminski, "The Right to Explanation, Explained," [2019] 34(1) *Berkeley Technology Law Journal* 189; Andrew D Selbs and Julia Powles, "Meaningful information and the right to explanation" [2017] 7(4) *International Data Privacy Law* 233.

processing that involve "high" risks for the rights and freedoms of the data subjects. The rationale underlying this articulation is quite clear: To facilitate an assessment of the actual level of risk for personal data (and individual rights and freedoms) by those subjects that are better placed to do so, i.e., the data controllers themselves. Indeed, Article 32 imposes upon data controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. In assessing the adequacy of the security level, particular account is taken of the risks deriving from the accidental or unlawful destruction, loss, modification, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed. These events are known as data breaches and are subject to an ad-hoc procedure by which controllers are required to notify these violations without undue delay (and possibly within 72 h of having become aware of it) to the competent supervisory authority.

Another general obligation requires data controllers and processors to keep records of processing activities. Generally, the obligation applies only to entities that have at least 250 employees or collaborators; however, such a quantitative requirement is replaced by a qualitative one under certain circumstances, for example, when the processing (even if conducted within organizations that do not exceed that threshold) still presents risks for the rights and freedoms of individuals.

On a second level, separate obligations apply to data controllers and processors when the processing of personal data is likely to result in a high level of risk for the rights and freedoms of individuals. Under these conditions, data controllers shall comply with the following requirements:

(a) Communication to interested data subjects in the event of a data breach (Article 34), that is due with a simple and clear language to inform individuals of the nature of the violation, except for where it would require disproportionate efforts or the controller can avoid the emergence of high risk for the relevant parties by adopting technical and organizational measures.
(b) Data protection impact assessment (DPIA), i.e., an assessment of the impact of the processing of personal data that includes an assessment of both the necessity and proportionality of the processing operations and of the risks for the rights and freedoms of the data subjects, as well as an indication of the measures envisaged to deal with the risks. When the impact assessment shows that the processing would likely result in high risk in the absence of mitigation measures adopted by the controller, the GDPR establishes an obligation of prior consultation of the competent supervisory authority prior to the processing operations being able to take place.
(c) The designation of a Data Protection Officer: this is a new figure shaped by the requirement for independence and competence. The DPO acts as a real supervisory body, exercising tasks and functions including the provision of information and advice in favor of the controller, monitoring on the effective application of the GDPR, and cooperation with the supervisory authority. The DPO must be "promptly and adequately involved in all matters concerning the protection of personal data" and provided by the controller and processor with the resources

necessary to discharge his/her duties and to access to personal data and processing operations.

This new legal framework, being grounded on the risk-based approach and shaped according to a flexible understanding of compliance, leaves data controllers with significant room to adopt the measures that better fulfill the obligations for the protection of data subjects' rights. However, this piece of legislation was framed with a clear understanding of the existing technologies at the time of its drafting, but may nevertheless give raise to new challenges with regard to disruptive technologies such as blockchain and Artificial Intelligence. The aforementioned Article 22 does not seem to capture the entire set of questions that these technologies advance nowadays. Some of these technologies (such as blockchain) may also be difficult to reconcile with the legal framework so defined when it comes to certain settings. For instance, public and permission-less blockchains may be difficult to subject to the GDPR, as far as certain provisions (such as those regarding the territorial scope of application or the right to deletion or to portability) apparently are not easily enforceable in such a digital environment. New efforts would be necessary from regulators and, where appropriate, courts to make sure that the same values that the GDPR safeguards can also be effectively protected in the context of disruptive technologies. As far as the right to be forgotten is concerned, the Court of Justice in *Google Spain* managed to enforce the Directive 95/46/EC provision on the right to cancellation vis-à-vis search engine service providers, achieving an important result by interpreting the rationale of the existing legislation and seeking a remedy that could fulfill that legal expectation in the digital world. There was no need, in other terms, to revisit the applicable law, albeit that the latter had been drafted in the pre-Internet era. Similar challenges and responses are then likely to also occur in the age of algorithms with regard to the GDPR.

4 Conclusions

The comparison conducted in the previous chapters between the domains of content and data in the European Union legal systems shows that digital technologies raise important questions that lawmakers have to address before it is too late. In the digital services market, for instance, the absence of a comprehensive legal framework has made it possible for online platforms to grow but ultimately also to acquire significant market positions that allow these new private powers to influence the circulation of content. Although content regulation is not directly the subject of an ad-hoc legal framework in the European Union and in the United States, it goes without saying that recent trends and events show the strong connection between the role of platforms and the actual scope of protection of freedom of expression. If at the beginning there were good reasons to believe that the absence of regulation would have proven beneficial and fostered the flourishing of new services, the time is probably ripe for a reconsideration of this original attitude of regulators, as content moderation carried out by social networks has proved to be more and more

influential. On the other hand, the legal framework applicable now to personal data shows a significant effort made by the European Union institutions to protect one of the core values of European constitutionalism (Europe's First Amendment, according to some scholars),[34] also vis-à-vis the role of digital platforms for which the processing of large amounts of personal data has been an inherent trait of their business model. The GDPR is probably not ready to face all the remarkable challenges and issues brought by disruptive technologies, but it is of course a good starting point whose effectiveness will be tested in the medium term. Also, it is based on a fairly flexible and open-ended approach, based on the idea that regulation can prove beneficial for both companies and individuals. It focuses on accountability and transparency, two values that may of course also play an important role in the context of the possible future regulation of online platforms, with a view to not placing constraints on the freedom to conduct business and the freedom of expression but to make and preserve the digital environment as a safer virtual square.

[34] Bilyana Petkova, "Privacy as Europe's first Amendment," [2019] 25(2) *European Law Journal* 140.