JOURNAL OF E-LEARNING AND KNOWLEDGE SOCIETY
Vol. 18, No. 3 (2022), pp. 8-21

INVITED PAPER

Digital constitutionalism to the test of the smart identity

Oreste Pollicino[a,1], Federica Paolucci[b]

[a]Università Commerciale L. Bocconi – Milan (Italy) and Agenzia europea per i diritti fondamentali, Vienna (Austria)
[a]Università Commerciale L. Bocconi – Milan (Italy)

(published: 31/12/2022)

Abstract

The law has become increasingly interested in issues related to algorithmic biases and decisions, particularly from the perspectives of the collection, use, and processing of personal data. The complex constellation of fundamental rights challenged by the new technologies is opening the door to an inedited concept of identity, citizenship, and city, shortening the distances between the world of the bits and the world of the atoms. Nonetheless, the legal issues at stake are profound and involve enforcing such rights and designing proper procedural mechanisms. In this sense, a crucial role is that of the courts since they have been and are called to find new stages of protection and guarantees. Therefore, with the aim to prove the necessity of a solid and by-design procedural mechanism, this paper is going to analyze those issues through the lenses of the krasis between algorithms and freedom of expression, and algorithms and data protection, while taking as a meaningful example the difficult enforceability of the right to erasure in the context of the algorithmic society.

DOI
https://doi.org/10.20368/1971-8829/1135815

CITE AS
Belleri, D., Baick, M., & Ratti. C. (2022). Digital constitutionalism to the test of the smart identity. *Journal of e-Learning and Knowledge Society*, *18*(3), 8-21.
https://doi.org/10.20368/1971-8829/1135815

1. Introduction

Between May 2017 and April 2019, the police in South Wales (UK) scanned approximately 500,000 faces while using automated facial recognition systems during public events. Technically speaking, FRT is identifiable as a *deep learning* system and a *multilayered deep neural network,* which can be applied to many different uses: to unlock a device; CCTV cameras used to match a face with a watchlist of possible thieves; e-boarding in the airports; e-identification systems in the public administration. The applicant, Mr. Bridges, a civil rights activist, brought a judicial claim against the law enforcement body to assess the legal basis of the technology and its compatibility with the right to respect for private life (Court of Appeal, 2020). That technology was meant to capture live biometric images automatically saved in a dataset and compared with face images already collected and itemized in a watchlist. The Divisional Court rejected Mr. Bridge's claim. On a second stance, the Court of Appeal considered the issue and found that the use by the police of the facial recognition

[1] corresponding author - email: oreste.pollicino@unibocconi.it

technology was unlawful on the ground that it was breaching the individuals' privacy and data protection rights. Remarkably, the Court found that the operation lacked a proper data protection impact assessment (DPIA), and it was insufficient to address the risks to some rights that the technology would infringe; not only on privacy but also it can produce a chilling effect on freedom of expression and freedom of association (§153).

Therefore, given «this particularly complex and difficult constellation of fundamental rights» (AG opinion, Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2013:424, para 133), the challenges of new technologies and how they are complemented with the public purposes, i.e., security and public order, impose on the (digital) constitutionalist deep thoughts on the impact of such sphere in the life of citizens. Those latter ones, as a matter of fact, are rather smart citizens, since they live in a world in-between bit and atoms. Nonetheless, data, artificial intelligence, and sensors are creating an unprecedented dimension of the *res publica,* and, consequently, of the experience of being a citizen that extends the border of the atomic world. Moreover, traditional models of the city (and human living) are called upon to coexist with the network. This immensely happens, for instance, in the context of what is called the smart city, a new sphere of digital urban space is called the smart city: an umbrella term by which the further integration of digital and real space is usually understood. Beyond any dystopian scenario that such a context is capable of generating and causing one to imagine, and which is of no interest there, the core is to be found precisely in the substance that is enabling the intersection that is taking place between urban space and the network: data. The ceaseless flows of information that from Siberia to Tierra del Fuego enable our contemporary world to function in all its forms are at the heart of the city of the future so that its functioning is rooted in the combination of Internet of Things (IoT), big data, ubiquitous computing, and the cloud. All these elements are the fundamental architectures on which the (ideal) smart citizenship rests, and they are responsible for making it more open, optimizable, and, above all, controllable.

The COVID-19 pandemic has highlighted the relevance of online platforms in the information society. For instance, Amazon provided deliveries during the lockdown phase, while Google and Apple offered their technology for contact tracing apps (Privacy-Preserving Contact Tracing, *apple.com* at www.apple.com/covid19/contacttracing). These actors have played a critical role in providing services that other businesses or, even the state, failed to deliver promptly. Therefore, the COVID-19 crisis has led these actors to become increasingly involved in our daily lives, becoming part of our social structure. In other words, their primary role during the pandemic has resulted in these actors being thought of as public utilities. Nonetheless, commentary has not been exclusively positive. The model of the contact tracing app proposed by these tech giants aroused various privacy and data protection concerns (see Daskal & Perauls, 2020). The pandemic has also shown how artificial intelligence can affect fundamental rights online without human oversight. Once Facebook and Google sent their moderators home, the effect of these measures extended to the process of content moderation, resulting in the suspension of various accounts and the removal of some content even though there was no specific reason for this (see also Dwoskin & Tiku, 2020). This situation has not only affected users' right to freedom of expression but has also led to discriminatory results and the spread of disinformation. Generally speaking, it is worth observing that the solidarity, both *infra* individuals and institution-wise, was expressed during the pandemic has also been mediated by the role of online platforms at the heart of individuals' lives and relationships.

Moreover, the increased use of algorithms to automate decision-making has sparked deep concern that such automated choices may produce discriminatory outcomes. The law has become increasingly interested in issues related to algorithmic biases and decisions, particularly from the perspectives of the collection, use, and processing of personal data. However, technological progress is, on closer inspection, putting the law in a corner from which the jurist is forced to question how AI systems integrate with the rationale of the norms for which they were intended. All without creating a context that can be to the detriment of the citizens themselves. An aspect that seems to capture the lawyer's attention is the risk that the algorithm can produce (and sometimes also reproduce) the social, racial, and gender biases in its decisions (Zarsky, 2016; Lambrecht & Tucker, 2019). Around the world, regulatory proposals are emerging to regulate artificial intelligence. Particularly, the European Union, since last April 2021, has been working on the European approach to AI with the proposal for a Regulation known as AI Act (Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussels, 21.4.2021 COM 2021). This very experience requires digital constitutionalism (for a deeper inspection of the concept, see De Gregorio, 2022) to reiterate the necessary sensitivity to bridging the challenges of new technologies with the protection of fundamental rights traditionally guaranteed to analog citizens. The legal issues at stake are a lot and, therefore, they open the floor for a deeper discussion on the enforcement as well as on the procedural mechanisms of such rights, and, therefore, on the role of the courts in addressing these challenges has not lost any significance, even during the pandemic, in its ability to resist interference from the public and private sectors. The question is whether courts will adopt new judicial frames or new strategies for dealing with the jurisdictional issue in order to address the increasing and troubling legal uncertainty surrounding new technologies. The next subsections provide an insight into the future challenges which courts will face in the field of freedom of expression and data protection. All these issues culminate in one specific and very discussed right, the right to erasure, that, in the context of AI, seems to exacerbate the challenges both to freedom of expression and data protection, being the link between the *habeas corpus* and *habeas data* (Rodotà and Conti, n. 14), since it is much entrenched with personal identity.

2. Algorithms and Freedom of Expression

The way in which we express opinions and ideas online has changed over the last 20 years. Courts have proved to have different approaches to the protection of freedom of expression online (this aspect is further explored in Pollicino, 2021). The Internet has been considered either as an opportunity by the US Supreme Court or as a threat by European courts (CJEU and ECtHR). This is no coincidence. The digital environment has indeed been a crucial vehicle for fostering democratic values such as freedom of expression (Benkler, 2006). At the same time, new threats have appeared on the horizon, leading courts to react to technology-driven changes.

At first glance, the characteristics of the Internet should have not entailed any risk for accessing information since pluralism was originally concerned with the scarcity of resources. On the other hand, in the world of atoms, one of the priorities in the media sector is to protect the pluralism of information. On the Internet, however, legal rules (and especially public law) were supposed to rely on the alleged self- corrective capacity of the market for information. Nonetheless, the evolution of the digital environment has challenged this paradigm (Valcke, Sukosd & Picard, 2015). Recently, the implementation of automated decision-making systems online has given cause for concern in terms of protection for freedom of expression.

The increasing implementation of these technologies by private actors such as search engines and social networks has led to questions as to how and to what extent automated decision-making technologies affect (or even determine) the paradigm of protection for freedom of expression online. This is not a neutral activity for the principle of the rule of law and the role of the courts as the actors called upon to express the last word when defining the boundaries of protection for rights and freedoms in the digital realm. The setting of a global private standard of protection of fundamental rights tends to create a hybrid paradigm, thus engaging the role of courts as mediators of the boundaries between law and technology. In order to understand how automation influences freedom of expression, it would be sufficient to consider closely the way in which information flows online. One example is particularly insightful in this context: enforcement of the right to be forgotten online. Search engines rely on automated decision- making systems, which help to organize and delist the vast amount of information they host. These private (and automated) systems create a need for data protection rights to be balanced against other fundamental rights, including, in particular, freedom of expression, as was made clear in the landmark decision by the CJEU in the *Google Spain* case (Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos and Mario Costeja González*, ECLI:EU:C:2014:317. See Lynskey, 2015).

This decision is indeed paradigmatic of role acquired by a private actor managing a search engine to make decisions in relation to personal data, and especially to expressions. Google enjoys broad margins of discretion in deciding whether to delist information. In fact, when search engines receive a request from a data subject, they are required to decide whether to uphold or dismiss it, thus balancing and enforcing fundamental rights online (Bassini, 2019). The primary issue is that this balancing is usually performed by artificial intelligence systems, which decide to organize and delist content. The involvement of these technologies in this field establishes another layer of complexity for freedom of expression since this fundamental right is not only balanced by a private actor like a search engine but is also subject to decision-making by automated systems, the outcome of which is not always reasonable.

These considerations could also be extended beyond the right to be forgotten online. Artificial intelligence systems help to interpret legal protection for freedom of expression by de facto setting a private standard of protection for fundamental rights in the digital environment (Klonick, 2018). It would be sufficient to focus on social media such as Facebook or YouTube in order to understand how freedom of expression and artificial intelligence are intertwined in the information society (Balkin, 2018). In fact, in order to organize (Gillespie, 2018) and moderate billions of items of content every day, platforms rely on artificial intelligence to decide whether to remove content or to signal certain expressions to human moderators. The lack of transparency and accountability within decisions concerning freedom of expression online means that what happens away from the screen cannot be measured. The implementation of machine learning technologies does not allow decisions taken in relation to expressions that are still private but that involves the public at large to be scrutinized. Absent any regulation establishing legal safeguards, online platforms will continue to be free to assess and remove speech according to their own opaque purposes (De Gregorio, 2019). Nonetheless, while US law still ensures a broad frame of protection for the Internet in general, and social media in particular, as, for instance, happened in Packingham (Packingham v North Carolina 582 US 2017), these challenges have instead led EU lawmakers to react against the power held by online platforms. By codifying some of the safeguards which the CJEU has identified in recent years in cases concerning freedom of expression online, the EU has tried to provide an initial answer to this dilemma. The adoption of the Copyright Directive can be taken as an example of a paradigm shift in that it not only considers platform liability, but also takes on board the lessons of the CJEU (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). It is no coincidence that the Copyright Directive has emphasized how obligations towards online content sharing service providers cannot overcome the ban on general monitoring (art. 17), which was firmly asserted in *Scarlet* and *Netlog* (Case C-70/10 Scarlet Extended SA v SABAM [2011] ECR I-11959; Case C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV [2012] ECR I-0000). Likewise, the creation of an economic threshold as a prerequisite for applicability constitutes another important example of proportionality, which also resulted from the need to protect the freedom to conduct business on the internal market. These examples of codification can also be noticed in soft-law documents adopted by the EU Commission in recent years in the field of hate speech and disinformation, for example (see also Pitruzzella & Pollicino, 2020). It would be sufficient to focus on the Recommendation on measures to effectively tackle illegal content online as well as the EU Code of Conduct on countering illegal hate speech online in order to understand how freedom of expression online has been taken more seriously also by lawmakers (the new "Code of Practice on Disinformation" was recently published and presented at the European Commission: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_3665).

Within this framework, the Digital Services Act will contribute to the codification of new rules and safeguards, which are also derived from EU case law (in this regard, see De Gregorio & Dunn, 2022). This change of approach might at first glance suggest a new appropriation of control over the technological factor by politicians. The new content curation safeguards should limit the role of courts in extending or narrowing the boundaries of the legal system. On the other hand, the new standards of protection are likely to result in another phase of judicial activism due to the need to fill the gaps within a legal framework, which, in the meantime, has already been superseded by new automated technologies. In other words, the courts have been far from marginalized, at least in Europe.

Nonetheless, the potential of artificial intelligence to challenge protection for fundamental rights is not limited to freedom of expression. The next subsection shows even more clearly how automated decision-making systems raise comparable challenges in the field of data protection and, consequently, encourage courts to shape protection for fundamental rights.

3. Algorithms and data protection

The *Google Spain* case could be taken as a relevant example also in the field of data protection. Indeed, as has already been observed, this case involves not only speech, but also personal data. Nonetheless, a closer look at the field of data protection can reveal other challenges for constitutional law in the information society, mainly due to the challenges to legal certainty and the unpredictability in relation to automated decision-making processes.

Over the last few years, unlike the US Supreme Court, the CJEU has shown that it clearly intends to take data protection seriously in the light of new challenges by building a European data protection fortress. Aside from *Google Spain*, as already discussed, the CJEU has had other opportunities to highlight the role of fundamental rights online.

In *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* [2014] ECR I-238) the CJEU stressed the relevance of the principle of the rule of law in avoiding the retention of personal data by public authorities for the purposes of fighting serious crime and its role in guaranteeing the limits and safeguards recognized by EU constitutional law. This was the reason why the CJEU invalidated the Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC). The disproportionate effects of its measures and the lack of safeguards in relation to data processing could result in the surveillance of the 'entire European population' (*Digital Rights Ireland,* n 54, 56).

Likewise, in the Schrems saga (Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, ECLI:EU:C:2020:559; Case C- 362/14 *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650), the CJEU went even further in order to ensure that the need to respect EU law is not negated due to the transnational exchange of personal data across the Atlantic. It is possible to consider how the parameter of adequacy is interpreted in two ways. First of all, moving from adequacy to essential equivalence could be considered a threat to the rule of law, as an extensive interpretation may reach beyond the literal wording of the provision. Nonetheless, it could also be argued that the need to ensure effective protection for the fundamental rights of privacy and personal data in the information society has led the CJEU to extend the boundaries of fundamental rights protection in order to avoid frustrating constitutional values and, de facto, to set aside the principle of the rule of law.

Nonetheless, the CJEU has not solved all of the issues. As is the case in the field of freedom of expression, it is possible to consider the codification of judicial advice. More specifically, the GDPR constituted a new step in the evolution of EU data protection law (Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation). In contrast to its approach under the Data Protection Directive adopted in 1995, which sought to achieve minimum harmonization, the EU shifted towards full harmonization by adopting the GDPR. This was not simply a formal change since the adoption of the GDPR not only avoids (potentially divergent) national implementation and fragmentation but also extends its effects horizontally into the private sector. Nonetheless, the GDPR still maintains a certain degree of discretion for Member States, which has led some to question the overall nature of the GDPR as a regulation (see, in particular, GDPR Arts 6, 9). Besides, the adoption of the GDPR does not imply that codification has solved the problem in the field of data protection and that the courts have no other roles that could be applied in place of the new EU data protection law framework. On the contrary, the courts will play a critical role in shaping a legal framework, the boundaries of which are still flexible and indirectly call for (judicial) interpretation.

This becomes evident if one focuses on issues arising in relation to new forms of automated processing that affect legal certainty and undermine the democratic safeguards that EU data protection law aims to protect. The lack of transparency and accountability in automated decision-making naturally challenges the aim of EU data protection law to ensure a transparent and fair framework for data subjects in relation to the processing of their data. Artificial intelligence is in fact proving to limit the possibilities for data controllers and subjects to carry out checks in relation to decision-making processes (Pasquale, 2015). It is no coincidence that this system clashes with the general principles of the GDPR (Art. 5 GDPR). Specifically, the principles of lawfulness, fairness, and transparency require that personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject. Nonetheless, the implementation of machine learning systems does not always allow data controllers to respect this principle. The black box effect limits the ability to look inside and understand how data inputs result in a particular output (Zarsky, 2017). Besides, the principles of purpose limitation and data minimization clash with the potential reuse of personal data for different goals by automated systems (Pasquale, 2015).

Even more importantly, the principle of accountability introduced by the GDPR requires data controllers to demonstrate compliance with the general principles mentioned above (Art. 5 (2)). For instance, the GDPR expressly requires data controllers to adopt appropriate technical and organizational measures that are designed to implement EU data protection principles in an effective manner and to integrate the necessary safeguards into processing. In addition, data controllers are also obliged to implement appropriate technical and organizational measures to ensure that, by default, only personal data that are necessary for each specific purpose are processed (Art. 25). Nonetheless, the GDPR also clarifies that, when assessing these obligations, it is necessary to take into account of "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" (Art. 24 GDPR).

The EU principles of privacy by design and by default are clear examples of the margins of discretion that a data controller can exercise in order to implement legal safeguards. Even if the data controller's responsibility is considered, the GDPR stresses that the implementation of technical and organizational measures that are capable of demonstrating compliance with the GDPR should still be read taking into account the nature, scope, context, and purposes of the processing activities of data as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons (Art. 24 GDPR). Within this context, the courts will play a crucial role in adjudicating claims that seek to scrutinize data controllers' accountability, which would otherwise be free to decide to what extent they comply with the GDPR. With this in mind, it is likely that the courts will play a critical role in interpreting the relationship between the GDPR's principles and norms and the implementation of artificial intelligence technologies. Similarly, the role of courts can also be understood by focusing on the rights of data subjects, especially the right of individuals not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (Art. 22). This right of data subjects has been analyzed primarily from the perspective of the right to explanation (Kaminski, 2019; Roig, 2017; Wachter et al., 2017; Malgieri & Comandé, 2017; Goodman & Flaxman, 2017).

Scholars have pointed out possible bases for the right to explanation, such as those provisions requiring that data subjects receive meaningful information concerning the logic involved, as well as the significance, and the envisaged consequences of, processing according to Articles 13 - 15 GDPR. In addition, the new rights provided for under the GDPR (including data portability and right to erasure) have been pinpointed as offering some legal grounds for broader control by individuals over the automated processing of personal data. This catalogue of guarantees can be better framed having regard to Recital 71 of the GDPR, which provides as follows: "in order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject, and prevent, inter alia, discriminatory effects on natural persons [...] or processing that results in measures having such an effect".

Within this context, transparency and accountability play a pivotal role. Since ensuring full transparency may prove to be difficult in this context, due to the protection afforded by legal systems to algorithms (eg through the legal protection ensured for trade secrets), courts (and data protection authorities) are likely to shape the meaning of transparency and accountability within automated decision-making systems. More specifically, this right of data subjects raises various interpretative issues, even beyond the debate on the right to explanation. Indeed, it is not easy to ensure legal certainty within this framework where there is no definition of the expression 'solely on automated processing' or of 'legal effects concerning him or her or similarly significantly affects him or her', as affirmed by the same Recital 71 of the GDPR.

The lack of clear definitions constitutes a clear challenge, which the courts will need to deal with, considering the extensive implementation of artificial intelligence technologies and the multiplicity of situations in which these systems can have legal effects on individuals. The GDPR has tried to establish some limits to the application of this right. Specifically, data controllers can rely on various exceptions where processing is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorized by Union 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 is based on the data subject's explicit consent (Art. 22 GDPR). Nonetheless, the GDPR also allows Member States to limit the application of this right of data subjects (Art. 23). This is an issue that reaches beyond technology and affects the entire structure of the GDPR. Despite its status as a regulation, it leaves the Member States broad margins of discretion at the domestic level (Malgieri, 2019). Within this framework, the role of judicial interpretation is likely to provide assistance in making policy decisions, leading to a further extension of judicial power over political power.

4. The case of the right to erasure

In the previous sections, it was given a brief overview of the main issues related to the relationship between algorithms, freedom of expression, and data protection. All these rights and issues come at stake when considering the realization of the right to erasure, as protected under art. 17 of the GDPR, in the context of AI (Floridi et al., 2022) and, particularly, machine learning (Black & Murray, 2019).

The right to erasure (or right to be forgotten) relies upon the assumption that someone's past does not clutter up someone's present. Therefore, the substantial "immortality of data" implies that these, if not updated, are destined to remain "frozen" at the very moment they are entered into the data life cycle. In an *onlife* landscape such as the one described, in which the information entered tends never to change, merely accumulating in a non-organic way, there is a risk that a person's identity has no way to ever evolve because it is crystallized, immobilized in many single instants of one's life.

This is why the right to erasure appears to be a vital tool for the future of contemporary society. It is also a very interesting procedural mechanism in the middle of the two souls of European privacy. Indeed, the Charter of Fundamental Rights of the European Union 2012/C 326/02 protects the right to privacy under Article 7 and the protection of personal data as enshrined in Article 8 (privacy and protection of private life as protected under art 7 relates to the management of personal information. Then, data protection, under article 8, provides safeguards for individuals while maintaining control of their data). The latter recognized the constitutional status of the right to data protection and also resulted in a shift from a mere economic dimension, as protected under Directive 95/46/EC, to a more comprehensive concept (as mentioned, R. Post underlined these dual conceptualisations of privacy, in particular under the lenses of the Google Spain judgment. Data privacy recalls a concept of fair processing of information and adequate measures of personal data protection, the former refers to the idea of dignity and protection of personal identity and private life. Hence, Post's conception of the right to be forgotten is distinguishing between data privacy, as protected under article 8 of the CFEU, and dignitary privacy, as protected by article 7 CFEU).

Before examining the premises for submitting an erasure request, it is crucial to distinguish between the right to erasure and the right to be forgotten. Those are frequently confused, and the GDPR does not help since it puts together the two under the same article. These two souls clearly emerged in the ECJ famous judgment known as Google Spain (as it is known, this right was much developed in the well famous case Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos - AEPD, Mario Costeja González, Grand Chamber, 13 May 2014, C-131/12. It is not the purpose of this paper to delve into this judgment. For a more in-depth analysis, this paper refers back to Pollicino, 2021), and were transposed in article 17 of the GDPR, which protects the right to be forgotten. However, this right, as developed from the looked (or under-examined) conflicts by the Court of Justice (see Pollicino & Bassini, 2014), is not meant to grant the erasure of information but their deindexing or de-listing (see Werro, 2009). In fact, the demand was not to erase data but suppress certain hyperlinks from the public result.

Therefore, the right to erasure as protected by the GDPR has a different meaning, at least on the paper. Article 17 of the GDPR grants the data subject the right to obtain the erasure of the data from the controller. The data controller proceeds with the erasure when some legal requirements are met. Namely, under European data protection law, deletion rights can be actioned in situations where the data has been processed illegally, when the consent has been withdrawn, or data are no longer necessary to fulfill a series of obligations (see article 17 par. 3 lists the grounds under which the processing is still considered necessary). Hence, the goal of the right to erasure is to re-balance power between data subjects and data processors. The data subject herewith becomes a right holder over his personal data (Tamò & George, 2014). When a data subject asks for erasure, the most reasonable circumstance is (or it should be) when data are improperly gathered, as established under article 17 para. 1 lett. d) of the GDPR (see also Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR part 1 adopted on 2 December 2019). However, as explained, granting such a result is not as easy as it may seem when data are processed within AI systems. Moreover, in this sense, the right to erasure goes hand in hand with the already mentioned minimization principle. It states that data should not be retained for longer than is necessary. However, also this latter aspect should need a reloading in order to make of the data minimization a practical tool and not just a hollow principle, as pointed out by Solove (2022).

This aspect should not be confused with the right to rectification or objection (Ausloos, 2016). The right to erasure is a weapon in the hand of the data subject; the data retention obligations, instead, are requirements to which the data processor is bound independently from the data subject's request.

On the opposite stance, the right to be forgotten (some scholars refer to it as the right to oblivion, Tamò & George, 2014) is not about removing data, but, as it was premised, it is connected with the right to control one's information. Hence, the right to be forgotten requires removing personal data from information tools or search engine results if an individual makes a valid request. The difference is not only semantic but logical. On the one hand, the right to erasure is a bureaucratic request to have data subject's data deleted or destructed; on the other hand, the right to be forgotten, profoundly linked with the expression of one's identity, is a request to be left alone (not by chance the referral is to the very first concept of privacy, as elaborated by Warren & Brandeis, 1890). It involves control over information privacy rather than the exercise of compliance data protection rights. As a result, the European privacy souls are reflected as protected under the Charter of Fundamental Rights of the European Union.

In fact, the right to be forgotten is not really about removing data. Nevertheless, it is a request that addresses the prohibition of search results to show a given piece of information and, more broadly, information dissemination. Hence, under the GDPR formulation, there is very little space for a right to be forgotten which means *oblio* (oblivion) since article 17 only involves a right to erasure. The intention of the European legislator, by putting under parenthesis the referral to the right to be forgotten, seems to give voice to both the perspective, at least in the *ratio legis*.

Out of the theoretical conflict, the main problem concerning the right to erasure (or the right to be forgotten) relies on the complexity of real-life tech and compliance environments. As it was previously announced, the practical realization of this right seems quite far from being achieved. The vagueness of Article 17, the comprehensive circumstances under which this right does not apply (para 2 and 3), and the technical neutrality of the norm, are just some of the issues at stake when it comes to the right to erasure.

Lastly, the fact that the word itself "erasure" does not clarify what the data processor demands to comply with the data subject's request (Villaronga et al., 2018). This is not a compliance problem only, but it also exposes the data processors to Authorities' sanctions (furthermore, regarding this latter aspect, the European Data Protection Board recently published the 'Guidelines 04/2022 on the calculation of administrative fines under the GDPR', open to public consultation, adopted on 16 May 2022). This aspect has at least two chilling effects. On the one hand, it can harness innovation and tech investments in the European market; on the other, it leaves space for even more opaque data processing and the adherence to middle-ground solutions that are unsatisfactory from either compliance or protection of fundamental rights. The risk relies on the reproduction of algorithmic shadow, meaning "the persistent imprint of the data that has been fed into a machine learning model and used to refine that machine learning system" (Li, 2022). Hence, even if data are deleted, at the state of the art of the current technical and regulatory framework, the machine can reproduce that same result since the act of deletion is not attacking the set on which it has been trained. Therefore, the following paragraph will further point out the main legal clashes in enforcing the right to erasure in machine learning systems.

4.1. "Lost in translation": a primer on machine unlearning helplessness under article 17

Machine learning outcomes are the result of statistical inferences (Floridi et al., 2022). When machine learning systems are involved, another aspect that makes the request for deletion difficult is identifying the data set that should be ultimately deleted. As a matter of fact, the programmers of contemporary machine learning systems create sets of data to be used as training data. On the base of this data set – which can be filled with both personal and non-personal data – the machine is requested to run the algorithm on the training data and to achieve a given goal by finding common patterns and producing a model that can be further deployed to achieve the ultimate goal and outcome. Hence, in this complex pattern, some questions emerge. When the data processor receives a request for erasure from the data subject, which kind of data is to be deleted? From which datasets? And, more importantly, how to actually obtain the erasure? Notably, in the case of different datasets, it is natural that personal data may be involved both in the training set and in the analysis set. It is to be said now that there are no crystal-clear answers to these questions (the issue will be further analyzed in the second part of the research project, also by running some empirical research in collaboration with data scientists). Some technical remedies are proposed, such as anonymization of data, functional encryption, selective amnesia, and model breaking [the author is primarily relying on the findings proposed by Villaronga et al. (2018). Other technical measures are studied in the following papers, (Cabral, 2020; Greengard, 2022)]. However, none of them seem to tackle the core of the problem: to clarify the extent of the right to erasure in the machine learning perspective.

Particularly, as mentioned above, there are some very technical specificities in the governance design of AI that are hard to reconcile with the GDPR. Another huge issue is to be found in the current lack of legal certainty as to how AI can be designed in a manner that is compliant with the regulation is not just due to the specific features of data protection rights. Moreover, this tension between GDPR and machine learning happens since the latter are designed to render the (unilateral) modification of data difficult. This matter is hard to reconcile with the GDPR's requirement that personal data be erased when specific circumstances apply (this aspect does not emerge only about machine learning but also with blockchain technology, as pointed out by Michele Finck in the study conducted for the European Parliament. Directorate General for Parliamentary Research Services, 2019).

Hence, there are three main relevant conceptual uncertainties threatening both data subjects' rights and processors' obligations.

First and foremost, many uncertainties rely on the term "erasure." Deleting data from machine learning data sets is burdensome since it implies retraining the entire model. It does not "address the underlying problem of making sensitive data disappear or become completely untraceable" (Greengard, 2022).

Secondly, it is challenging to demonstrate that the retrained model is fully corrected. Namely, it has been cleaned up from the wrongfully obtained data, and the biased are not reproduced. Technical factors and governance design thus burden the difficulty of complying with Article 17 GDPR. Indeed, even if there would be a means of ensuring compliance from a technical perspective, it may be organizationally tricky to reach out to all the datasets.

Thirdly, because of a certain degree of unpredictability and autonomy is frequently challenging to find who the liable party in the case of damage caused by artificial intelligence applications is. In particular, it is to look at those situations in which the outcome of the processing carried out by the artificial intelligence is not fully controllable *a priori* (in this regard, in fact, there is a part of the literature that reflects on the establishment of a new AI liability, see *ex multis* Bassini et al., 2018). Moreover, according to the principle of accountability is the processor's duty to identify "taking into account state of the art, the costs of implementation and the nature, scope, context, and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller, and the processor, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk" (see article 32 of the GDPR. Moreover, it is to note that the right to erasure obligation imposed is an obligation of means and not an obligation of ends). Hence, the legislator delegates to the data processor the burden of identifying how to fulfill the requirements dictated by the rule, dropping them into the concrete case, and taking responsibility not only for implementation but also for evaluating the risks. Those aspects emerge when the processing is not linear and involve data controllers and sub-controllers since, often, their contracts establish the execution of some data subject's rights, including the right to erasure. Therefore, the logic of accountability is challenged not only on the crowded level of responsibilities arising from the regulation but also in the case of assigning responsibilities to the presence of automated decision-making (see, in particular, Grozdanovski, 2021). Lastly, Article 17 reflects a sense of data memory that relies on humans, not the somewhat different machine memory.

All these aspects that have been listed here involve several uncertainties in interpreting and applying GDPR, especially the right to erasure, posing a strong interpretative work on the courts. This creates a deficiency in the norm that states the European status of privacy as the First Amendment (Petkova, 2019) and provokes a burden on the data processors, typically private actors, which are demanded to find a way to achieve this goal, technically and legally. As was previously mentioned, this opaque situation also affects the rights of the data processor. As a matter of fact, and, particularly with regard to facial recognition systems, it is possible to observe a trend followed by many European – and not only (see the Federal Trade Commission sanction in the case Everalbum, Inc., also d/b/a Ever and Paravision, decision and order docket no. c-4743/2021) – authorities that are sanctioning companies that collected face data asking for their deletion. Since, as noted above, it is highly complex to ensure erasure of some kind, such a sanction seems to go to exacerbate those opacities that already in themselves put the rights of individuals at risk, going to undermine the true *ratio* for sanctions: namely, to be effective, proportionate, and dissuasive (Article 29 Data Protection Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679', adopted on 3 October 2017).

5. Digital Constitutionalism in Action: Which Remedies can be Invoked against the Emergence of Digital Private Powers?

In the light of the context set out above, in which the judicial enforcement of fundamental rights is strictly connected with the new challenges of digital constitutionalism, one particular question needs to be addressed (and possibly answered): which remedies should be available to achieve the aims of this new round of modern constitutionalism, with specific regard to the rise of new private powers in competition with public authorities?

Two possible remedies can be identified. The first concerns the possible horizontal application of fundamental rights vis-à-vis private parties. The second focuses instead on the path that could be followed in the new season of digital constitutionalism and will explore, in particular, the possibility that a constellation of new rights could be identified to deal with the new challenge posed by algorithms. In other words, the Easterbrook dilemma between the 'law of animals' and the 'law of horses' will be considered from both sides. On the one hand, the horizontal effects doctrine focuses on existing instruments applied to new (digital) legal challenges. On the other hand, calls for the introduction of new rights arise out of the opposite trend, which seeks to rethink categories by providing new substantive and procedural safeguards.

The suitability of these two remedies will be assessed by considering each of them in turn, starting with the issue of the possible horizontal application of fundamental rights. It is evident that, in order to understand the feasibility of such remedies in the context of new digital challenges, it is important to take a step back and explore briefly the theoretical foundations of the issue.

A good starting point could be Alexy's assumption that the issue of the horizontal effect of fundamental rights protected by Constitutions (and Bills of Rights) cannot be detached in theoretical terms from the more general issue of the direct effect of the same rights (Alexy, 2002; Romeo, 2018). In other words, according to the German legal theorist, once it is recognised that a fundamental right has a direct effect, that recognition must be characterized by a dual dimension. The first, vertical dimension concerns the classic relationship of 'public authority vs individual freedom', while the second, horizontal dimension focuses on the relationship between private actors, but also, as mentioned above, the much less classic relationship between new private powers and individuals/users.

The problem with Alexy's assumption, which is quite convincing from a theoretical point of view, is that the shift from the Olympus of the legal theorist to the arena of the law in action risks neglecting the fact that the approach of courts from different jurisdictions might be quite different as far as the concrete recognition of the horizontal effect of fundamental rights is concerned. This should not come as any surprise because the forms and limits of that recognition depend on the cultural and historical crucible in which a specific constitutional order is cultivated.

As far as the US is concerned, the state action doctrine apparently precludes any possibility to apply the US Federal Bill of Rights between private parties and consequently any ability for individuals to rely on such horizontal effects, and accordingly to enforce fundamental rights vis-à-vis private actors (Gardbaum, 2003; Tushnet, 2003; Huhn, 2006). The reason for this resistance to accepting any general horizontal effect on the rights protected by the US Federal Bill of Rights is obviously that the cultural and historical basis for US constitutionalism is rooted in the values of liberty, individual freedom, and private autonomy. The state action doctrine is critical to understanding the scope of the rights enshrined in the US Constitution. Indeed, were the fundamental rights protected by the US Constitution to be extended to non-public actors, this would result in an inevitable compression of the sphere of freedom of individuals and, more generally, private actors. For instance, such friction is evident when focusing on the right to free speech, which can only be directly enforced vis-à-vis public actors.

Historically, the state action doctrine owes its origins to the civil rights cases, a series of rulings dating back to 1883 in which the US Supreme Court recognized the power of the US Congress to prohibit racially-based discrimination by private individuals in the light of the Thirteenth and Fourteenth Amendments.

Even in the area of freedom of expression, the US Supreme Court extended the scope of the First Amendment to include private actors on the grounds that they are substantially equivalent to state actors. In *Marsh v Alabama* (326 US 501, 1946) the US Supreme Court held that the State of Alabama had violated the First Amendment by prohibiting the distribution of religious material by members of the Jehovah's Witness community within a corporate town, which, although privately owned, could be considered to perform a substantially recognizable 'public function' in spite of the fact that, formally speaking, it was privately owned. In *Amalgamated Food Emps Union Local 590 v Logan Valley Plaza* (391 US 308, 1968), the US Supreme Court considered a shopping center similar to the corporate town in *Marsh*. In *Jackson v Metropolitan Edison Co* (419 US 345, 1974), the US Supreme Court held that equivalence should be assessed in the exercise of powers traditionally reserved exclusively to the state. Nonetheless, in *Manhattan Community Access Corp v Halleck* (587 US, 2019), the US Supreme Court more recently adopted a narrow approach to the state action doctrine, recalling, in particular, its precedent in *Hudgens v NLRB* (424 US 5071976).

This narrow approach is also the standard for protecting fundamental rights in the digital domain and, consequently, the US Supreme Court would seem to restrict the possibility to enforce the free speech protections enshrined in the First Amendment against digital platforms, as new private powers. More specifically, and more convincingly, it has been observed by Berman that the need to call into question the implications of a radical state action doctrine (Berman, 2000) can lead, in the digital age, to the transformation of cyberspace into a totally private 'constitution free zone' (Bassini, 2019, p. 182). Balkin has highlighted a shift in the well-established paradigm of free speech, described as a triangle involving nation-states, private infrastructure, and speakers. In particular, digital infrastructure companies must be regarded as governors of social spaces instead of mere conduit providers or platforms (Balkin, 2012). This new scenario, in Balkin's view, leads to a new school of speech regulation triggered by the dangers of abuse by the privatized bureaucracies that govern end-users arbitrarily and without due process and transparency; it also entails a danger of digital surveillance that facilitates manipulation.

Shifting from the US to Europe, the relevant historical, cultural and consequently constitutional milieu is clearly very different. The constitutional keyword is *Drittwirkung*, a legal concept originally developed in the 1950s by the German Constitutional Court, which presumes that an individual plaintiff can rely on a national Bill of Rights to sue another private individual alleging the violation of those rights [The *Lüth* case concerned a *querelle* about the distribution of the anti-Semitic movie *Jüd Jüss* in a private location. Following the conviction, Lüth appealed to the German Constitutional Court complaining of the violation of her freedom of expression. The German Constitutional Court, there- fore, addressed a question relating to the extension of constitutional rights in a private relationship. In this case, for the first time, the German court argued that constitutional rights not only constitute individual claims against the state, but also constitute a set of values that apply in all areas of law by providing axiological indications to the legislative power, executive, and judicial. In the present case, the protection of freedom of expression develops not only vertically towards the state, but also hori- zontally since civil law rules must be interpreted according to the spirit of the German Constitution. German Constitutional Court, judgment of 15 January 1958, 1 BvR 400/51]. In other words, it can be defined as a form of horizontality in action or a total Constitution (Kumm, 2006). It is a legal concept that, as mentioned, has its roots in Germany and then subsequently migrated to many other constitutional jurisdictions, exerting a strong influence even on the case-law of the ECJ and ECtHR (*X and Y v The Netherlands*, App no 8978/80, Judgment of 26 March 1985).

It should not come as any surprise that a difference emerged between the US and European constitutional practice as regards the recognition of horizontal effect on fundamental rights. As noted above, individual freedom and private autonomy are not constitutionally compatible with such recognition. On the other hand, however, human dignity as a super-constitutional principle supports such recognition, at least in theory (Dupré, 2016).

However, as mentioned above, it is also worth reaching beyond the debate on horizontal/vertical effects of fundamental rights in the digital age in order to propose an alternative weapon for the challenges that will need to be faced during the new round of digital constitutionalism. Most notably, it is necessary to propose a frame that describes the relationship between the three parties that Balkin puts at the heart of the information society: platforms, states, and individuals (Balkin, 2012). In other words, a digital habeas corpus of substantive and procedural rights should be identified, which can be enforced by the courts as they are inferred from existing rights protected under current digital constitutionalism (De Gregorio, 2019, 2022). While substantive rights concern the status of individuals as subjects of a kind of sovereign power that is no longer exclusively vested in public authorities, procedural rights stem from the expectation that individuals have to claim and enforce their rights before bodies other than traditional jurisdictional bodies, which employ methods different from judicial discretion, such as technological and horizontal due process.

If, on the one hand, this new digital *pactum subjectionis* requires new rights to be recognised and protected, it is also necessary to understand how their enforcement can be effective, how they can actually be put into practice. In other words, it is necessary to couple the claim for a new catalogue of substantive rights with the need for certain procedural guarantees that allow individuals to ensure that these 'quasi-legal' expectations can actually be met. Therefore, it is necessary to speculate also on the 'procedural counterweight' to the creation of new substantive rights, focusing on the fairness of the *process* by which individuals can enforce them. In fact, since speculation has hitherto focused on the exercise of powers, there is no reason to exclude from the scope of procedural guarantees those situations in which powers are vested in private bodies charged with the performance of certain public functions (della Cananea, 2016).

Digital platforms can be said to exercise administrative powers that are normally vested in public authorities. However, considering how rights can be exercised vis-à-vis these new actors, vagueness and opacity can still be discerned within the relevant procedures. Among others, the right to be forgotten clearly shows the lack of appropriate procedural safeguards, since steps such as the evaluation of a delisting request and the adoption of the relevant measures (whether consisting of the removal of a link or confirming that it is lawful) rely on an entirely discretionary assessment, supported by the use of algorithms. Therefore, the merely horizontal application to the fundamental right to data protection enshrined in Article 8 EUCFR does not prove to be satisfactory. Moreover, the notification and take down mechanisms implemented by platforms hosting user-generated content do not entirely fulfil the requirements of transparency and fairness so as to render the status of the user/individual enforcing his/her rights vis-à-vis these platforms comparable to the status of citizens exercising their rights against public authorities. It is argued that the time is ripe for filling this gap.

Procedural rights will play a pivotal role in ensuring that these new substantive rights are actually protected and rendered enforceable vis-à-vis emerging private actors. Within the context of research into big data and predictive privacy violations, such as the case of the right to erasure witnesses.

6. Conclusion

In the right to erasure and the right to be forgotten saga, the European Court played a crucial role in defining a high standard under EU Law to protect fundamental rights of privacy and data protection by distinguishing the latter's protection from the former. However, it is now time to consider the risks of such an approach. Risks are reflected by the mentioned issues on stretching the stitches of the right to erasure within machine learning systems. Unlike the past, the current challenges do not seem to be controlled under the previous framework but, on the contrary, it poses new issues that must be solved with new perspectives (Custers, 2022). It is definitely not possible to treat machine memory as human memory.

In light of the analysis so far, there seems to be little doubt that the right to erasure has many legal – and technical – issues being applied in the case of personal data processed by machine learning systems. Therefore, the *krasis* between the data protection framework, the protection of individuals' private lives, and the safeguard of economic rights are incredibly challenged by the need and the novel relationship created by AI. At the state of the art, the two systems are "lost in translation," and this missing bridge directly threatens the individuals' human rights and the safe development of machine learning systems (a new duty of privacy loyalty as in the words of Richards & Hartzog, 2020). The European data protection laws, abstractly the best possible model, often turn out to be inadequate in providing adequate protection and ineffective. This is all the more so when confronted with artificial intelligence applications in which the *a priori* determinability of computing processes is not apparent. The purpose of processing is often unclear. Hence, the reloading of the right to erasure is the vessel of a new culture of privacy that sheds light on the need for a new model that considers these challenges from another perspective.

This cultural evolution is the necessary and natural continuation of the transition between the proprietary model based on informational self-determination (*ius excludendi alios*) (Soro, 2021), to another paradigm based on the promotion and free development of personality, including in all social formations it takes place.97 This revolution must necessarily rethink the relationship between data and artificial intelligence and, therefore, the dichotomy of personal and non-personal data, seeking to understand how the latter can provide valuable information that makes up an individual's identity. Only by making this shift will it be possible to make the substantive and procedural protections already provided for personal data protection – including the right to erasure – effective for AI. On the contrary, this crystallization will only impose models designed for different eras and technologies on a world where these metaphors no longer seem to belong, eroding the soundness of an entire mechanism at the expense of protecting fundamental rights. Within this framework, both the horizontal effect doctrines and new substantive and procedural rights seem to be promising candidates among the available remedies to be necessarily included in the AI Act. In the face of these challenges, the courts will likely by no means lose the predominant role over political power acquired in recent years. The challenges raised by new automated technologies can potentially operate as a new call for courts to protect fundamental rights in the information society.

Notes

The paper is the result of the idea of both the authors. However, para. 2, 3, and 5 are ascribable to Oreste Pollicino and para. 4 and 4.1 to Federica Paolucci. Paragraphs 1 and 6 are attributable to both the authors.

References

Alexy, R. (2022). *A Theory of Constitutional Rights* (pp. 570-71). Oxford, Oxford University Press. See

Ausloos, J. (2016). The Interaction between the Rights to Object and to Erasure in the GDPR' (*CITIP blog*, 25 August 2016) at https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to- erasure/

Balkin, J. (2018). Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' 51. *UC Davis Law Review* 1149.

Balkin, J.M. (2012). Free Speech Is a Triangle. 118 *Columbia Law Review* 2011.

Bassini, M. (2019). Fundamental Rights and Private Enforcement in the Digital Age. *European Law Journal* 182, 25(2).

Bassini, M., Liguori, L., & Pollicino, O. (2018). Sistemi Di Intelligenza Artificiale, Responsabilità e Accountability. Verso Nuovi Paradigmi?', in Franco Pizzetti (Eds), *Intelligenza artificiale, protezione dei dati personali e regolazione*. Giappichelli.

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* New Haven, CT, Yale University Press.

Berman, P.S. (2000). Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation. 71 *University of Colorado Law Review* 1263.

Black, J., & Murray, A.D. (2019). Regulating AI and Machine Learning: Setting the Regulatory Agenda. 10 European journal of law and technology.

Cabral, T.S. (2020). Forgetful AI: AI and the Right to Erasure under the GDPR. 6 European Data Protection Law Review 378.

Custers, B. (2022). New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era. 44 Computer Law & Security Review 105636.

Daskal, J., & Perault, M. (22 May 2020). The Apple-Google Contact Tracing System Won't Work. It Still Deserves Praise', *Slate* at https://slate.com/technology/2020/05/apple-google-contact- tracing-app-privacy.html

De Gregorio, G. (2019). Democratising Content Moderation: A Constitutional Framework' 36. *Computer Law and Security Review* 1.

De Gregorio, G. (2022). *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge University Press. doi:10.1017/9781009071215

De Gregorio, G., & Dunn, P. (2022). The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' 59. *Common Market Law Review* at https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/59.2/COLA2022032 accessed 20 May 2022.

della Cananea, G. (2016). *Due Process of Law Beyond the State.* Oxford, Oxford University Press.

Directorate General for Parliamentary Research Services (2019). *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?* (Publications Office 2019) at https://data.europa.eu/doi/10.2861/535

Dupré, C. (2016). *The Age of Dignity. Human Rights and Constitutionalism in Europe.* Oxford, Hart Publishing.

Dwoskin, E., & Tiku, N. (24 March 2020). Facebook Sent Home Thousands of Human Moderators due to the Coronavirus. Now the Algorithms are in Charge. *The Washington Post* at www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/

Floridi, L., et al. (2022). CapAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act. Social Science Research Network.

Gardbaum, S. (2003). The "Horizontal Effect" of Constitutional Rights. 102 *Michigan Law Review* 388.

Gillespie, T. (2018). *Custodians of the Internet Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT, Yale University Press.

Goodman, B., & Flaxman, S. (2017). European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". *AI Magazine* 38(3) 50.

Greengard, S. (2022). Can AI Learn to Forget?. https://cacm.acm.org/magazines/2022/4/259391-can-ai-learn-to-forget/fulltext

Grozdanovski, L. (2021). In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law. 58 Common Market Law Review. At https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/58.1/COLA2021005

Huhn, W.R. (2006). The State Action Doctrine and the Principle of Democratic Choice. 84 *Hofstra Law Review* 1380.

Kaminski, M.E. (2019). The Right to Explanation, Explained. *Berkeley Technology Law Journal* 189, 34(1).

Klonick, K. (2018). The New Governors: The People, Rules, and Processes Governing Online Speech' 131. *Harvard Law Review* 1599.

Kumm, M. (2006). Who is Afraid of the Total Constitution? Constitutional Rights as Principles and the Constitutionalization of Private Law. *German Law Journal* 7(4) 341.

Lambrecht, A., & Tucker, C. (2019). Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads. *Management science*, 65(7), 2966-2981.

Li, T. (2022). Algorithmic Destruction. SMU Law Review, SSRN.

Lynskey, O. (2015). Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. 78 *Modern Law Review* 522.

Malgieri, G. (2019). Automated Decision-making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations. *Computer Law and Security Review* 1, 35(5).

Malgieri, G., & Comandé, G. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. 7 *International Data Privacy Law* 243.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information.* Cambridge, MA, Harvard University Press.

Petkova, B. (2019). Privacy as Europe's First Amendment. 25 European Law Journal 140.

Pitruzzella, G., & Pollicino, O. (2020). *Hate Speech and Disinformation: A European Constitu- tional Perspective.* Milan, Bocconi University Press.

Pollicino, O. (2021). *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* Bloomsbury Publishing.

Pollicino, O. (2021). *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*. Bloomsbury Publishing.

Pollicino, O., & Bassini, M. (2014). Reconciling Right to Be Forgotten and Freedom of Information: Past and Future of Personal Data Protection in Europe. 2 Diritto pubblico comparato ed europeo 641.

Richards, N.R., & Hartzog, W. (2020). A Duty of Loyalty for Privacy Law. Social Science Research Network. SSRN Scholarly Paper 3642217 at https://papers.ssrn.com/abstract=3642217 accessed 18 May 2022.

Roig, A. (2017). Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)' 8(3) *European Journal of Law and Technology* 1.

Romeo, G. (2018). Building Integration Through the Bill of Rights? The European Union at the Mirror. 47 *Georgia Journal of International & Comparative Law* 21.

Solove, D.J. (2022). The Limitations of Privacy Rights'. Social Science Research Network. SSRN Scholarly Paper 4024790 at https://papers.ssrn.com/abstract=4024790

Soro, A. (2021). Un Diritto Di Libertà, *Riservatezza* Treccani.

Tamò, A., & George, D. (2014). Oblivion, Erasure and Forgetting in the Digital Age. 5 JIPITEC at http://www.jipitec.eu/issues/jipitec-5-2-2014/3997

Tushnet, M. (2003). The Issue of State Action/Horizontal Effect in Comparative

Constitutional Law. 1 *International Journal of Constitutional Law* 79.

Valcke, P., Sukosd, M., & Picard, R. (Eds.) (2015). *Media Pluralism and Diversity: Concepts, Risks and Global Trend*. London, Palgrave.

Villaronga, E.F., Kieseberg, P., & Li, T. (2018). Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten. 34 Computer Law & Security Review 304..

Wachter, S., Mittelstadt, B.D., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making does not Exist in the General Data Protection Regulation. 7 *International Data Privacy Law* 76.

Warren, S.D., & Brandeis, L. (1890). The Right to Privacy' (1890) 4, no.5 Harvard Law Review 193.

Werro, F. (2009). The Right to Inform v. The Right to Be Forgotten: A Transatlantic Clash. Social Science Research Network. SSRN Scholarly Paper ID 1401357 at https://papers.ssrn.com/abstract=1401357

Zarsky, T. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology, & Human Values*, 41(1), 118-132.

Zarsky, T.Z. (2017). Incompatible: The GDPR in the Age of Big Data 47 *Seton Hall Law Review* 995.