Bialystok Legal Studies
Białostockie Studia Prawnicze
2026 vol. 31 no. 1

sciendo

DOI: 10.15290/bsp.2026.31.01.02

Received: 24.08.2025
Accepted: 13.12.2025

Arianna Maceratini
University of Macerata, Italy
arianna.maceratini@unimc.it
ORCID ID: 0000–0001–7519–9016

The Digital Agora: Emerging Technologies, Freedom of Information and Democratic Space

Abstract: The digital revolution, fuelled by information technologies, has profoundly transformed the perception of reality and subjective interactions, with significant political, legal, social and economic implications. Current communication technologies hold a pervasive, often opaque, computational power that develops in virtual contexts in which the individual merges with the digital environment. In this scenario, the risk is that algorithmic solicitations, based on in-depth knowledge of individual habits, produce a form of hidden governance of choices, accentuating the information asymmetry between users and digital service providers. The contemporary world, defined by data correlations and algorithmic selections, thus takes on the characteristics of a 'black-box society', in which the distinction between the state and the market is blurred, new forms of surveillance emerge, and democratic principles and the rule of law are called into question. In the absence of defined spatial boundaries, regulatory divergences between the United States and Europe on the right to freedom of expression highlight the need to harmonize different legal and cultural visions. Therefore a global regulatory approach is proposed that can integrate human values into algorithms and promote digital education as a tool to increase civic awareness and collective responsibility in the information ecosystem.

Keywords: computational power, digital information, right of expression, democracy, rule of law

Introduction

The informational revolution, generated and fuelled by digital technologies, has profoundly transformed our perception of reality and the dynamics of human interactions, with wide-ranging political, legal, social and economic implications (Floridi, 2012). This evolution has given rise to an 'infosphere' populated by both natural and

© 2026 Arianna Maceratini published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

artificial informational agents capable of autonomously collecting and processing data (Floridi, 2017). Within this infosphere, the virtualization of reality redefines value: access to digital information now complements, and often exceeds, the importance of owning material goods, revealing a shift toward the immateriality of what is exchanged (Amato Mangiameli & Campagnoli, 2020; Han, 2022; Rifkin, 2001). In this context, contemporary information and communication technologies exercise a subtle yet pervasive computational power (Durante, 2019), shaping a virtual dimension in which individuals become part of the environment itself, experiencing an 'onlife' continuity between the digital and the analogue worlds (Floridi, 2017, p. 53).

The construction of the individual as an informational system leads to a proxy culture driven by vicarious or indirect data that establishes correlations between information and predictions that are often *contra legem* and discriminatory (O'Neil, 2017, p. 28). This functions from the perspective of the personalization of performance, through which the individual is understood first and foremost as a consumer (Rifkin, 2001, p. 65), using recommendation systems driven by profit motives which may differ from the values developed by a genuinely democratic discourse (Habermas, 2023). So even if algorithms seem to operate for a neutral implementation of personal satisfaction, there is no objectivity in the filtering or in the personalization of information (Thurman et al., 2013); instead, they work with users in a 'co-productive manner' (Jasanoff, 2004) and, as they are made by humans, they could be fallible and spoiled by many prejudices. In addition, algorithms progressively narrow subjective action, reducing it to a sum of choices and preferences already expressed. The result is crystallized thought, a procedure that solves problems through codified steps, excluding spontaneity and the unexpected (Han, 2022, pp. 11, 53–54; Talia, 2018, p. 98), and highlighting several critical issues connected to the lack of transparency in the use of the criteria that define the output, which result in inadequate information being provided to the public (Amato Mangiameli, 2019; Palazzani, 2020; Zambonelli, 2020). In these circumstances, the risk is that suggestions become so performant as to establish a kind of hidden government of choice (Zambonelli, 2020, p. 66); in fact, although it is still the subject who decides on circumscribed aspects of the virtual experience, the outcome of the latter appears to be determined mainly by the algorithm. This amplifies, with unprecedented strength, the traditional nexus between knowledge, surveillance and power (Foucault, 1975), but from another perspective – that is, through a *smart* power that through algorithmic opacity makes the individual transparent, and that does not order but subtly induces the optimization of behaviour and the control of actions (Han, 2023, pp. 9–11), structuring a relevant information asymmetry between internet provider, digital platforms and the user of online services (Perri, 2020, pp. 17–18).

This essay examines some problematic nodes of the 'virtual agora' through the lens of algocracy, that is, the power of algorithms and the platforms that deploy them, focusing on their impact on freedom of information in the democratic space. From

a philosophical-legal perspective, it argues that only by intertwining normative and ethical-political dimensions can the complexity of digital transformations in public discourse be grasped: in this regard, rather than proposing a new theoretical model, the paper offers some critical reflections that invite a rethinking of traditional paradigms through algorithmic mediation, comparing European and US approaches that, while they share a concern for the influence of digital platforms, diverge in their cultural premises and regulatory visions.

1. The algocracy in the era of digital information

According to Aneesh (2006, 2009), algocracy, a term originally connected to the organization of the workplace, describes a networked digital environment in which informational power is increasingly exercised by algorithms that enable certain modes of interaction and organization while inhibiting others. Danaher later expanded this notion, defining algocracy as 'a system in which algorithms are used to collect, compare and organize the data by which decisions are made thereby shaping the ways in which individuals interact with information and with one another within governance systems' (2016, pp. 2–3). Algorithms are conceived as precise, executable sequences of actions designed to solve specific problems, and are characterized by the finiteness of the steps, their generality in referring to and solvinga class of problems, and the unambiguity and repeatability of the nexus between data and results (Sartor, 2022, pp. 96–97). In this sense, they function as tools of governance and as forms of 'politics by other means' (Latour, 1988, p. 142), embodying the technocratic logic of digital power. Consequently, in a society where information is widely shared and mediated through data correlations and algorithmic selection, it paradoxically entails inhabiting a 'black-box society' (Pasquale, 2015), in which the boundaries between state and market increasingly blur.

In this regard, a relevant critical issue is represented by the economic exploitation of digital data, often obtained through mere exchanges on the Web, but in the absence of the fully informed and conscious consent of the stakeholders (Faini, 2019, p. 316; Rodotà, 2014, pp. 27–32), an exploitation which is set up by a small number of public and private operators able to control the wealth of information, and exercising, in an opaque way, an epistemic monopoly (Orrù, 2021, p. 205) and an authority equal, if not superior, to that of national governments in guiding the opinions and actions of citizens (Zambonelli, 2020, p. 13). In this way, a private and self-regulatory power, which takes on the characteristics of factual sovereignty, puts in place political mechanisms of dubious legitimacy that introduce unprecedented forms of surveillance and discrimination (Rodotà, 2012, pp. 394–395) that reflect on the very future of democracy (Faini, 2019, p. 63) – unknowns that are made even more serious by their lack of spatial circumscription or corresponding legal regulation (Casonato,

2019b, p. 178). Furthermore, a lot of disinformation can be found on the Web, fuelled by fake news (Ziccardi, 2019, p. 187) and often also supported by national media and institutional profiles, which are aimed at obtaining a direct, albeit virtual, relationship with citizens (Ziccardi, 2019, p. 23): this, in the abstract, could present a considerable possibility for information and participation, but unfortunately it frequently resolves in the discrediting of divergent opinions and leads to distracting attention from issues of general relevance (Habermas, 2023, p. 69). The viral amplification of messages lowers the level of public discussion and political debate (Habermas, 2023, pp. 64, 113–114), generating a gradual overlap between public and private. In fact, 'real-time digital democracy is a *democracy of presence*: it turns the smartphone into a *mobile parliament* that debates continuously and everywhere […] It accelerates the degeneration of the public sphere because it tirelessly publicizes the private sphere' (Han, 2023, pp. 35–36; emphasis original). These dynamics have significant implications for the protection of individual rights (Ziccardi, 2019, p. 37), as seen from the proliferation of fake profiles, trolls, spam, viruses and chatbots that generate algorithmic communication flows mimicking natural conversation (Ziccardi, 2019, pp. 70–71, 188).

Equally concerning is the phenomenon of reverse censorship, which drowns out unwelcome or minoritarian information in an overabundance of content, fabricating artificial consensus around specific viewpoints. As algorithms gain prominence in managing online information, private actors – digital platforms and internet service providers – have gradually assumed functions traditionally held by public authorities. In this context, the algocracy reaches its full expression in the infrastructural power of platforms that shape the digital environments where knowledge is produced and circulated, performing a quasi-normative role that deeply influences rights and democratic deliberation. This underscores the need for a flexible, multi-stakeholder regulatory framework in which self-regulation complements public oversight (Faini, 2019, p. 411; Stradella, 2020, p. 80), ensuring that decisions of general interest are subject to political deliberation and the realization of democratic values.

2. The challenges of surveillance capitalism for democratic systems

The growing concentration of knowledge, driven by the supranational dimension of the Web and by a regulatory framework that remains largely reactive to digital transformation (Faini, 2022), threatens substantive equality (De Minico, 2019, p. 113). At the same time, public authorities' use of private digital data further risks enabling mass surveillance systems through partnerships with major technology companies (Faini, 2019, pp. 183–187), undermining the openness of democratic societies (Hayes, 2012, pp. 167–175). Meanwhile, the increasing privatization of the Web has consolidated the power of a few 'landowners of knowledge' (Orefice, 2018,

p. 158), laying the foundations for 'surveillance capitalism' (Zuboff, 2019), which produces 'equivalence without equality' (Zuboff, 2019, p. 394) and reduces individual freedom to the lowest common denominator of the virtual market. This allows a pervasive economic logic that goes so far as to predict and modify individual actions, including political and electoral behaviour, altering the most basic democratic principles and the meaning of popular sovereignty (Barberis, 2020; O'Neil, 2017; Zuboff, 2019).

This phenomenon supports the algorithmic selection of online content based on previously expressed preferences, and represents a threat to democracy by reducing meaningful discussion in the public sphere, fostering polarization, making individuals more vulnerable to censorship, propaganda or even self-propaganda (Pariser, 2011; Sunstein, 2017) and fuelling the rise of populism (Habermas, 2017). In this way, 'microtargeting' weakens the democratic process and the rule of law (Han, 2023, p. 27), 'because voters are not educated on a party's political program. Instead, they are shown manipulative advertising and not infrequently fake news tailored to their psychodrama' (Han, 2023, p. 28). This refers to an interpretation of reality to which the virality of its dissemination lends the qualification of authenticity (Ziccardi, 2019, p. 52). The emergence of multiple 'filter bubbles' (Pariser, 2011) illustrates how algorithmic recommendation systems tend to confine users within cultural and ideological boundaries, exposing them mainly to content that reinforces their pre-existing beliefs and producing increasingly personalized outputs. By restricting exposure to diverse viewpoints, filter bubbles also risk diminishing creativity, intuition and learning, while weakening social capital (Pariser, 2011) and ultimately eroding the potential of a pluralist public sphere. In this sense, they foster self-referential communication that blurs the line between the private and public domains, giving rise to competition among semi-public spaces (Habermas, 2023, pp. 61–67).

These dynamics are also reflected in the notion of echo chambers (Sunstein, 2017), where individuals tend to seek political information consistent with their own views and engage primarily with like-minded people (Han, 2023, pp. 43–45). Such mechanisms undermine public deliberation and civil debate (Sunstein, 2017), while revealing the growing asymmetry of knowledge between information producers and users (Casonato, 2019a, pp. 714–715). As a result, already shared information gains even greater visibility, despite the digital realm's vast potential to disseminate diverse data and news. At the same time, users risk being absorbed into 'digital swarms' (Baumann, 2010, p. 97) that amplify herd-effect behaviours (Ziccardi, 2019, p. 217). Thus, critically reflecting on algocratic power and on the identification of the responsibility of the political system to prevent these phenomena, significant questions about freedom of expression, pluralism and informational fairness emerge, placing algorithms, in their function as content filters capable of nurturing crystallized thinking that limits personal and collective choice (Zambonelli, 2020, pp. 118–121) at the centre of the

discussion, in opposition to the rational justification of democratic decisions (Habermas, 2002, pp. 33–35; 2023, pp. 65–69).

3. The right of freedom of expression on the Web

3.1. The American normative and judicial approach

The concentration of technological and informational power in the hands of major platforms has turned algocracy, which Danaher (2016) sees as a 'threat' toward democratic systems, into one of the most pervasive forms of digital governance, compelling a serious consideration of how different legal systems respond to these dynamics. Since algorithmic power acts as a new form of private regulation over collective experience, the legal response inevitably mirrors each system's conception of freedom, responsibility and rights protection. In this sense, the European and US approaches, though both aware of the political and social impact of digital platforms, rest on distinct cultural and philosophical foundations, leading to divergent ways of balancing technological innovation with democratic safeguards.

The United States' legal and judicial approach to online information emphasizes freedom of expression and limited legal liability for digital platforms. In the US, the legal approach to online information in fact rests on two basic pillars: the First Amendment to the Constitution and Section 230 of the Communications Decency Act, the first rule introduced by Congress, in 1996, to regulate the role of internet service providers. These regulatory instruments have shaped a digital environment characterized by considerable freedom of expression and a distinctive role for online platforms, which enjoy very limited legal liability: indeed, the First Amendment very broadly protects freedom of speech and of the press and has been interpreted by case law as also applying to online expression. This means that, in general, the state cannot censor or restrict content published on the Web unless it falls into very narrow categories, such as incitement to violence or defamation, and up to the point of bordering on hypotheses of child pornography. This protection has fostered the development of an open and pluralistic digital environment, although not without problems related to the circulation of disinformation or hate content. Rounding out the picture is Section 230 of the Communications Decency Act, a provision with a crucial impact on the way the internet has developed which states that interactive online service providers are not to be held liable for user-generated content. In addition to this type of immunity, Section 230 also grants platforms the right to freely moderate content, filtering or removing it, without losing their legal protection, thus becoming true players in the information mediation process. In fact, although originally conceived as neutral intermediaries, platforms actually operate by their own criteria in the selection, promotion or removal of content, often through opaque algorithms and internal policies that are not always clear and effective, with a profound impact

on public opinion and the visibility of content. Consequently, in recent years the role of platforms has been in the centre of lively political debate, starting from Section 230, in the assessment of whether these digital actors, which are private in nature, can implement content moderation choices that are not allowed to public authorities, which are directly bound by the First Amendment (Bassini, 2019, pp. 49–52). On this point, on the one hand conservatives accuse platforms of restricting freedom of expression, especially regarding content that is right-wing or contrary to mainstream culture; on the other, progressives criticize the lack of control over harmful content, such as health misinformation or hate speech. In this conflict of positions, both sides have raised the issue of possible reform of Section 230, but so far no concrete proposal has been able to take firm hold.

In American juridical decisions, there are some significant rulings; in this regard, a landmark case is *Trump v. Twitter*, in which the (then-former) US president was banned from the platform after the assault by some of his supporters on Capitol Hill on 6 January 2021. The case reignited the debate over the power of platforms to silence even prominent political figures, and highlighted how private regulation of content can conflict with the public perception of free speech (Judgment of the US Supreme Court, 2022). Another significant judgment is *Gonzalez v. Google*, considered by the US Supreme Court in 2023: in this case, family members of a victim of a terrorist attack accused YouTube, owned by Google, of 'amplifying' radical content through its algorithms. The case raised profound questions about the degree to which platforms are responsible not only for what they host, but for how they convey information; since the Court avoided a ruling that would fundamentally change the legal framework, the debate remains open (Judgment of the US Supreme Court, 2023; Fabiano, 2024, p. 98).

Very interesting, since it presents elements of distance from previous rulings, is the judgment of the Supreme Court in *Moody, Attorney General of Florida, et al. v. Netchoice, LLC, DBA Netchoice, et al.* (Judgment of the US Supreme Court, 2024) on the freedom of expression and guarantees offered by the First Amendment, a ruling that considers not so much, as previously, aspects of the non-responsibility of digital platforms, but rather their activity of moderating content which may fall within the free manifestation of thought (Fabiano, 2024, p. 89). This decision in fact represents the first case in which content moderation is seen as a right of the managers of online platforms, based on the guarantee of the First Amendment (Bassini et al., 2024; Mantovani, 2024). From this very recent perspective that examines the activity of content moderation, therefore, the focus is shifted from the guarantee for private subjects from possible government interference to considering any limitations of thought that can be carried out by other private subjects (Fabiano, 2024, p. 90). Therefore, in this specific case, the Opinion of the Court on the merits concerns the freedom of expression of the manager of the digital platform, and refers to the state laws of Texas and Florida which, in addition to providing limits to the activity of content moderation,

also required that the provider had justified its decisions for content censorship. The Opinion of the Court – taking into account that the lower courts had not correctly carried out the social challenge control, that is, they had correctly evaluated the contested regulation in all its possible implications, considering instead only the position of the major providers (Fabiano, 2024, pp. 103–104) – therefore highlighted how the government cannot interfere in the expression of private thought, since the purpose of Section 230 is the protection of freedom of thought from public influence (Fabiano, 2024, p. 95). In this way, the Supreme Court decision of 1 July 2024 could be a first step toward ever-increasing freedom of expression on social networks; all the positive aspects of this must be considered, but so also must be the critical issues represented by the possible manipulation and conditioning of collective thought, which on this point increases the already notable distance from the European approach to these issues (Fabiano, 2023; Fabiano, 2024, p. 100; Pollicino, 2023).

Overall, the US legal approach has fostered an online ecosystem strongly oriented toward freedom of expression and technological innovation, but it has left large 'grey areas' regarding the accountability of digital platforms, a principle carefully considered instead by both the 2018 European General Data Protection Regulation (GDPR, 2016, Art. 24) and the Digital Services Act (DSA, 2022, Arts. 4–20). The American perspective to date does not seem to consider the gradual transformation of the role of online platforms from mere infrastructure providers into powerful information brokers, raising urgent questions about the future of internet regulation, digital democracy and the balance between freedom and responsibility. While this approach has fostered an open, dynamic and innovative internet, it has also contributed to the spread of disinformation, online hate speech and extreme content, with minimal regulatory intervention by the state.

3.2. The European regulatory and jurisprudential approach

The European context detaches itself from the American approach, being characterized by constitutional provisions aimed at broadly, but not absolutely, protecting the freedom of manifestation of thought (Abbondante, 2017, pp. 56–59). This principle, is in fact, balanced with other values and rights of equal importance, such as human dignity, the right to identity and personal image, privacy and personal data protection. Second, even in the first European regulatory orientation, the online service provider, as of the dictate of the now-dated E-Commerce Directive no. 31/2000, the online service provider is under no obligation to monitor or check in advance the content of posts and comments entered by users, or to actively search for facts or circumstances indicating illegal activities, except where the provider takes an active role in conveying the information; this latter aspect outlines the distinction between content moderation activities, the figures of a mere transmission provider, cache provider and host provider, and the related legal responsibility (Directive 2000/31/EC, Arts. 12–14). This approach is outlined in the famous *Google Spain* judgment (Judg-

ment of the CJEU, 2014), where the CJEU held that a search engine operator acts as a 'controller' of personal data when indexing third-party web pages, recognized its active role in affecting fundamental rights and confirmed its responsibility to evaluate and, where appropriate, remove links upon delisting requests.

The gradual expansion of the functions of online service providers over the years, in some cases to trace attitudes proper to public authorities (Bassini, 2019, p. 55), has, however, prompted an increasingly broad interpretation of the role and responsibilities referable to such entities. Even the European Union has developed a direction aimed at increasing the accountability of online providers beyond the provisions of Directive 2000/31/EC, as witnessed by the EU Commission's 2017 Guidelines about the obligation to monitor information transmitted or stored by online service providers. This increases the providers' aggravating their burden by enshrining the principles of 'take-down', imposed by the need for Member States to provide detailed regulation of the process leading to the effective and timely removal of illicit content, and 'stay-down', preventing the reappearance of illicit content similar to that already subject to take-down.

In the regulatory field, the European Union is also moving in a different direction, aiming to balance freedom of expression with the protection of human dignity, the rights of consumers and democracy. In fact, for greater protection of the delicate balance between freedom of expression and the guarantee of the correctness of online information, the European Union has in recent years introduced several key pieces of legislation: here, it is worth mentioning the GDPR, which establishes protective rights for users over their personal data and imposes stringent obligations on digital platforms on transparency, individual consent and the processing of user data. Also relevant is the 2023 Digital Markets Act, which regulates online information 'gatekeepers' in order to prevent anticompetitive practices, including restrictions on combining personal data from different sources, a set of obligations to allow users to install applications from third-party platforms, prohibitions on bundling services, and a prohibition on promoting one's own services under certain conditions, which, in this case, cannot be offered in a more favourable way in rankings. Furthermore, the Data Governance Act encourages the reuse of some public data and the creation in the European marketplace of a data-sharing space.

A particular mention should also be made of the 2022 Digital Services Act, which came into effect in 2024, inspired by the principle that 'what is unlawful *offline* must also be unlawful *online*' (Council of the European Union, 2021) and introducing rigorous accountability obligations for digital platforms, primarily for very large online platforms. To tackle illegal content and online misinformation, the Digital Services Act establishes clear obligations for digital service providers, proportional to the size and risks of the platforms. These include measures to quickly counter illegal content while respecting fundamental rights such as freedom of expression and data protection (Arts. 12–14, 17–19). Marketplaces must enhance the tracking and monitoring

of traders to ensure product safety and must conduct random checks to prevent the reappearance of illegal content (Arts. 22–25). The Act also prohibits deceptive practices, including 'dark patterns' designed to manipulate users' choices, and restricts certain forms of targeted advertising, such as those aimed at minors or based on sensitive data (Arts. 24, 27). Very large online platforms and search engines – defined as those with at least 45 million monthly users – face additional obligations imposed by the Commission to prevent systemic risks, including the spread of illegal content, impacts on fundamental rights, interference in electoral processes, gender-based violence and mental health issues, and must undergo independent audits (Arts. 26–34). Furthermore, platforms must provide users with the option to opt out of algorithmic recommendations based on profiling and allow authorized authorities and researchers access to the platform's data and algorithms, while avoiding anticompetitive practices (Arts. 29–31, 33–34). As can be noticed, the DSA calls for the transparency, as far as possible, of algorithms, effective content moderation procedures and the introduction of systems for the rapid removal of illegal content, promoting systemic risk assessment with reference to disinformation, online violence and the protection of minors.

Measures such as the DSA or GDPR are particularly interesting in this field of study because they can foster significant regulatory influence. While the DSA regulates platform governance within the EU, its implications also connect to the broader 'Brussels effect' (Bradford, 2020), through which EU rules shape global practices as multinational companies adapt to European requirements to access the EU market. Although this dynamic traditionally underscores the contrast between the EU's rights-based model and the more market-driven US approach, it also fosters convergence, as firms often adopt EU-compliant practices globally, contributing to greater alignment between European and US frameworks.

Some interesting aspects can also be pointed out on the jurisprudential level, such as the 2019 *Glawischnig-Piesczek v. Facebook Ireland* ruling, regarding a liability case for defamatory content, specifically concerning an Austrian policy that had called for the removal of offensive content posted on Facebook. In this regard, the CJEU ruled that a platform can be obliged to remove or block offending content, even equivalent or identical content, globally, clearly increasing the liability of platforms in dealing with defamatory content (Judgment of the CJEU, 2019). The role of platforms in the sharing of copyrighted content was also addressed by the ruling in *YouTube and Cyando*, which concerns certain cases related to the unauthorized sharing of copyrighted material on YouTube and Uploaded. In this regard, the CJEU ruled that platforms are not automatically liable, but they may be liable if they do not act quickly after reporting, with the reinforcement of the concept of liability contingent on knowledge and inaction (Judgment of the CJEU, 2011). Finally, on the problematic relationship between data protection and market competition, mention should be made of the *Meta Platforms Ireland v. Bundeskartellamt* ruling of 2023, which fol-

lowed the German competition authority's challenge to Meta's use of data collected without explicit consent: the CJEU has, therefore, confirmed that antitrust authority can intervene in privacy issues, thereby enhancing consumer protection on multiple fronts, such as privacy, competition and transparency (Judgment of the CJEU, 2023). As can be seen, in the European approach, major online platforms can no longer operate as neutral subjects but are considered actors with specific powers and responsibilities, and have to ensure a secure and transparent digital environment that complies with fundamental rights.

Conclusions

The issue of freedom of expression in the digital world cannot be confined to commercial considerations, as it involves the delicate balance between freedom and responsibility, the role of AI, concrete expressions of freedom of thought and the serious risk of thought manipulation by digital tools (Fabiano, 2024, p. 107; Manganelli, 2023), which have the potential to influence the democratic stability of state of law (Fabiano, 2024, p. 101). Consequently, in the absence of spatial boundaries that can frame virtual interactions, it becomes essential to harmonize diverse world views and their corresponding regulatory frameworks concerning the role and responsibilities of major online operators, while ensuring that technology remains anchored to the universal dimension of fundamental rights (Rodotà, 2014, pp. 58–59). In this regard, cooperation between the EU and the United States could be grounded in a mix of regulatory instruments, shared standards, institutional dialogue and joint research initiatives, capable of reconciling the European vision, centred on individual rights and the protection of the public interest, with the US approach, more focused on market dynamics and innovation.

As algorithms must reflect human values and ethical principles, even at the cost of efficiency (O'Neil, 2017, pp. 294–299), it becomes essential to adopt an approach that is 'ethical by design' and that incorporates fairness, transparency and accountability throughout the entire development process. This means using representative data, creating explainable and modular systems and ensuring human oversight through specific checkpoints. These efforts must be supported by auditing mechanisms, the traceability of decisions, and tools to remedy unfair outcomes, alongside active user and public participation to align technologies with shared social values. Ultimately, ensuring that algorithms operate in line with fundamental rights and the public good requires the integration of ethics, technology and governance, while the promotion of digital literacy and lifelong learning is essential to cultivate awareness and responsibility in the face of potential algorithmic threats to democracy.

REFERENCES

Abbondante, F. (2017). Il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea. *Informatica e diritto*, *43*(1/2), 41–68.

Amato Mangiameli, A. C. (2019). Algoritmi e big data. Dalla carta sulla robotica. *Rivista di filosofia del diritto/ Journal of Legal Philosophy*, *8*(1), 107–124.

Amato Mangiameli, A. C., & Campagnoli, M. N. (2020). *Strategie digitali. #diritto_educazione_tecnologie*. Giappichelli.

Aneesh, A. (2006). *Virtual migration: The programming of globalization*. Duke University Press.

Aneesh, A. (2009). Global labor: Algocratic modes of organization. *Sociological Theory*, *27*(4), 347–370.

Barberis, M. (2020). *Come internet sta uccidendo la democrazia. Populismo digitale*. Chiarelettere.

Bassini, M. (2019). La cassazione e il simulacro del provider attivo: Mala tempora currunt. *MediaLaws – Rivista di Diritto dei Media*, *2*, 248–257.

Bassini, M., Finocchiaro, G., & Pollicino, O. (2024, 7 October). Il 1 emendamento USA tutela le piattaforme e dà loro un ruolo editoriale. *Il Sole 24 Ore*. https://www.ilsole24ore.com/art/il-primo-emendamento-usa-tutela-piattaforme-e-da-loro-ruolo-editoriale-AFmB0MiC

Baumann, Z. (2010). *Consumo, dunque sono*. Laterza.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Casadei, T., & Pietropaoli, S. (2021). *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali, sfide sociali*. Wolters Kluwer.

Casonato, C. (2019a). Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro. *BioLaw Journal/ Rivista di BioDiritto*, *25*, 711–724.

Casonato, C. (2019b). Potenzialità e sfide dell'intelligenza artificiale. *BioLaw Journal/Rivista di BioDiritto*, *1*, 177–182.

Council of the European Union, What is illegal offline should be illegal online: Council agrees position on the Digital Services Act, 25 November 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/

Danaher, J. (2016). The threat of algocracy: Reality, resistance and accommodation. *Philosophy & Technology*, *29*, 245–268.

De Minico, G. (2019). Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria. *Politica del diritto*, *1*, 89–115.

De Tullio, M. F. (2016). La privacy e i big data verso una dimensione costituzionale collettiva. *Politica del diritto*, *4*, 637–696.

Durante, M. (2019). *Potere computazionale. L'impatto delle ICT su diritto, società, sapere*. Meltemi.

European Parliament and Council. (2000). Directive 2000 no. 31 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market. https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng

European Parliament and Council. (2022, 14 September). Regulation 2022/1925 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937

and (EU) 2020/1828 (Digital Markets Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925

European Parliament and Council. (2022, 19 October). Regulation 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

Fabiano, L. (2023). Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati. *Diritto dell'informazione e dell'informatica*, *4–5*, 597–643.

Fabiano, L. (2024). Content moderation e free speech clause: il controverso rapporto fra libertà e responsabilità delle piattaforme digitali nella più recente giurisprudenza della Corte suprema federale USA. *Federalismi. Rivista di Diritto Pubblico, Italiano, Comparato, Europeo*, *27*, 88–107.

Faini, F. (2019). *Data society. Governo dei dati e tutela dei diritti nell'era digitale*. Giuffrè.

Faini, F. (2022, 8 June). *Principi etici e giuridici per la tecnologia*. Media2000. https://www.media2000.it/fernanda-faini-giurista-digitale-principi-etici-e-giuridici-per-la-tecnologia/

Floridi, L. (2012). *La rivoluzione dell'informazione*. Codice.

Floridi, L. (2017). *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*. Raffaello Cortina.

Foucault, M. (1975). *Sorvegliare e punire. Nascita della prigione*. Einaudi.

Habermas, J. (2002). *Il futuro della natura umana. I rischi di una genetica liberale*. Einaudi.

Habermas, J. (2017). La risposta democratica al populismo di destra. *Micromega*, *2*, 4–24.

Habermas, J. (2023). *Nuovo mutamento della sfera pubblica e politica deliberativa*. Raffaello Cortina.

Han, B.-C. (2022). *Le non-cose. Come abbiamo smesso di vivere il reale*. Einaudi.

Han, B.-C. (2023). Infocrazia. Le nostre vite manipolate dalla rete. Giulio Einaudi Editore.

Hayes, B. (2012). The surveillance-industrial complex. In *Routledge handbook of surveillance studies* (pp. 167–175). Routledge.

Jasanoff, S. (2004). *States of knowledge: The co-production of science and the social order*. Routledge.

Judgment of the CJEU of 13 May 2014 on the case of *Google Spain, S. L., Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González*. https://op.europa.eu/en/publication-detail/-/publication/1df672d5–05b4–11e4–831f-01aa75ed71a1/language-en

Judgment of the CJEU of 3 October 2019 on the case of *Glawischnig Piesczek v. Facebook Ireland*. https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=49929

Judgment of the CJEU of 22 June 2021 on the case of *YouTube and Cyando*. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62018CJ0682

Judgment of the CJEU of 4 July 2023 on the case of *Meta Platforms Ireland v. Bundeskartellamt*. https://curia.europa.eu/juris/document/document.jsf;jsessionid=F3DD0CA874FF40844471F-2F6AC22FD50?text=&docid=275125&pageIndex=0&doclang=IT&mode=req&dir=&occ=-first&part=1&cid=97875

Judgment of the US Supreme Court of 5 June 2022 on the case of *Trump v. Twitter.* https://www.govinfo.gov/app/details/USCOURTS-cand-3_21-cv-08378/context

Judgment of the US Supreme Court of 18 May 2023 on the case of *Gonzalez v. Google* no. 21–1333. https://www.supremecourt.gov/opinions/22pdf/21–1333_6j7a.pdf

Judgment of the US Supreme Court of 1 July 2024 on the case of *Moody, Attorney General of Florida, et al. v. Netchoice, LLC, DBA Netchoice, et al.*, no. 22–277. https://www.supremecourt.gov/opinions/23pdf/22–277_d18f.pdf

Latour, B. (1988). The politics of explanation: An alternative. In S. Woolgar (Ed.), *Knowledge and reflexivity: New frontiers in the sociology of knowledge* (pp. 155–176). Sage.

Manganelli, A. (2023). Piattaforme digitali e social network fra pluralità degli ordinamenti, pluralismo informatico e potere di mercato. *Giurisprudenza Costituzionale*, *2*, 883–904.

Mantovani, E. (2024, 18 July). Piattaforme digitali: l'attività di selezione dei contenuti è protected speech. La Corte Suprema USA limita gli interventi di regolazione statale nel settore digitale. *Diritti Comparati*. https://www.dirittocomparati.it/piattaforme-digitali-lattivita-di-selezione-dei-contenuti-e-protected-speech-la-corte-suprema-usa-limita-gli-interventi-di-regolazione-statale-nel-settore-digitale/

Monti, M. (2019, 15 October). *La corte di giustizia, la direttiva e-commerce e il controllo contenutistico online: le implicazioni della decisione C 18–18 sul discorso pubblico online e sul ruolo di Facebook*. MediaLaws. https://www.medialaws.eu/la-corte-di-giustizia-la-direttiva-e-commerce-e-il-controllo-contenutistico-online-le-implicazioni-della-decisione-c-18–18-sul-discorso-pubblico-online-e-sul-ruolo-di-facebook/

O'Neil, C. (2017). *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia*. Bompiani.

Orefice, M. (2018). *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*. Aracne.

Orrù, E. (2021). Verso un nuovo Panottico? La sorveglianza digitale. In T. Casadei & S. Pietropaoli (Eds.), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali, sfide sociali* (pp. 203–216). Wolters Kluwer.

Palazzani, L. (2020). *Tecnologie dell'informazione e intelligenza artificiale*. Studium.

Pariser, E. (2011). *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin.

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

Perri, P. (2020). *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*. Giuffrè.

Pollicino, O. (2023). Di cosa parliamo quando parliamo di costituzionalismo digitale? *Quaderni costituzionali*, *3*, 569–594.

Rifkin, J. (2001). *L'era dell'accesso. La rivoluzione della new economy*. Mondadori.

Rodotà, S. (2012). *Il diritto di avere diritti*. Laterza.

Rodotà, S. (2014). *Il mondo nella rete: quali i diritti, quali i vincoli*. Laterza.

Sartor, G. (2022). *L'informatica giuridica e le tecnologie dell'informazione*. Giappichelli.

Stradella, E. (2020). Stereotipi e discriminazioni: dall'intelligenza umana all'intelligenza artificiale. *Consulta Online*, 1–10. https://giurcost.org/contents/giurcost//LIBERAMICORUM/stradella_scrittiCostanzo.pdf

Sunstein, C. R. (2017). *#republic: Divided democracy in the age of social media*. Princeton University Press.

Talia, D. (2018). *La società calcolabile e i big data. Algoritmi e persone nel mondo digitale*. Feltrinelli.

Thurman, N. (2011). Making 'The daily me': Technology, economics and habit in the mainstream assimilation of personalized news. *Journalism: Theory, Practice & Criticism*, *12*(4), 395–415.

Thurman, N., & Schifferes, S. (2012). The future of personalization at news websites: Lessons from a longitudinal study. *Journalism Studies*, *13*(5–6), 775–790.

Zambonelli, F. (2020). *Algocrazia. Il governo degli algoritmi e dell'intelligenza artificiale*. Scienza Express.

Ziccardi, G. (2019). *Tecnologie per il potere. Come usare i social network in politica*. Raffaello Cortina.

Zuboff, S. (2019). *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*. Luiss University Press.