

# Regulating Artificial Intelligence – Balancing Between Protecting Citizens Privacy and Fostering the Industry’s Growth in Europe

Ștefan-Marian Dumitru<sup>1</sup>

<sup>1)</sup> *Bucharest University of Economic Studies, Bucharest, Romania*  
E-mail: stefan.dumitru91@gmail.com

---

**Please cite this paper as:**

Dumitru, S.M., 2023. Regulating Artificial Intelligence - Balancing Between Protecting Citizens Privacy and Fostering the Industry’s Growth in Europe. In: R. Pamfilie, V. Dinu, C. Vasiliu, D. Pleșea, L. Tăchiciu eds. 2023. *9<sup>th</sup> BASIQ International Conference on New Trends in Sustainable Business and Consumption*. Constanța, Romania, 8-10 June 2023. Bucharest: ASE, pp. 385-391

DOI: [10.24818/BASIQ/2023/09/054](https://doi.org/10.24818/BASIQ/2023/09/054)

---

**Abstract**

The digitization of daily life has entered all areas in which humans activate, be it work, entertainment, social environments, or other areas of interest. The political environment has not been omitted, especially due to social media platforms. As it currently stands, social media has been playing for a number of years a significant role in disseminating and accelerating social debates, bringing to the surface latent issues as well as propagating voices which otherwise might represent the fringe opinions of small groups. In this context, research has been ongoing to understand the nuanced way in which it has impacted society, as a perpetrator of disinformation, and the impact it has had on European regulations by increasing the protection of data and privacy, after the entry into force of EU Regulation 679/2016. Thus, the objective of this article is to offer a legal and ethical framework for the utilization of artificial intelligence in Europe. The study utilized a systemic research method to look into the intricate and interconnected issues involved in regulating social media platforms, identifying key themes and patterns that emerged from the data, which were then utilized to create recommendations for the regulation of social media platforms, that can be utilized by researchers and policy makers.

**Keywords**

EU regulations, social media, privacy, digital identity.

DOI: [10.24818/BASIQ/2023/09/054](https://doi.org/10.24818/BASIQ/2023/09/054)

---

**Introduction**

The rapid and widespread changes brought about by technology and social media have raised numerous questions about their impact on society. Many believe that these changes have created a crisis that affects every aspect of our lives (McGuire, 2017). Understanding this complex phenomenon is challenging but necessary. With the establishment of a continuous link between online and offline dimensions, citizens express their opinions and feelings in a social climate that is becoming increasingly personalized and multidimensional. Before the internet, social identity and networking were constrained by spatial and temporal limitations. However, the internet has expanded the boundaries of social networks, creating a new world in which to socialize, cyberspace. Cyberspace offers the medium through which individuals interact, in the familiar system of social networks combined with multimedia, content creation, and sharing features of the web. Social networks are now the meeting point for using digital media in various ways, including supporting social networks and expressing one's social identity while analyzing other network members' social identities (Boccia Artieri and Marinelli, 2018). This raises questions about the relational and communicative scope of social networks in the ongoing digitization process. How do social media platforms influence the building and molding of the user's identity, especially for users that are very young? What effects do they have in terms of opportunities and risks?

This study also examines the European legislature and community jurisprudence's reaction to this issue, indicating the required reforms which would be targeted at safeguarding citizens and their private environment. It is important to consider the role of social media platforms in the construction of an

individual's identity and their impact on society. We will also look at the European legislature and community jurisprudence's response to these issues and suggest necessary reforms to protect individuals and their privacy.

### **Review of the scientific literature**

Digital media has become very important for people to socialize, connect with others, and even take part in new forms of activism (García-Peñalvo, 2016). This can help people to overcome challenges in collective participation, especially during times of crisis. However, there are problems with the shift from an information society to a seduction society, which has been highlighted by the COVID-19 pandemic. Despite this, modern society is heavily influenced by technological and digital innovation, which has led to a debate on how networks affect almost all aspects of our lives. Some people think technology has a mystical power and view it too simply (Landini, 2017). Evgeny Morozov (2015) has identified "Internet-centrism" and "solutionism" as two problematic views that neglect important social and political factors. Thus, we need to address technological change discussions by recognizing that technology is not always the solution to real-world problems. While we can appreciate the benefits of being interconnected, there are also new risks and uncertainties emerging. This means that we don't have a clear direction towards a desired goal when it comes to technology. The boundary between our online and offline lives is now blurry and subtle, and this hybrid practice is called Onlife. It's like the mangrove's environment, which lives in brackish waters where seas and rivers meet. According to Floridi, we are now in an existence where there is no longer a difference between online and offline, but there is an Online, which is as hybrid as the mangrove habitat. In this context, we face a semantic reversal where information now influences technology, unlike in previous technological evolutions. Our lives are becoming increasingly personal and managing a multilateral dimension where we live both online and offline. This case study aims to trace new ridges of study in this context. Digitalization has posed questions that are not purely technological but must be contextualized within socio-historical processes. This article aims to demonstrate that we have reached a point of no return. Within the sociology of the media, it is possible to identify three main paradigms to analyze the forms that society and individuals' relations with communication take in the digital turn, but this research will not do so. Thus, it is evident that social media has such a significant impact on society and individuals that it now affects every aspect of public and private life. This phenomenon must be addressed by legal practitioners who need to study and analyze its impact on legal situations and relationships. Recently, it has been argued that technology and its evolution have radically transformed social relations and the daily lives of individuals, including the area of inheritance. This transformation affects not only the course of an individual's life but also the way in which their personality can be realized after their passing. Social networks on the web become a social space where individuals exercise fundamental rights such as free expression of thought or economic initiative. It is an authentic society where each person builds their digital identity based on their profile, including personal data, political and sexual orientation, friendship networks, interests, business preferences, images, and various types of information.

The utilization of social media has benefits, but it also comes with risks to the user's identity and personal data. Social media platforms rely on collecting and managing personal information, and regulations are mostly defined by agreements between users and the platforms (Martone, 2020). To understand the impact of social media on individuals, it's important to examine the concept of digital identity, which is the online representation of a person or entity that includes identifying information. In the past, identity was only physical, but now digital identity is composed of a mass of data that partly reflects and partly distorts an individual's real identity. Digital identity is crucial for accessing the digital community and for identifying oneself within social networks. When users sign up for social media, they create a profile that represents their identity and agrees to the platform's terms and conditions, including the privacy policy that lists how data will be processed. Since social media regulations are often removed from national legal systems, protecting individuals' identity, privacy, and data circulation has become more complex (Martone, 2020). Nevertheless, legal practitioners and the European legislator have recognized the importance of these issues and introduced rules to protect individuals. With the evolution of technology, personal identity has changed, affecting privacy and confidentiality, which are closely tied to it.

### **Research methodology**

The research in this study aims to delve into the intricate and interrelated problems related to the regulation of social media platforms. The study considers the importance of striking a balance between protecting the fundamental rights of individuals and accommodating the interests of economic operators while ensuring the privacy and security of users. To achieve this delicate balance, the study proposes a multifaceted

approach that involves legal, educational, and technological measures. Thus, employing a systemic research method, the study involves investigating the complex and interrelated issues surrounding the regulation of social media platforms. Delving into a vast collection of existing literature on social media regulation to identify the main issues and arguments being discussed. Thus, key themes and patterns emerged from the data, that were used to develop recommendations for regulating social media platforms. The study highlights the importance of clear and informed consent, transparency in data usage, and collaboration between social media platforms and public authorities to guarantee user privacy and security. Overall, the research method is comprehensive and multi-dimensional, acknowledging the complexity of the issue and utilizing various methods of data collection and analysis to gain a better understanding of different perspectives and issues involved. The recommendations for regulating social media platforms are carefully considered to balance the needs of users, the interests of platforms, and the control of authorities.

### Results and discussion

The amount of personal data being shared and collected has grown rapidly, as people themselves publish their own information. This has raised concerns among jurists about the need for protection and the methods of protection. One consequence of this trend is the increased risk of the telematic information system being used for social control through sophisticated forms of cybercrime. The evolution of cyber security threats over the past 25 years has been significant. The maturity of social media has made it more difficult to combat cybercrime, as it has led to a fundamental shift in criminal behavior and organizational logic from offline organized crime.

Looking at the evolution of the concept of privacy, it's interesting to see how it has changed from just protecting the personal and intimate aspects of an individual, to also encompassing the right to control and dominate the circulation of personal data (Wall, 2015). There is a need to investigate whether the right to access social media and the right to privacy when it comes to the circulation of data on Web 2.0 are compatible, and whether legislative interventions so far have been able to strike a balance and suggest a functional reform perspective for the multiple interests in the field. In 1995, the protection of personal data became part of European law with the approval of Directive 95/46/CE, which emphasizes the importance of respecting fundamental rights and freedoms, particularly privacy, while also contributing to economic and social progress and the well-being of individuals (Stanzione, 2020). There was a clear intent to create a regulation that would connect the demands of the free market and competition with human dignity and the development of personality. The Charter of Fundamental Rights of the European Union, adopted in 2000, emphasized everyone's right to the protection of personal data, as well as the right to access and correct data collected (EC, 1995). And with the Lisbon Treaty's entry into force, it was enshrined in the TFEU that the protection of private citizens date is guaranteed by the treaties, highlighting its importance for each individual. As Table 1 shows, the evolution of legislation on the matter has been an decades long endeavor.

Year	Event
1950	European Convention on Human Rights (ECHR), enshrines that citizens have a right for their private life to be respected, through Article 8.
1981	The Council of Europe adopts the most comprehensive document on the protection of personal data - Convention 108.
1995	The European Union implement legislation on the protection of personal data, via Directive 46/95.
2007	The Lisbon Treaty, via the TFEU, enshrines that personal data protection is a right of every citizen, giving legal competences to the Council and European Parliament to enact legislation.
2018	The European Union adopts the General Data Protection Regulation (GDPR) and enters into force.

*Source: European data protection supervisor, 2023*

It's evident that regulating social media platforms is critical to ensure fair use and protect the fundamental rights of citizens such as privacy and freedom of expression (Landau, 2013). This is especially important given the current reality, where social platforms are filled with numerous threats such as the dissemination of false information and hate speech. The European Parliament and Council have the legal power to regulate

these platforms. However, due to the fast-paced evolution of technology and the ubiquitous nature of social networks, the European legislator had to intervene to regulate and restrict the massive collection and sharing of personal data. Reforms are needed since the current Directive 95/46/EC has failed to prevent the fragmentation of personal data protection across the EU, eliminating legal uncertainties or the perception of risks associated with online operations. This is further compounded by the changing concepts of privacy and data protection due to the advancements in online services.

In 2016, a new European Regulation was issued to replace the previous directive on the processing of personal data. The regulation applies to all personal data processing, except for reasons of national or common security or criminal investigations. Personal data defines the information that can be used to aid in the identification of a natural person, whilst processing relates to any operation that can be performed with the utilization of said personal data (EC, 2016). This regulation aims to protect individual privacy and their personal sphere, as stated in Article 5. The article requires that processing is carried out legally, fairly, and transparently for rightful purposes, and utilizing legal methods that are in line with said purposes. Thus, legality implies compliance with the rules of the system as a whole, not just data protection laws. Fairness involves good faith in the utilization of data in line with ethical standards. Transparency guarantees that the subject which has his data utilized is aware of the processing, which is essential for giving informed consent. Consent is a vital element in the legislation that protects privacy and personal data, and it must be free, informed, specific, and unambiguous (EC, 2016).

The legislation and the way social networks are accessed reveal issues with the concept of consent. While the regulation defines consent, it fails to regulate it fully, leading to a broad interpretation of its application. Article 7(4) of the regulatory act creates confusion in regard to whether or not consent has been given freely, especially when online services and social networks make consent a condition of use. This consent also includes the processing of data not necessary for the provision of the service and its transmission to other companies, which have an interest in utilizing the data for commercial purposes. Such situations make the presumption that consent has not been freely given. The European legislator assumes that consent is not freely given if it is a non-negotiable part of the general terms and conditions of the service. Social networks make matters even more complex by not requiring specific consent for each individual processing (Popoli, 2019). To determine if consent has been given freely, without a shred of doubt, it requires proper and open access to information, which would mean it should enable access to the process by which information is managed, as well as a form of legal right on the data. However, the information provided by social networks does not provide such control.

Apart from the technical and legal complexities, there's another important factor to consider today's society heavily relies on the analysis of vast amounts of data, which has become a valuable asset (De Franceschi, 2019). Some people argue that personal data processing has shifted from protecting a fundamental right to commercializing data. Those who believe in the former see personal data as a part of a person's identity, and it should be processed correctly. On the other hand, those who believe in the latter consider data as a commodity with value, and it can be traded. As noted by Resta and Zeno-Zencovich, (2014), many service providers offer free services to users, which are financed by users' personal data, often used for advertising purposes. Some legal frameworks support the use of personal data for direct marketing purposes, but it requires the user's full and unforced consent. Such is the case of the Italian Court of Cassation, which undertook, in 2018, the task of analyzing how the trade of personal data is undertaken, concluding that personal data can be exchanged, but it should be with full consent (Cass, 2019). This debate continues, and there's a growing awareness among legal practitioners to limit the trade of personal data. The Court of Justice of the EU emphasizes the importance of protecting personal data, linking it to fundamental human rights (CJEU, 2003). However, despite the risks, users seem to care more about accessing services and enjoying their benefits than about the protection of their data.

As technology continues to rapidly evolve, it has become increasingly important to regulate social platforms to ensure their responsible and secure use for users (Gillespie, 2018). However, this regulation is a complex and constantly evolving topic, as it must consider ongoing processes. It is crucial that regulation is constantly updated to include new developments and improvements brought about by the advancements in new technologies. As an example, a current hot topic is the increasing advancement and use of machine learning, artificial intelligence and blockchain technology. As such systems have begun to be integrated in social media platforms, as a means of attracting and maintaining engagement by users, regulation should be adapted to limit the potential negative effects of these technologies. AI is augmenting the human experience, and with it our lives, and as such, it is crucial that society should be aware of the positive and negative effects on collective and individual ethics (Vallor, 2016). However, defining artificial intelligence is a difficult task and there are many different definitions. To address the challenges and opportunities offered by artificial intelligence, the European Union has been floating the idea of intervening and

regulating the use and limitations of AI, and with the advent of chatGPT, the debate has been spurred into overdrive, as countries such as Italy, decided in March of 2023 to impose a temporary ban on it. (Riegert, B. 2023). The purpose of the debate is to create regulation which would aid in the protection of the EU's sovereignty in digital matters, by utilizing legal tools and abilities to model global regulation in a set of norms and standards that would become a global influencer of norms.

The regulation that the EU proposes for AI attempts to implement several goals. First, it wants to guarantee that AI programs are secure and in compliance with the fundamental legislation of values and rights that the EU guarantees. Second, it wants to guarantee that a legal framework will give the necessary stability that will give companies the stability they desire to encourage them to innovate and invest in AI. For such a task to be achieved, it is imperative that advancements be made in the implementation of legislation and protection of citizens' rights and security. Third, the EU's want to encourage the development, under the rule of the single market's regulations, of AI that prevents market fragmentation and offers equal benefits for all citizens.

With the increased use of artificial intelligence, it is crucial that regulation is constantly updated to reflect the progress that technology has seen, incorporating the benefits and negatives of the new developments. The European Union's proposal for AI regulation aims to achieve several specific goals, developing AI under the legal framework of the single market and of the EU treaties. The aim is to prevent any dangers that may arise from the opacity, unpredictability, and autonomy of some AI systems (EC, 2021), while ensuring legal certainty to encourage investments and innovation in AI. A good reason for supporting the EU's intervention is that it would impose transparency and predictability on an otherwise opaque industry that might allow AI systems to advance more than they should. However, the intrinsic limit of the horizontal approach is that it be applicable to all sectors in which AI can be implemented, be they the financial sector or the health sector. Thus, comprehensive laws must be developed, to avoid ad-hoc solutions, and thus, apply to all AI systems, even those that have yet to be developed.

## Conclusions

This work has brought up several questions that haven't been completely answered yet. There have been some regulatory or jurisprudential interventions that have helped, but there are still legal issues to be addressed. We need to find a balance between protecting individual fundamental rights, such as privacy and freedom of expression, and the interests of economic operators who want to provide services and make profits. Users need to be more aware of the importance of their personal data, and we need broader and clearer legislative intervention to make sure that happens. One idea is to reform European laws on personal data protection when it comes to social platforms. We believe that data should have a purely moral function and should not be negotiated unless it's necessary to use a particular app or platform. There needs to be a new regulation to prevent social networks from limiting their available functions as a form of punishment towards users that opt out of sharing their information. Consent needs to be truly informed, and the disclosures should be clear and understandable to everyone. They should not be hidden in links or navigation windows. Consent must be outlined and defined clearly, so there's no room for interpretation.

There are other things to consider too. Education is important, and users need to be educated on issues related to privacy and online security to make informed decisions. Decentralization could be helpful, in the sense that groups of users are being managed, instead of a case-by-case scenario, thus ensuring a diminished reliance on algorithms and a boost in transparency in how user data is utilized. Social platforms must cooperate with public authorities in creating legislation that safeguards user privacy and security, instead of resisting such efforts, under the guise of diminished returns due to overregulation. As all social media platforms have a global outlook to their business and global reach, all of these actions would propagate the regulatory framework imposed by the EU, encouraging the positive creation of similar norms, across countries. In summary, regulating social platforms is a complex issue that requires deeper reflection equilibrium between the needs of users, the interests of platforms and the control of authorities.

The study presented an in-depth exploration of the complex and interrelated issues surrounding the regulation of social media platforms, providing a legal and ethical framework for the utilization of artificial intelligence in Europe. The findings of the study shed light on the importance of balancing individual fundamental rights with the interests of economic operators while ensuring user privacy and security are protected. The study proposes a multi-pronged approach, including legal, educational, and technological interventions, to address these issues and provide recommendations for regulating social media platforms. While the study offers valuable insights into this important topic, there are some limitations to be considered. The research primarily focuses on the European context, and additional research is needed to examine the regulatory frameworks of other regions. Furthermore, the study's conclusions are based on the

current state of technology and legislation, and these frameworks may change in the future. Therefore, ongoing research and updates to regulatory frameworks are essential to ensure that the recommendations remain relevant and effective.

## References

- Boccia Artieri, G. and Marinelli, A., 2018. *Introduction: Platforms, Algorithms, Formats. How Online Information Is Evolving*. *Problemi dell'Informazione. Rivista Quadrimestrale*, (3), pp.349–368. <https://doi.org/10.1445/91657>
- CASS Italy, 2019. *sez. Un., Sentenza Cassazione Civile n. 19681 del 22/07/2019, N. 19681*. [online] Available at: <<https://sentenze.laleggepertutti.it/sentenza/cassazione-civile-n-19681-del-22-07-2019>> [Accessed 15 April 2023].
- Court of Justice of the European Union, 2003. *Judgment May 20, 2003, Joined Cases C-465/00, C-138/01 and C-139/01*. [pdf] Available at: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CC0465>> [Accessed 15 April 2023].
- De Franceschi, A. (2019). *"Payment" through personal data in Personal Data in European Law*". Giappichelli. Turin, Italy.
- Riegert, B. 2023. *EU: ChatGPT spurs debate about AI regulation*. Deutsche Welle. Available at: <<https://www.dw.com/en/eu-chatgpt-spurs-debate-about-ai-regulation/a-65330099>> [Accessed 11 May 2023].
- European Commission, 2016. *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, EU Regulation No. 679/2016*. [online] Available at: <[https://www.eumonitor.eu/9353000/1/j4nkv6yhcbpeywk\\_j9vvik7m1c3gyxp/vk3t7p3lbczq](https://www.eumonitor.eu/9353000/1/j4nkv6yhcbpeywk_j9vvik7m1c3gyxp/vk3t7p3lbczq)> [Accessed 11 March 2023].
- European Commission, 2021. *Proposal for legislation with regards to Artificial Intelligence. Bruxelles, 21.4.2021, COM(2021) 206 Final 2021/0106(COD)*. [online] Available at: <[https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF)> [Accessed 11 March 2023].
- European Commission, 1995. *Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. [online] Available at: <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5>> [Accessed 11 April 2023].
- European data protection supervisor, 2023. *The History of the General Data Protection Regulation. Bruxelles*, [online] Available at: <[https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation\\_en](https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en)> [Accessed 11 May 2023].
- García-Peñalvo, F.J., 2016. La socialización como proceso clave en la gestión del conocimiento. *Education in the Knowledge Society (EKS)*, 17(2), pp.7–14. <https://doi.org/10.14201/eks2016172714>.
- Gillespie, T., 2018. Regulation of and by platforms. In: *The SAGE Handbook of Social Media*, SAGE, Newcastle upon Tyne, UK, pp. 254-278.
- Landau, S., 2013. Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *IEEE Security & Privacy*, 11(4), pp.54–63. <https://doi.org/10.1109/MSP.2013.90>.
- Landini, S., 2017. Digital identity between personal protection and intellectual property. *Rivista di diritto industrial*, 2017, pp.181-182.
- Martone, I., 2020. On the Transmissibility of Personal Data Due to Death: The Intricate Relationship between Digitalization and Confidentiality. In: *New Models of Succession Law: Internal, European and Comparative Perspectives*; EUT University Editions of Trieste: Trieste, Italy, 2020; p.87.
- Mazzamuto, S., 2019. The Principle of Consent and the Power of Revocation. In: *Free Movement and Protection of Personal Data*. Giuffrè: Milan, Italy, p.993.
- McGuire, M.R., 2017. Cons, Constructions Misconceptions of Computer Related Crime: From a Digital Syntax to a Social Semantics. *Journal of Qualitative Criminal Justice & Criminology*, 6(2). <https://doi.org/10.21428/88de04a1.505d151e>.
- Morozov, E., 2015. *The Internet will not save the world*. Milano, Italy: Mondadori.
- Mosco, V., 2004. *The digital sublime: myth, power, and cyberspace*. Cambridge, Mass: MIT Press.
- Popoli, A.R., 2019. The adaptation of Social Network Sites to GDPR: An Unfinished Path. In: *The Law of Information and Computer Science Journal*. Giuffrè Editore: Milan, Italy, pp.1298-1299.

- Resta, G. and Zeno-Zencovich, V., 2014. Will and Consent in the Use of Online Services. *Quarterly Journal of Civil Procedure Law*, pp.411-440.
- Stanzione, M.G., 2020. Freedom of expression and right to privacy in the dialogue of the courts. The vessel of the right to be forgotten. *Eur. Dirit. Priv.*, 3, pp.991–992.
- Vallor, S., 2016. *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780190498511.001.0001>.
- Wall, D.S., 2015. Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organised Crime*, 2(2), pp.71-90.