MYKOLAS ROMERIS UNIVERSITY
LAW SCHOOL
INSTITUTE OF PRIVATE LAW

CLÉA HYNEK
EU LAW AND GOVERNANCE

NEW TECHNOLOGIES AND FREEDOM OF EXPRESSION

Master thesis

Supervisor –
Prof. Dr
Lyra Jakulevičienė

Vilnius, 2025

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DMA	Digital Markets Act
DSA	Digital Services Act
ECtHR	European Court of Human Rights
ECHR	European Convention on Human Rights
EU	European Union
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technologies
IoT	Internet of Things
NICT / NTIC	New Information and Communication Technologies
OECD	Organisation for Economic Co-operation and Development
UDHR	Universal Declaration of Human Rights

INTRODUCTION[1]

Relevance - In a world in transition, technological networks are becoming increasingly complex, fast and powerful[2], sometimes surpassing our neural connections. Thus, freedom of expression, a fundamental pillar of any democracy, is facing unprecedented challenges. It becomes relevant and urgent to study the relationship between new technologies and freedom of expression.

In such a context, technical progress has given their inventors, the powerful private companies, an exponential influence on public debate and our freedoms[3]. It is not surprising that some of these actors, such as the CEO of Meta, Mark Zuckerberg, make new technologies tools to serve their ideas. Thus, in 2019, during a speech given at Georgetown University, he stated that: "Citizens who have the freedom to express themselves publicly constitute a new force of our world: a fifth power"[4]. By this, he justified his new refusal to check the political advertisements broadcast on his platform, even if they contained false information.

Is here illustrated, the way in which private companies divert the vocabulary of our fundamental rights to legitimize their practices[5]. In other words, behind the libertarian ideology he displays, hides a capitalist reality: speech becomes a commodity[6].

Moreover, while new technologies undeniably expand the public space of communication, they carry off drifts by becoming tools of manipulation, disinformation, surveillance and censorship[7].

---

[1] NB: In this thesis, the expression 'European law' will be used in a broad sense, encompassing both European Union law and law originating from the Council of Europe, notably the European Convention on Human Rights. When the analysis will focus specifically on one or the other of these two legal orders, reference will be made, as the case may be, to the "law of the European Union" or to the "law of the Council of Europe".

[2] Dominique Cardon, *À quoi rêvent les algorithmes ?*, (Paris : Seuil, 2015).

[3] Notably : Julie E.Cohen, *Between Truth and Power: The Legal Construction of Informational Capitalism* (New York: Oxford University Press, 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019), ISBN: 9781610395694.

[4] Mark Zuckerberg, speech at Georgetown University, 17 October 2019, transcript in *"Mark Zuckerberg Stands for Voice and Free Expression," Meta, 2019.*

[5] Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven: Yale University Press, 2018).

[6] Shoshana Zuboff, *supra* note 3 ; Marc Dugain et Christophe Labbé, *L'Homme nu: La dictature invisible du numérique (Paris: Robert Laffont, 2016).*

[7] Notably : Suzanne Vergnolle, *Normalisation de la surveillance et propagation de la manipulation : quelle place pour la liberté d'autodétermination ?*; Mare & Martin. *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, 2023. ⟨hal-03605112⟩.

But, more alarmingly, and maybe even more secretly, some States, authoritarian ones such as some which are proclaiming to be democratic ones, buy or rent new technologies from those private companies in order to themselves control the public debate or by asking them to suppress content preventively. It is particularly harmful for the freedom of expression as ironically, those who are supposed to protect it, are also those who violate this right. And it can go far, as manipulating the result of an election, a vote like it has been the case for the referendum on Brexit. The Cambridge Analytica society was used to guide the population opinion to answer "Yes" to the need of Brexit[8].

Faced with this reality, the European Union has become aware of the excesses of new technologies and decided to regulate technological actors. We have therefore seen the appearance of key texts such as: the Digital Services Act (hereinafter DSA)[9], the Digital Markets Act (hereinafter DMA)[10], the General Data Protection Regulation (hereinafter GDPR)[11]. They testify to his desire to establish accountability in law, and transparency. The European Union is trying in this way to regain control of the situation and register as a protector of our freedom of expression.

However, the subject is all the more relevant as it reveals the limits of European law. Its sufficiency and effectiveness, in the face of the frenetic pace of technical progress that systematically exceeds the law are questionable[12]. Indeed, although the ECHR strongly and durably protects our freedom of expression, these existing instruments struggle to protect us from the negative effects of new technologies.

The European Union must be careful not to rush into this race in the face of new technologies. A recent project, ChatControl promises to be particularly problematic regarding its respect for our fundamental rights[13]. Under cover of the protection of security and minors, the European Union risks placing freedom of expression in a vice between the economic logic of platforms and the security logic of states.

---

[8] Investigation into the use of data analytics in political campaigns A report to Parliament 6 November 2018 , Information Commissioner's Office.

[9] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (*Digital Services Act*).

[10] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (*Digital Markets Act – DMA*).

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (*General Data Protection Regulation – GDPR*).

[12] Notably : Antoinette Rouvroy et Thomas Berns, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux*, no 177 (2013) : 163–196, https://shs.cairn.info/revue-reseaux-2013-1-page-163.

[13] EDRi, *Chat Control: The EU's plan to scan your private messages*, European Digital Rights, 2023 (updated 2024).

Significance - because the subject touches on several disciplines: law, sociology, technological sciences, this thesis will be useful for a diversity of researchers, practitioners who wish firstly to realize the cost (benefits/drifts) what do new technologies have on freedom of expression and, secondly, deepen their critical knowledge of current tools for the protection of this freedom in a digital/technological context.

Finally, this thesis is of practical and citizen interest. At a time when the main place of exercise of freedom of expression is online and governed by new technologies, it becomes essential for each individual to understand the conditions of their supervision, to be warned about the risks of manipulation, of (self)censorship and the necessity and legal means available to protect oneself from it.

Overview of the research on the selected topic - Although there is a wealth of literature on this subject, few writings fully explore the paradoxical relationship between freedom of expression and new technologies. On:

- **The legal writings**

From a legal perspective, recent literature has focused on the European regulation of platforms. Laurence Burgorgue-Larsen[14], or even Pierre Auriel and Mathilde Unger (*La régulation par les plateformes*, 2024)[15] analyse the tension between freedom of expression and content moderation. As for Suzanne Vergnolle[16] in particular, highlights the standardization of surveillance and the growing complexity of the right to informational self-determination.

Authors such as Romain Tinière[17] invite to find a balance between the protection of freedom of expression and the fight against illegal or harmful content.

Goa Kacou[18] warns that if certain new technologies open up new spaces for expression and emancipation, they can be vectors of disinformation, propaganda, making necessary an interdisciplinary approach combining law, ethics, regulation in order to protect our real freedom of expression.

Finally, the jurisprudence of the ECtHR and of the EUCFR remains the cornerstone of reflection on the legitimate limits of this fundamental right.

---

[14] Laurence Burgorgue-Larsen, « Les Nouvelles Technologies », *Pouvoirs*, no. 130 (2009/3): 65-80.

[15] Pierre Auriel et Mathilde Unger, *La régulation par les plateformes. La liberté d'expression contre la liberté de modération ?* (Paris : Raison publique, 2024).

[16] Suzanne Vergnolle, *supra* note 7.

[17] Romain Tinière, « L'Union européenne et la régulation des plateformes de médias sociaux au prisme de la liberté d'expression », *Revue de l'Union européenne*, n° 650 (2021) : 413.

[18] Goa Kacou, "*Problématique de la liberté d'expression à l'ère de la communication numérique*," *Revue ivoirienne des Sciences du Langage et de la Communication* (SLC), no. 10 (December 2016): 243–256.

Complementary literature - In order to examine the European legal response and the opinions of legal scholars on this issue, it is essential to draw on a phenomenological assessment of the consequences of new technologies on freedom of expression. This is why certain sociopolitical and philosophical works are relevant, as they examine the various changes in this freedom in this unique context.

- **The philosophical and critical writings**

At the base of the reasoning, Michel Foucault[19] on the relationship between knowledge and power, Shoshana Zuboff (*The Age of Surveillance Capitalism*)[20] and Eli Pariser (*The Filter Bubble*)[21]. They lay the foundations for analyzing how digital technologies impact public speech as well as transform into mechanisms of social control.

Marc Dugain and Christophe Labbé (*L'Homme nu,* 2019)[22] and Dominique Cardon (*À quoi rêvent les algorithmes,* 2015)[23] strongly warn about the drifts of digital technology and algorithms.

- **The sociopolitical writings**

Some, such as Romain Badouard[24], introduce the idea of a regulation of online content distributed between states, platforms, and internet users themselves that could result in participatory censorship and take up Lessig's expression: 'Code is law'[25].

Scientific novelty - While there is abundant and exhaustive sociopolitical literature on the impact of new technologies on freedom of expression, European legal doctrine is less comprehensive, as the EU does not have a unified and comprehensive framework for the exercise of this freedom in the digital world. It is these gaps that the thesis aims to fill in.

Therefore, although this thesis remains predominantly legal in nature, it will propose an interdisciplinary approach combining the humanities, sociology, political science, and natural sciences (empirical studies of mechanisms, such as explaining how the algorithm used for Facebook works in practice). In this way, we will be able to establish a record of the phenomenological changes in freedom of expression brought about by new technologies and thus better assess the effectiveness of the European legal response.

---

[19] Michel Foucault, *Surveiller et punir. Naissance de la prison* (Paris : Gallimard, 1975).
[20] Shoshana Zuboff, *supra* note 3.
[21] Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (New York : Penguin Books, 2011).
[22] Marc Dugain et Christophe Labbé, *supra* note 6.
[23] Dominique Cardon, *supra* note 2.
[24] Romain Badouard, « La régulation des contenus sur Internet à l'heure des "fake news" et des discours de haine », *Communications*, no 106 (2020/1) : 161–173 (Paris : Éditions du Seuil) ; Romain Badouard, "*Ce que peut l'État face aux plateformes*," *Pouvoirs* 177, no. 2 (2021): 49–58, https://droit.cairn.info/revue-pouvoirs-2021-2-page-49?lang=fr.
[25] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); *see also* Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006).

On the other hand, as most private platforms are owned by American CEOs, the doctrine has focused on the US response, or adopted a global approach. This thesis proposes to examine the European model, which tends to focus on regulating these platforms, seeking a balance between restriction, freedom, and security.

Furthermore, the relationship between the protection of personal data and the protection of freedom of expression remains little explored. And this, even though the fear of surveillance in particular can lead to a phenomenon of self-censorship.

The contribution to legal research is thus to bridge the gap among freedom of expression law, data protection law, and technological regulation.

Research problem - The analysis of different legal, and complementary ones (social and philosophical and political texts) revealed several unanswered questions. The most burning question is the following: *To what extent new technologies, designed as instruments of emancipation and dissemination of speech, contribute today to the redefinition or even the restriction of freedom of expression in Europe, and does European law dispose-are there sufficient tools to preserve the effective exercise of it?*

Putting in other words : *How does the technological redefinition of freedom of expression in Europe reveal the limits of its legal protection?*

The present research aims to provide elements of an answer to this question.

Aim of the research - The purpose of this thesis is to analyze current and upcoming European regulations relating to new technologies in order to determine what needs to be modified, what should be retained to ensure a sustainable balance, ethical and viable between the freedom of expression and new technologies.

Indeed, today's technologies generate many uncertain situations and potential threats, which it is necessary to identify in order to be able to propose appropriate regulatory approaches. It is all the more pressing as democracy risks becoming obsolete in the face of the rise of private companies and States using the technologies.

This work is thus part of the balanced protection of freedom of expression as recognized by European case law, notably the Handyside v. United Kingdom judgment which states that:

"Freedom of expression constitutes one of the essential foundations of a democratic society, and one of the primordial conditions for its progress and the development of each individual."[26]

Objectives - To achieve this goal, we will:

1. The first objective is to analyze how new technologies both expand and limit the exercise of freedom of expression in Europe.
   This involves examining how private platforms modify the rules of expression in the public online space and influence the opinion of the population. It will be possible by examining the emergence of new forms of control, meaning the negative impacts of new technologies such as algorithmic visibility, surveillance, and self-censorship.
2. to assess whether the European legal framework (through the analysis of instruments such as the DSA, GDPR, caselaw) is adequate to safeguard freedom of expression when this right has been reshaped by new technologies, and whether it constitutes a sufficient framing of regulatory and moderation powers.
3. to explore the interdependence between data protection and freedom of expression;
4. to propose a track for new, balanced models of digital governance that ensure genuine rather than merely formal freedom of expression in the digital era.

Methodology - The way in which we will achieve our objectives will be done via:

- **Documentary analysis -** Collection and analysis of data from legal sources and scientific articles in order to study the regulations, societal consequences and practical use of cases of new technologies;
- **Comparative method:** firstly, to demonstrate the instrumentalization of new technologies, secondly, to analyze what degree of regulation allows for greater freedom of expression;
- **Hypothesis formation:** to propose scenarios for future regulation.
- **Qualitative empirical method**: Case studies (for example #MeToo, ...) to determine the liberticidal effects of new technologies.
- **Critical approach:** to assess the real impact of new technologies on freedom of expression and whether the current European legal response is sufficient.

[26] European Court of Human Rights, *Handyside v. The United Kingdom*, no. 5493/72, Judgment of 7 December 1976, § 49.

Defence statements

1. Real freedom of expression can only be ensured by governance that frames the influence of platforms and their algorithms, while protecting privacy and individual freedom of thought.

   The objective of this research is not to advocate a preventive or intrusive intervention of European regulation, but to study how far legal and ethical frameworks can and must go to maximize real freedom of expression, without restricting it. Indeed, intervening too early or too widely would amount to establishing preventive surveillance contrary to the very principles of democracy and the Charter of Fundamental Rights of the European Union. However, the absence of a framework leaves the field open to invisible forms of manipulation, where platforms and their algorithms direct thoughts, emotions, and behaviors without control or transparency. The challenge is therefore not to control speech, but to preserve the conditions for free speech by acting on the technical and economic mechanisms that shape it.
2. The protection of freedom of expression in Europe requires a deep adaptation of the European legal and ethical framework, which is currently insufficient to face the transformations brought about by new technologies and the growing influence of private digital actors.

Structure of Research - It consists of two main parts.

In the first part of the master's thesis, it is proposed to the reader a phenomenological observation of the mutations brought by new technologies on the exercise and the traditional legal framework of freedom of expression.

The second part provides a legal analysis of the European response, if it manages to protect the freedom of expression in this special context. It then moves beyond the current state of the law to assess which type of governance would be best to ensure sustainable protection of this fundamental right facing new technologies.

CHAPTER I - NEW TECHNOLOGIES AS A VECTOR OF EMANCIPATION AND REDEFINITION OF FREEDOM OF EXPRESSION

This chapter is divided into two subchapters. Firstly, the thesis is about recalling the importance and central square of the freedom of expression, broadly thus more specifically in the context of the new technologies and the digital world. Therefore, we will establish an observation of the mutations of this freedom that will help us to introduce the judicial corpus from the EU about new technologies.

Sub-chapter 1 - Freedom of Expression in face of Digital Technology: Foundations and Expansion of the European Public Space

1. The European legal framework for freedom of expression

There is no doubt that the particular importance of freedom of expression is ingrained as it is commonly accepted that *"Freedom of expression constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and for the development of every man."*[27] From this right depend all the others. In fact, freedom of expression guarantees pluralism, transparency, accountability. Putting in other words it means that without it, no other fundamental right can be truly exercised.

But, as we live now in a digital world, we are facing structural upheavals caused by technological evolution which drastically changed the conditions of exercise of the freedom of expression (inability to speak freely without fear of censorship or surveillance, not having the possibility to be really heard and read, restrictive access to a pluralism of information due to censorship and manipulation, limited of denied access to communication channels,...). Legally, these transformations may be translated into potential interferences with freedom of expression.

The EU and the Council of Europe must therefore protect this crucial pillar from new technologies, for example Artificial Intelligence, and have rules ready to be used against massive and arbitrary surveillance such as the one that exists in the US. In fact, the US authorities, through their repressive initiative named "Catch and Revoke", are using AI surveillance tools based on interpretative algorithms designed to intentionally target migrants and pro-Palestine student protestors. But, these probabilistics technologies *"have massive margins for error, and can often be discriminatory and biased."*[28]

---

[27] Ibid.

[28] Erika Guevara-Rosas, Senior Director for Research, Advocacy, Policy and Campaigns, Amnesty International, *USA/Global: Tech Made by Palantir and Babel Street Pose Surveillance Threats to Pro-Palestine Student Protestors and Migrants*, Amnesty International, 21 August 2025, https://www.amnesty.org/en/latest/news/2025/08/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/.

As a consequence, Erika Guevara-Rosas, Senior Director for Research, Advocacy, Policy and Campaigns at Amnesty International, explained that this action " *risks supercharging arbitrary and unlawful visa revocations, detentions, deportations and violations of a slew of human rights. These include the rights to privacy, freedom of expression and access to information, freedoms of movement equality and non-discrimination, and the right to liberty and protest.*"[29] It has impacts on freedom of expression because some people can have their visas revoked, be arrested, or be deported solely for expressing a protected political opinion.

Accordingly, this example illustrates the significance of having a strong European legal framework in order to effectively protect our freedoms. This is why this thesis is carried out, first, to sum up the traditional legal framework of this important right before analyzing how digital technologies have reshaped the conditions of expression.It is also an example to illustrate the kind of interference that European regulation must address.

As for the other rights defended by the EU inspired from the ECtHR, at least freedom of expression benefits from an equivalent protection to the one of the Council of Europe. This is due to the parallelism between the ECHR and the CFREU established by article 52 §3 of this latest document[30]. Indeed, for so-called mirror rights, which include freedom of expression, it is quite logical to assume that all ECtHR case law applies within the EU. Given that, cases of the ECtHR are relevant and need to be presented here. The case law of the ECtHR has been very rich and, over the years, has made it possible to determine the contours of this right to freedom of expression and then to assess its scope.

Freedom of expression is protected at all stages : internationally, through article 19 of the Universal Declaration of Human Rights (UDHR)[31] and article 19 of the International Covenant on Civil and Political Right (ICPR) which says : *"Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."*[32] And, it is also protected on a regional scale. In the same way, the Council of Europe protects this right with article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the EU, with article 11 of the Charter of Fundamental Rights of the European Union (CFREU). They both say : *"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless*

[29] Ibid.
[30] European Union, *Charter of Fundamental Rights of the European Union*, OJ C 83, 30 March 2010, art. 52(3).
[31] United Nations General Assembly, *Universal Declaration of Human Rights*, 1948.
[32] United Nations, International Covenant on Civil and Political Rights, 16 December 1966, art. 19.

of frontiers."[3334] As we can see, the definitions given in these three texts are similar meaning that there is a general understanding about the substance of this right, the scope of it is consequently homogeneous. On another hand, the appearance of this freedom in most of the principal documents protecting human rights only reinforces the prominence of freedom of expression.
Furthermore, these supranational texts protect both dimensions of freedom of expression. Thus, both articles affirm that freedom of expression has two distinct aspects: freedom of opinion (internal dimension) and freedom of broadcasting, otherwise known as freedom to receive and communicate information (external dimension). These two freedoms refer to two different realities: the content of the information itself and the vehicle for the information.

First, freedom of opinion allows everyone to defend their ideas, even if they are part of a minority view. It implies the right to be listened to in a tolerant manner. Thus, according to the ECHR, freedom of expression applies *"it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society"."*[35]

Therefore, the plurality of conflicting opinions falls within the scope of these two articles. Freedom of expression therefore seeks to protect speech that may once have been marginalized, even if it may create tensions between individuals. This view has not only been adopted in legal circles. George Orwell, for example, said: *"If liberty means anything at all, it means the right to tell people what they do not want to hear."*[36]

Secondly, freedom of dissemination, the second component, concerns the means of expression. It has been recognized that this freedom generally goes hand in hand with freedom of access to the Internet[37] and access to public information[38]. Thus, the Charter and the Convention also protect the right of access to the digital society.

There are many different types of information carriers, and they are becoming increasingly diverse: print media, radio, videography, photography, television broadcasting, and,

---

[33] Charter of Fundamental Rights of the European Union, art. 11.
[34] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No. 5, 4 November 1950, as amended by Protocols Nos. 11 and 14, art. 10.
[35] *Handyside v. The United Kingdom*, *supra* note, 26.
[36] George Orwell, *The Freedom of the Press* (unpublished preface to *Animal Farm*, written in 1945, first published posthumously in 1972), in *The Collected Essays, Journalism and Letters of George Orwell*, vol. IV, ed. Sonia Orwell and Ian Angus (London: Secker & Warburg, 1972).
[37] European Court of Human Rights, *Jankovskis v. Lithuania*, n°21575/08, Judgment of 17 January 2017, §62.
See more recently: European Court of Human Rights, *Vladimir Kharitonov v. Russia*, n°10795/14, judgment of 16 November 2020.
[38] European Court of Human Rights (GC), *Magyar Helsinki Bizottság v. Hungary,* n°18030/11, Judgment of 8 November 2016, §156.
See more recently: European Court of Human Rights, *Centre for Democracy and the Rule of Law v. Ukraine*, n°75865/11, decision of 3 March 2020, §49.

of particular interest to us here, the internet, social media, and more generally, ITC (such as communication networks, AI, …) .

There is no real definition of new technologies, either at the European or the international level: *"This acronym is characterized by uncertainty due to the very vagueness of the concepts covered by the terms 'technologies' (hardware? software? . . .), innovations (at what point can a system be considered new?) or 'information' and 'communication'."*[39] These concepts are indeed abstract, although omnipresent in economic, social, and legal doctrine. It remains difficult to define them precisely because, as Govaere has pointed out, the acronym ICT in particular covers multiple and evolving realities. Perhaps this is a deliberate choice on the part of users of the term, as it allows new creations to be easily integrated, which is rather useful given the rapid pace of progress.

However, for the sake of clarity in this thesis and to avoid any misunderstanding, a definition will be proposed. The EU has provided a broad definition of what it means by emerging technologies, characterizing them as: *"Technologies that are currently developing, or that are expected to be available within the next five to ten years, and are creating, or are expected to have significant social or economic effects. Examples: Big Data, Artificial Intelligence (AI), Blockchain, sensors, Internet of Things (IoT)."*[40] But still, we can also deduce from the DMA that new technologies are reflected in particular in the development of digital services and online platforms that play a central role in the digital economy, are capable of directly connecting businesses and users, generate significant network effects, and concentrate economic power around a few players known as "gatekeepers." At the international level, the OECD defines them in terms of their effects as follows: *"Emerging technologies, from synthetic biology and neurotechnology to artificial intelligence, immersive and quantum technologies, are characterized by rapid development and uncertainty in trajectory and impact."*[41] This notion can therefore be understood as technologies in the making, undergoing significant transformation that is likely to bring about structural changes of various kinds (social, economic, legal). This overlaps with the idea that ICTs are more than just technical progress; they are a systemic change that shapes the way we produce, communicate, and work. Given that we are focusing on studying the relationship between new technologies and freedom of expression, it is important to precise what we mean by ICTs. This refers to all technologies that enable access to and

[39] V. Govaere, *The Evolution of Work with New Information and Communication Technologies (NICT). Part I: NICT – Definitions and Uses*, Scientific and Technical Notes No. 221, French National Research and Safety Institute for the Prevention of Occupational Accidents and Diseases (INRS), 2002, 27 pp., available at: ffhal-01420146.

[40] European Commission, *Digital-Ready Policymaking – Glossary*, Interoperable Europe, available at: https://interoperable-europe.ec.europa.eu/collection/digital-ready-policymaking/glossary?utm.

[41] OECD, *Emerging Technologies*, OECD Global Forum on Technology, available at: https://www.oecd.org/en/topics/sub-issues/emerging-technologies.html.

processing of information and those that facilitate communication, i.e., all media that enable the recording and storage of information, as well as all the functionalities involved in disseminating and transmitting this information. Henceforth, this includes computer and network hardware as well as software and algorithms. In concrete terms, these are the devices, network components, applications, and systems whose combination enables individuals to interact[42].

For the sake of precision, Govaere proposed an analysis grid consisting of seven cumulative criteria to establish whether or not something belongs to ICTs:

1. Networking – interconnection and digital circulation of data.
2. Automation of intellectual work – ready-to-use software replacing cognitive tasks.
3. Multimedia – integrated processing of text, sound, image, and video.
4. Convergence – fusion of technologies (computing, telephony, audiovisual).
5. Nomadism – mobile use, detached from a fixed location.
6. Multipolar use – cross-functional circulation and exploitation of information (decision-making, planning,..).
7. Normalizing effect – creation of de facto technological standards (e.g., HTML, universal formats).

Ultimately, we understand that new technology encompasses all intellectual processes based on electronics that serve an organizational purpose. In other words, as summarized in J. Spérandio's work, they ensure the networking and processing of information because they enable media convergence and digital interactivity[43].

In this thesis, we will not examine the relationship between freedom of expression and each new existing technology. Instead, we will focus on the most relevant categories for legal and ethical analysis, namely:

1. Artificial Intelligence (AI): *"a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"[44];*

---

[42] European Commission, *Glossary: Information and Communication Technology (ICT)*, Eurostat, available at:https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT) ; CyberUniversity, *NTIC: Tout sur les nouvelles technologies de l'information et de la communication*, available at: https://www.cyberuniversity.com/post/ntic-tout-sur-les-nouvelles-technologies-de-linformation-et-de-la-communication.

[43] Jean Spérandio, *Les nouvelles technologies de l'information et de la communication*, Paris: Presses Universitaires de France (PUF), coll. « Que sais-je ? », 1998.

[44] Artificial Intelligence Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Art. 3(1).

2. Algorithms: *"Algorithms are a process, a set of rules or instructions that enable a computer program to combine multiple sources of information to generate results. They are also used to operate social media platforms and determine the content presented to each user."*[45]
3. Social networks and digital platforms: these connected communicative infrastructures are the substitutes for traditional media. For example, platforms such as Meta, X, TikTok, YouTube, Instagram, Snapchat.
4. Big data and personal data processing: this action *"means any operation or set of operations which is performed on personal data or on set of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*[46]
5. Internet and network infrastructures: nor the DSA, or the AI Act, the DMA or the GDPR provide a legal definition of them because they are taken for granted as technical. They can be defined as a worldwide interconnected dematerialized system which enables communication and circulation of information between users with the support of network infrastructures.

Each of these technologies greatly expands the ways in which we communicate, to such an extent that they have considerably redefined our freedom of expression.

Finally, it is important to distinguish between new technologies (an innovation in a given technical field) and emerging technologies (resulting from the convergence of several technologies)[47].

Thus, while new technologies are profoundly redefining the terms and conditions of communication, they do not alter the fundamental nature of this freedom. On the contrary, these technological developments make it all the more important to remember that freedom of expression is protected at 360 degrees by states.

So, due to the fact that freedom of expression is the cornerstone of any democracy*, "the landmark freedom of modernity"*[48], and "*one of the pillars of democracy, afforded an enviable*

See also the broader, non-binding definition proposed by the European Commission's High-Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Disciplines*, 2019, §4.

[45] Amnesty International, *Technology*, https://www.amnesty.org/fr/what-we-do/technology/.

[46] General Data Protection Regulation , art. 4(2).

[47] V. Govaere, *supra* note 39.

[48] Elisabeth Zoller, "Foreword : Freedom of expression : precious right in Europe, Sacred right in the United States", *84 Ind, L.J.* 803 (2009): 803.

position on a particularly high pedestal within many fundamental rights frameworks"[49], it enjoys full protection as States have both negative and positive obligations[50]. Herewith, Member States first have an obligation of abstention and must therefore not interfere with the freedom of expression of natural or legal persons within their jurisdiction. These negative obligations are coupled with procedural rights, meaning that public authorities must act by adopting all necessary measures to effectively guarantee our rights and freedoms. Thus, the ECtHR[51] has explained that positive obligations in relation to freedom of expression imply that States are required to create an environment conducive to participation in public debate by allowing people to express their opinions and ideas without fear. For example, the ECtHR has described States as the ultimate guarantors of pluralism[52].

However, it is not just because this freedom is highly protected, that all forms of expression are. Like all other freedoms, freedom of expression is not absolute; it can be limited, and since one person's freedom of expression must coexist with the freedoms of others or the public interest, a balance must be struck. Not all information falls within the scope of Article 10 of the ECHR or Article 11 of the CFREU. This is delimited in Article 10(2) of the ECHR and Article 52 of the CFREU. Within the Council of Europe, public policy clauses are specified for each freedom and are referred to as special interference clauses, whereas the EU has one clause for all the rights it protects, which is therefore referred to as a general interference clause.

There are three conditions for restricting freedoms: first, any restriction must be provided for by law, i.e., understood as a sufficiently accessible, foreseeable and legally binding normative basis (such as regulatory instruments, case-law, general principles of law,...), secondly, it must pursue a legitimate aim; and, finally, the measure must be proportionate and necessary in a democratic society, which refers to the existence of a pressing social need[53]. Verification of this third condition involves a three-part test:

1. Adequacy: Does the restriction of freedom enable the objective to be pursued? ;

---

[49] European Court of Human Rights, *Airey v. Ireland*, n°6289/73, Judgment of 9 October 1979, §24: *"The Convention aims to protect rights which are not merely theoretical or illusory, but practical and effective."*.
See also: Aoife O'Reilly, "In Defence of Offence : Freedom of Expression, Offensive Speech, and the Approach of the European Court of Human Rights", 19 *Trinity C.L. Rev*. 234 (2016): 235.

[50] Ibid., §25: *"The implementation of a State's obligations under the Convention sometimes requires positive measures; in such cases, the State cannot remain passive."*.

[51] European Court of Human Rights, *Dink v. Turkey*,n° 2668/07, 6102/08, 30079/08, Judgment of 14 September 2010, §137.
See also similarly in the context of the EU: Court of Justice of the European Union (GC), *Poland v. Parliament and Council*, C-401/19, Judgment of 26 April 2022, §§ 47, 55, 56, 67.

[52] European Court of Human Rights, *Informationsverein Lentia and others v. Austria*, n° 13914/88; 15041/89; 15717/89; 15779/89; 17207/90, Judgment of 24 November 1993.

[53] Notably: European Court of Human Rights, *Sekmadienis Ltd v. Lithuania*, no. 69317/14, Judgment of 30 January 2018, §71.
See also similarly in the context of the EU: Court of Justice of the European Union (GC), *Poland v. Parliament and Council*, C-401/19, Judgment of 26 April 2022, § 82-84.

2. Necessity: Is there a less intrusive solution? ;
3. Proportionality: Does it create an excessive burden in relation to the objective pursued? In other words, *"in the light of the case as a whole and determine whether it was 'proportionate to the legitimate aim pursued' and whether the reasons adduced by the national authorities to justify it are 'relevant and sufficient'."*[54]

The exhaustive list of exceptions (meaning legitimate interest) presented is the following : interests of national security, territorial integrity, public safety, prevention of disorder or crime, protection of health or morals, protection of the reputation or rights of others, preventing the disclosure of information received in confidence, or maintaining the authority and impartiality of the judiciary.

More broadly, according to Article 52§1 of the CFREU: *"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others"*[55].

However, it is important to remember that the principle is freedom, the exception is restriction[56], since freedom of expression is an "enabling right," essential to the exercise of all other rights[57], indispensable to the very existence of a free society[58]. The limitations and restrictions admitted on this freedom are therefore few and subject to strict proportionality controls, particularly in the political and public interest spheres[59].

Thus, as it had been said, every expression is not protected and the worst is the one which constitutes an abuse of right prohibited by article 17 of the ECHR and article 54 of the CFREU. These articles mean that : *"Article 17, insofar as it applies to groups or individuals, aims to prevent them from deriving from the Convention a right that would enable them to engage in an activity or perform an act aimed at destroying the rights and freedoms recognized in the Convention."*[60] In the context of freedom of expression, when information is considered hateful

---

[54] Notably: European Court of Human Rights, *Frisk and Jensen v. Denmark*, no. 19657/12, Judgment of 5 December 2017, §51.

[55] Charter of Fundamental Rights of the European Union, art. 52(1).

[56] European Court of Human Rights, *The Sunday Times v. The United Kingdom*, no. 6538/74, Judgment of 26 April 1979, §65: *"The Court is faced not with a choice between two conflicting principles but with a principle of freedom of expression that is subject to a number of exceptions which must be narrowly interpreted."*

[57] United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc, A/HRC/17/27, 16 May 2011.

[58] United States Supreme Court, *Palko v. Connecticut*, 302 U.S. 319 (1937), doctrine of Justice Cardozo.

[59] Recall in the European Court of Human Rights, *Lingens v. Austria*, no. 9815/82, Judgment of 8 July 1986 ; *Sunday Times v. United Kingdom*, *supra* note 56 ; European Court of Human Rights, *Observer & Guardian v. United Kingdom*, no. 13585/88, Judgment of 26 November 1991.

[60] Charter of Fundamental Rights of the European Union, art. 54.

or openly denies the freedoms and values upheld by the Convention or the Charter, it constitutes an abuse of rights.

These limits on freedom of expression show that, despite its democratic importance, it is not absolute. This raises the question of who is competent to decide whether an expression is protected or not. Indeed, its concrete scope varies depending on whether one is within the system of the Convention or that of the EU, the latter having a limited scope of application. Due to the principle of conferral of powers: the fundamental rights of the EU are only binding on Member States, institutions, bodies, and agencies within the scope of the powers conferred by the founding treaties. Consequently, the Charter of Fundamental Rights, the scope of which is expressly specified in Article 51(1), applies only when Member States implement EU law. Historically, this limitation can be explained by the initial reasons for the creation of the EU. The Community project was initially structured around an economic objective: reconstruction after the world war. In doing so, the EU was given powers in the areas of the common market, free movement, competition, and services. The protective foundation of fundamental freedoms was only developed later. Thus, even though the Charter is not applicable in general and abstractly, and without conditions, in practice, when it comes to new technologies' situations, the EU law can still be it. As European interventions relating to them are in fact linked to different areas of competence: the internal market and digital services ; this is why the EU still has power over new technologies. And, this is why the EU covers the economic functioning of platforms and the services they provide, rather than strictly and directly speaking the link between new technologies and freedom of expression. The ECHR acts as a general safeguard for freedom of expression in the European digital space, with the Charter establishing a parallel between it and the convention.

In conclusion, the Council of Europe, above all, but also the EU, through its support for the protective framework of the ECHR and the ECtHR, make it a point of honor to guarantee our freedom of expression by : both the expression itself and its medium are strongly protected, even when it is disturbing, restrictions of this freedom are subject to strict control,

Digital technology does not change these old principles, but tests them almost insidiously, without anyone really daring to realize the enormity of its impact, which combines both positive and negative contributions to this freedom.

2. Positive transformation of freedom of expression

Since the moment of the creation of the Internet, its benefits for the freedom of expression of all the human kind has been obvious, unquestioned. So unquestioned that, it is since, commonly admitted that *"the Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest.*"[61] This unanimous opinion persists with the entry of new technologies, such as social media, AI and algorithms, generative IA, …, which come with more and more advantages. As for the industrial revolution or media revolution of previous centuries (printing), the first stage of the digital revolution was marked by a general enthusiasm ; we first saw the good aspects this era brought to us.

At the same time, life before their emergence, and life with them, are drastically different, both practically and socially and politically. Before, during the pre-digital era, information was primarily disseminated through traditional media, newspapers, radio, and television. As a result, the flow of information was slow. Access to expression was less democratic, as only certain actors were heard on a large scale or had the opportunity to be heard; as a result, minorities, for example, had less visibility than they do today. Secondly, there were fewer spaces for expression; public debates took place in physical forums and in the conventional media. Expression had a limited geographical reach and could be filtered by intermediaries (publishers, journalists, authorities). Public expression therefore remained geographically restricted and socially controlled.

New technologies have thus multiplied the swiftness of transmission of expressions, making it instantaneous. Speech has become structurally democratized: anyone can publish, share, comment, i.e., act virtually, unlike in the past when this was mainly reserved for the press. This acceleration of expression has been accompanied by its amplification, made possible by the creation of new forums and digital public spaces such as social networks and collaborative platforms. These spaces are much more easily accessible, open, and geographically unlimited, in other words, they are borderless. From a legal perspective, this democratization of speech raises the question of whether the traditional protection framework of freedom of expression as guaranteed under articles 10 ECHR and 11 CFREU, remains adapted to this changing era.

---

[61] European Court of Human Rights, *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, Judgment of 1 December 2015, §§ 49–56 (see also European Court of Human Rights, *Ahmet Yıldırım v. Turkey*, no. 3111/10, Judgment of 18 December 2012, § 54).

It is now possible to reach a global, multicultural, and transgenerational audience. A post on a social network such as X, Instagram, or Facebook can be seen by millions of people in just a few minutes. This interconnectedness also makes it possible to instantly communicate with a stranger on the other side of the world. These new virtual forums therefore enable international and interconnected expression.

This reconfiguration of the forum is not limited to amplifying speech and its speed; it also transforms the means of expression. In the Magyar JetiZrt v. Hungary case[62], the ECtHR acknowledged that simply sharing a hyperlink and, more generally, using web mechanisms (links, sharing, interconnections) constitutes an act that falls within the scope of Article 10 of the Convention. Through this case, it is judicially recognized that online interactions have become an expression, extending the traditional frame of this fundamental right. It raises the same question as to whether the traditional framework of freedom of expression under articles 10 ECHR, and 11 CFREU remains adapted.

At this stage, it is clear that new technologies have structurally transformed the public sphere of expression, but their positive impacts continue. In addition to those mentioned above, they have also helped to rebalance the unequal power relationship between states and protesters by giving the latter a powerful means of expression and a space for expression and mobilization for minority or marginalized groups. They are likely to have greater visibility, paving the way for them to act in favor of societal change. Movements such as #MeToo, Black Lives Matter, and 15-M have demonstrated the mobilizing power of private platforms.

In the case of the 15-M movement, also known as Indignados, that emerged in Spain on May 15, 2011 in response to the severe economic crisis, which notably resulted from the increased mistrust of the political system at the time, new communication technologies (social networks, hashtags, online forums) have played a driving role. They have facilitated mobilization and coordination, expanded the space for expression via forums independent of traditional media[63], by accelerating dissemination (a rapid means of expression, for example, the ability to comment with a single gesture from home). This movement led to the creation of a new political party in Spain: Podemos. All in all, the 15-M movement illustrates how online platforms have reinforced collective participation, raising again questions about the sufficiency of protection provided by the traditional framework.

---

[62] European Court of Human Rights, *Magyar Jeti Zrt v. Hungary*, no. 11257/16, Judgment of 4 December 2018, §§ 73–76.

[63] IPS News, "Spain's Indignados Take to the Streets Again," May 30, 2012, https://www.ipsnews.net/2012/05/spains-indignados-take-to-the-streets-again/.

For this pillar of democracy, the changes we are experiencing today are leading to its redefinition. Freedom of expression no longer means simply saying what you think: it also means having the right to be heard, to mobilize, and to participate actively in public life.
We understand that: *"The internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information."*[64] That is why, from now on, blocking an entire platform (and not just the contentious content) constitutes a disproportionate infringement on freedom of expression[65].

Nevertheless, the Internet forces us to share our worldview, otherwise we fall back into the isolation of the past. The opening up of space for expression indirectly forces individuals to use these digital channels: if we do not express ourselves, if we remain passive, we return to a form of intellectual and social isolation ("the isolation of yesteryear"). They are no longer just a distraction but truly "the place to be" in order to express oneself and be heard. Thus, paradoxically, these new technologies, by bringing freedom of speech to its peak, also pose its greatest danger: the vital dependence of freedom of expression on ICTs makes this era particularly precarious. For example, around 47% of French people get their news via social media every day, and more than 9 out of 10 are Internet users, according to the ARCOM/ARCEP Digital Usage Reference Framework[66]. Not using them would be tantamount to intellectual and social isolation. As Mr. Tinière pointed out, the quasi-hegemonic concentration of platforms such as Facebook and Twitter makes it difficult to use other media, especially for those seeking a wide audience. Even though this section was about the position transformations, it foreshadows the structural problem online platforms have built and the necessity of a better legal response.

This is because, even though we are living in a golden age[67] of freedom of expression, where the internet is simultaneously a vehicle for emancipation and a tool of tyranny, after highlighting the beneficial contributions of new technologies to freedom of expression, it is necessary to examine their abuses and risks, this paradox of amplified but fragile freedom.

---

[64] *Ahmet Yildirim v. Turkey*, *supra* note 61, §54; see also *Cengiz v. Turkey*. *supra* note 61.
[65] *Cengiz v. Turkey*. *supra* note 61.
[66] ARCEP & ARCOM, *Référentiel des usages numériques*, June 2024, https://www.arcep.fr/fileadmin/user_upload/pole-numerique-arcep-arcom/referentiel-usages-numeriques-arcep-arcom_juin2024.pdf.
[67] Romain Badouard, *La régulation des contenus sur Internet à l'heure des « fake news » et des discours de haine* (Paris: Presses de Sciences Po, 2020), 45–46.

Sub-Chapter 2 - The paradoxes of digital freedom of expression: between openness, surveillance and manipulation

1. The negative impacts of new technologies over freedom of expression

1.1. Direct limits of freedom of expression

Every technological advance brings its share of benefits and drawbacks[68]. The digital age therefore appears to be a double-edged sword: on the one hand, the ability for individuals to express themselves on the internet is an unprecedented tool for exercising freedom of expression[69]; on the other hand, the advantages of this medium come with a number of risks, as *"defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online. "*[70]

This first drift stems from the misuse of these new technologies by certain users. Social media are therefore both forums for citizen mobilisation and for promoting extremist ideologies. As an example, it was social media that enabled Daesh to spread its deadly propaganda and to facilitate recruitment across the world.

Furthermore, anonymity and pseudonymity combined with the tendency to forget social norms, may foster a sense of protection against legal condemnation. This can encourage the spread of ideas that are not protected by the Charter or the Convention by making their words less thoughtful, harsher, and more unrestrained[71]. These trolls are created by platforms in that they promote an environment where provocation is rewarded[72]. But, trolling is the logical result of a system based on provocation and conflict[73]: the more aggressive and outrageous the content, the more emotional it is, the more it circulates. We are therefore faced with a systemic loop: the existence of illegal content reduces our freedom, which increases content moderation and reduces it even further. This systemic loop shows how difficult it is to apply the traditional framework, recall in the first-sub-chapter, in an environment where the boundary between protected and unprotected discourse is blurred. It raised two questions : where is the limit of the State's positive obligations to protect freedom of expression from online abuses, and, where is the limits of imposing responsibility to private platforms.

---

[68] European Court of Human Rights (GC), *Delfi AS v. Estonia,* Judgment of 16 June 2015, no. 64569/09, §110.
[69] Ibid.
[70] Ibid.
[71] Tom Clucas, "'Don't Feed the Trolls'," in *Violence and Trolling on Social Media*, ed. Sara Polak and Daniel Trottier (Amsterdam: Amsterdam University Press, 2020).
[72] Ibid.
[73] Ibid.

In addition to these abuses, new technologies have also introduced multifactorial forms of censorship and self-censorship which may constitute interferences with freedom of expression. First of all, this can originate from ourselves. Michel Foucault[74] described how the carceral panopticon theorized by Bentham creates a feeling of being observed to the point it spontaneously induces the adaptation of individuals' behavior. This is similar to Plato's allegory of the cave[75]. Transposed to the digital world, this mechanism illustrates the logic of platforms: every action, whether it be posts, clicks, searches, or reactions, can be processed by algorithms. Users, like the prisoners, may feel watched by platforms, governments, and other users. This has serious consequences for freedom of expression as it pushes individuals to adjust their discourse, to not express their real opinions because of the fear of being observed. Such "chilling effect", resulting from the inhibiting effect of constant vigilance has been recognized by the European Court of Human Rights, particularly in cases involving mass surveillance[76]. Moreover, the fear of excessive collection or misuse of data can also be a limiting factor on freedom of expression. These mechanisms may constitute restrictions to the protected freedom of expression which may pose problems with regard to the regime of justification for possible restrictions posed by the CFREU or the ECHR. They raise questions about the sufficiency of the EU legal response to deal with disproportionate interferences.

Secondly, it can come from the platforms themselves through : suspension, shadow ban, profiling. In fact, combining the analyses of Vergnolle[77], Rochfeld[78], and more generally the documentation on algorithmic filtering, we realize that platform algorithms do not just order created content and make it visible, they do much more... Their impact on user behavior is enormous; they predict it in order to better optimize it and influence behaviour by reshaping the conditions of communications. Profiling carried out by algorithms via the analysis of non-quantifiable data automatically classifies individuals, which undoubtedly leads to restrictions: what we can see, what we can receive, what we say, how we are perceived. Individuals may no longer choose the parameters of their space for expression such as their visibility, the audience they reach ; as it is the result of increasingly complex and opaque calculations. As a result, new technologies may constitute a restriction to our freedom of expression.

On the other hand, new technologies have a direct impact on our freedom of expression, or at least on their owners, since they allow certain content to be filtered, prioritized, and even

[74] Michel Foucault, *supra* note 19.
[75] Marc Dugain et Christophe Labbé, *supra* note 6.
[76] European Court of Human Rights (GC), *Zakharov v. Russia*, no. 47143/06, 4 December 2015; Big Brother Watch, commentary on *Zakharov v. Russia*.
[77] Suzanne Vergnolle, *supra* note 7.
[78] Judith Rochfeld, "Contre l'hypothèse de la qualification des données personnelles comme des biens", in *Les biens numériques*, dir. E. Netter et A. Chaigneau (Paris : CEPRISCA, 2015), 221 s., spéc. 225.

made invisible at will. This is known as shadow banning, a form of censorship through invisibility[79]. This form of censorship is more insidious than explicit deletion. This censorship is vicious because it relies on silent algorithmic processing, first modulating visibility, then reducing it without the user noticing. This makes the infringement on freedom of expression all the greater, because it goes unnoticed. It creates a paradox: everyone can speak, with social media presenting itself as the ultimate vehicle for expression, but no one can be sure of being heard, and if they are, it may only be by those who think like them.

The fact that the purpose of new technologies is strictly economic, to learn as much as possible about each of us, has transformed our freedom of expression, which is no longer just the right to express oneself but also, and above all, the emerging right to be heard, seen, and exposed. Thus, freedom of expression is also at stake in the battle for visibility[80]. The emergence of a new aspect of this freedom does not directly imply a problem. It is primarily a conceptual change marking a paradigm shift: from formal/theoretical freedom of expression, "I can say what I want," to functional freedom of expression, "my words can be heard, seen." However, new technologies allow everyone to speak, but this does not guarantee that they will be heard[81]. Technological advances have made this feeling of being overshadowed by others all the more real: the abusive use or ostentatious visibility of some can silence others. It also means that platforms have more means and ways to restrict freedom of expression. Who would be heard in a crowded café if they weren't given a microphone? It's similar on social media, except that instead of asking for the microphone, you have to understand the algorithmic mechanics, and sometimes the microphone can only be handed to you by a third party, private platforms...

In addition to being directly restricted by deletion and explicit moderation, freedom of expression is also subject to indirect, more subtle and insidious limitations.

1.2 Indirect limitations of freedom of expression

Digital technologies have therefore multiplied the forms of control: surveillance, disinformation, online harassment, trolls...[82] but also polarization. Algorithmic logic is not limited to classifying content: it allows messages to be tailored to each individual, opening the door to what Shoshana Zuboff calls *surveillance capitalism*[83]. The latter seeks not only to predict

[79] Romain Badouard, "Shadow ban. L'invisibilisation des contenus en ligne," *Esprit*, no. 11 (2021): 75-83.
[80] Romain Badouard, *La régulation des contenus sur Internet à l'heure des « fake news » et des discours de haine* (Paris : Presses de Sciences Po, 2020).
[81] See notably: Shoshana Zuboff, *supra* note 3 ; Tom Clucas, *supra* note 71.
[82] Olga Dovbysh et Esther Somfalvy, *"Understanding Media Control in the Digital Age"*, *Media and Communication*, vol. 9, n° 4, 2021, p. 1-4, available at: https://doi.org/10.17645/mac.v9i4.4861.
[83] Shoshana Zuboff, *supra* note 3.

our behavior, but to modify it, to the point of automating us and companies learn to *"write the music, and then let the music make them dance."*[84] Manipulation does not need a physical element, a foreign body, to influence our minds. This is why the manipulation of new technologies is described as invisible.

This transformation of our means of expression is not neutral: it creates conditions in which certain opinions appear spontaneously more legitimate, while others appear more marginal, prioritizing some opinions over others. Algorithms have thus invaded all areas of human life, marking "*an epistemological, anthropological, and more broadly civilizational turning point."*[85]

The Cambridge Analytica scandal provides a perfect illustration of this. As Christopher Wylie[86] revealed, platforms continuously process a staggering amount of data, giving them the power to understand individuals' psychology. These data permit private actors to influence the outcome of an election by adapting the campaign to every individual. Unified public debate is disappearing in favor of an infinite number of "debate clones" that are invisible to each other.

Gérald Bronner has argued that this environment, structured by competition for attention, automatically favors the most extreme and sensationalist content: individuals are then exposed to a deregulation of the cognitive market, which makes manipulation all the easier[87].

This dynamic reveals a more profound change: data mining. Based on profiling, it reconstructs individuals from fragmented information by coding and statistical correlations[88]. In this way, they intrude into our minds by influencing our thoughts, emotions, and opinions, creating a profile for each individual and shaping them to achieve their ends[89]. This is why the doctrine asserts that profiling establishes determinism. It is what Antoinette Rouvroy[90] calls *algorithmic governmentality* as the code is law[91]. Eventually, with big data, we have gone beyond the dictatorship envisioned by Orwell in 1984, inspired by known models of tyranny.
Another question is raised here : how the freedom of expression can be effectively exercised when its conditions are shaped by automated decision-making systems.

The risk is not only technical in nature; it stems primarily from the economic model of digital platforms. In some ways, the use of new technologies may be seen as based on the

---

[84] Ibid.
[85] P. Adam*, « Connected factory », Dalloz Dr. Soc., 2018, 1,* citing É. Sadin, *La vie algorithmique. Critique de la raison numérique* (Paris : L'Échappée, 2015), 30. A9ric-la-vie-algorithmique-2015.pdf?utm.
[86] Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America, (New York: Random House, 2019).
[87] Gérald Bronner, *Apocalypse cognitive* (Paris : PUF, 2021).
[88] Antoinette Rouvroy et Thomas Berns, *supra* note 12.
[89] Suzanne Vergnolle, *supra* note 7.

[90] Antoinette Rouvroy et Thomas Berns, *supra* note 12.
[91] Lawrence Lessig, *supra* note 25.

following adage: if you don't pay for something, you're not the customer, you're the product. Thus, the monetisation of personal data reshapes the conditions of exercise of freedom of expression.

Political microtargeting poses a direct threat to collective freedom of expression: by sending a different message to each individual, it destroys the very possibility of a common public space. This constitutes a form of structural censorship, not through the suppression of speech, but through the radical fragmentation of its reception. The affiliation of these phenomena to the interferences possible under Article 10 ECHR and 11 CFREU is very questionable given their indirect and structural impacts on freedom of expression.

Moreover, new technologies, and more specifically their algorithmic systems, not only create a profile for each user, but also lock them into filter bubbles[92]. In 2011, Eli Pariser analyzed the phenomenon of web personalization and theorized this idea in relation to the internet, as it was the emerging and revolutionary technology of the time: *"The internet is showing us what it thinks we want to see, but not necessarily what we need to see."* [93] In other words: *"A squirrel dying in your front yard may be more relevant to your interests right now than people dying in Africa."*[94] So profiling and moderation, the consequences of which we have seen above, also have the effect of allowing content to be personalized**.** Here again, we are facing a paradigm shift with equally harmful effects.

Content personalization traps each user in invisible bubbles or echo chambers[95] by presenting the "most suitable" information, thereby confirming their preconceptions[96] and amplifying their personal biases[97]. Algorithms homogenize the content seen by a user in order to retain their attention and maximize their engagement. Instead of opening individuals to contradictory ideas and promoting creativity, algorithms polarize and caricature the world by making disagreement invisible[98]. By leaning on the psychological phenomenon called confirmation bias and limiting exposure to diverse opinions, digital platforms may interfere with the State's positive obligation to guarantee pluralism. The resulting fragmentation of public debate affects the exercise of freedom of expression by impoverishing it and undermining pluralism. Moreover, the indirect nature of those limitations makes it more complicated to regulate them compared to direct censorship.

---

[92] Eli Pariser, *supra* note 21.
[93] Ibid.
[94] Eli Pariser, *supra* note 21, (citing Mark Zuckerberg).
[95] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton : Princeton University Press, 2018), https://doi.org/10.2307/j.ctv8xnhtd.
[96] Gérald Bronner, *supra* note 87*,* 51.
[97] Cass R. Sunstein, *supra* note 95.
[98] Cass R. Sunstein, *supra* note 95.

In the end, new technologies embody an existential paradox for freedom of expression: they make the means of communication infinite, but simultaneously shape, filter and polarize messages. The phenomena analyzed in this chapter reveal the innate power of new technologies to shape freedom of expression. New technologies have transformed the very structure of expression and its vectors in various situations such as electoral context (through targeting content), political discourse (through algorithmic amplification and invisibilisation), online hate speech (through moderation), surveillance in the name of security (such as ChatControl) through access of a massive amount of data.

Their deviations then raise the question of a framework for these tools and the power of their owners: how to preserve the values of pluralism, tolerance, and the spirit of openness in an environment dominated by private actors and where States are actors of censorship and manipulation ? Does the current European legal framework have sufficient tools to meet this challenge? It is these questions that we will try to answer in the next chapter. We will first analyze European regulation, then we will explore which model of technology governance should be pursued.

CHAPTER II - NEW TECHNOLOGIES AS LEGAL, ETHICAL AND POLITICAL CHALLENGE FOR FREEDOM OF EXPRESSION

This chapter is divided into two subchapters. Firstly, the thesis will analyze how the European Union supervises the new role of platforms, and deals with libertical drift brought by new technologies. Therefore, the research will analyze the legal framework framing the relation between new technologies and freedom of expression before suggesting a complementary contribution of the implementation of an ethical co-governance.

Sub-chapter 1 - Regulatory Supervision the new Expression Governors: a Challenge for the EU

1. The new role of Platforms: from Neutral host to Algorithmic Censor

The technological revolution has brought about a silent but radical transformation: public space is no longer public because it belongs to companies. Discussion "forums" and "channels" are owned, moderated, and ultimately controlled by a handful of private actors. This concentration of power creates an oligopoly with enormous consequences for all aspects of our freedom of expression. The dominance of public actors is no more, and this has not escaped the attention of European courts such as the ECHR and the CJEU, which have gradually recognized the quasi-public role of platforms.

Therefore, in order to understand this subtle transfer of power, it is necessary to examine how these jurisdictions have dealt with the emergence of these new spaces for expression. The ECHR took the first step toward recognition in its ruling in Appleby and Others v. the United Kingdom, in 2003, recognizing that a private space could be an essential venue for the exercise of freedom of expression. In this case, environmental activists wanted to distribute leaflets in a (private) shopping center, but the owner of the Galeries refused, so they invoked a violation of Article 10 of the Convention. Both domestic courts and the ECHR ruled that there had been no violation. But, this later admit that : "*Where, however, the bar on access to property has the effect of preventing any effective exercise of freedom of expression or it can be said that the essence of the right has been destroyed, the Court would not exclude that a positive obligation could arise for the State to protect the enjoyment of the Convention rights. "*[99] Some legal

[99] European Court of Human Rights, *Appleby and Others v. the United Kingdom*, no. 44306/98, Decision of 6 May 2003, § 47.

scholars[100] have sought to apply this case law to private platforms, given that social networks are presented as the "modern public square"[101] playing a role similar to that of traditional public squares. By way of illustration, the general blocking of an entire platform[102] constitutes a violation of Article 10 of the Convention, reinforcing the idea that access to these public forums is essential to the effective exercise of freedom of expression.

A similar logic exists in competition law: the theory of essential facilities. One might think of transposing this to new technologies. This doctrine considers that a dominant company, owning infrastructure that is indispensable to a service and that others cannot reasonably replicate, cannot refuse access to that infrastructure. This is because such access is necessary to enter or compete in a market. To better understand this idea, let us consider the most common example: railways. As the rail network cannot be replicated by third parties, if its owner refuses them access, they cannot provide their services. The owner therefore closes the market by preventing new competitors from entering. The convergence with the reasoning developed in the Appleby ruling is clear: in both cases, a private actor controls a structurally indispensable space (for expression in one case, for competition in the other).

However, platforms today play a role of comparable importance, as they tend to establish themselves as the ultimate vehicles for expression and determine visibility (a new component of freedom of expression) and audience reach. Furthermore, it seems realistic to believe that it would be complicated to create a platform capable of competing with existing ones such as Facebook, YouTube, X, and TikTok; it could not offer the same level of visibility and expression. Several authors support the transposition of this theory to the digital world: digital infrastructures should be seen as essential facilities with an equally transposable obligation for their owners. Thus, N. Guggenberger[103] argues that this doctrine of competition law is applicable to the digital economy. According to him : "*while courts have mainly applied the doctrine to physical infrastructure, its potential now lies in addressing the gatekeeping power of online platforms."*[104]

---

[100] See notably: Anett Pogácsás, book review of András Koltay, *New Media and Freedom of Expression: Rethinking the Constitutional Foundations of the Public Sphere* (Oxford: Hart Publishing, 2019), 224 pp., ISBN 978-1-50991-649-8.

[101] Supreme Court of the United States, *Packingham v. North Carolina*, No. 15-1194, argued February 27, 2017, decided June 19, 2017, (referring to social media as the "modern public square"). Although this judgment falls within U.S. constitutional law, it is frequently relied upon in European legal scholarship to analyse issues related to digital exclusion and effective access to the online public forum.

[102] *Ahmet Yıldırım v. Turkey*, *supra* note 61, § 68 ; *Cengiz and Others v. Turkey, supra* note 61.

[103] Nikola Guggenberger, "The Essential Facilities Doctrine in the Digital Economy: Dispelling Persistent Myths," *Yale Journal of Law & Technology* 23 (Spring 2021), 301–33, available at: https://yjolt.org/sites/default/files/23_yale_j.l_tech._301_essential_facilities_0.pdf?.

[104] Ibid.

While R. Dacar[105] examines the possibility that access to Big Data could fall under the theory of essential facilities.

But, caution is required when applying this doctrine. As the CJEU has not formally established its application to new technologies, this extension remains controversial, especially with regard to non-physical infrastructure. It should be noted that certain decisions point in this direction, without explicitly establishing the doctrine. These include the Google Shopping[106], and Meta/Bundeskartellamt[107] cases. In Google Shopping, the CJEU ruled that given the particular circumstances linked to the nature of the infrastructures, Google abused its dominant position by favoring its proper services compared to those of its competitors. In Meta/Bundeskartellamt, the CJEU observes that the access to a massive amount of data creates entry barriers, coupled with the absence of real consent for the users, reinforces the dominant position of Meta. These reasons are particularly relevant as digital platforms have access to a large quantity of data, and are capable of shaping the conditions of exercise of freedom of expression.

This theoretical reflection should therefore be used as a tool for prospective analysis rather than positive law. And this tool allows us to assert that the law cannot ignore the grandiose power that private actors derive from the indispensable nature of the technological structures they possess.

Although it was not handed down by a supranational court, this idea is echoed in the CasaPound v. Facebook decision[108], in which the judge recognized that this social network performs a "public interest function" in the exercise of freedom of expression and can therefore be considered a "constitutionally constrained actor." In other words, this court implicitly follows the reasoning provided by the ECtHR in the Appleby ruling and applies it to the digital context. This decision foreshadows, in a way, the likely progress of European case law on freedom of expression and new technologies.

We are thus on the path to recognizing the quasi-public role of platforms. A second step was taken with the Delfi ruling[109], in which the ECtHR recognized that certain digital intermediaries are no longer neutral hosts, but organizers of online discourse. The Court held a news portal liable for hateful comments posted by users because of its effective technical control (deletion, filters). The doctrine undersigned that : "*Delfi is considered to have exercised a*

---

[105] R. Dacar, "The Essential Facilities Doctrine, Intellectual Property Rights, and Access to Big Data," *IIC – International Review of Intellectual Property and Competition Law* 54 (26 October 2023): 1487–1507.
[106] Court of Justice of the European Union (GC), Judgment of 10 September 2024, *Google LLC and Alphabet Inc. v. European Commission*, Case C-48/22 P, EU:C:2024:726, §146.
[107] Court of Justice of the European Union (GC), Judgment of 4 July 2023, *Meta Platforms Inc. and Others v. Bundeskartellamt*, Case C-252/21, EU:C:2023:537, §§ 132-134.
[108] Tribunale di Roma, *CasaPound v. Facebook*, Judgment of 14 February 2020, no. 80961/19.
[109] *Delfi AS v. Estonia*, *supra* note 68, §§113-117.

substantial degree of control over the comments published on its portal."[110] Indeed, *"The appellant held an economic interest in proactively inviting readers to publicly comment on articles, as the number of visits to the website depended on the number of comments, and the revenue earned from the advertisements published relied on the number of visits."*[111] This shows that private actors are active, as they play an intermediary role by moderating the content they sponsor. However, the more they moderate, the more responsible they become and the more they become private regulators of expression: responsibility becomes an indicator of power.

Twenty years later, after explaining that the owner of a Facebook account could open forums accessible to the public on the Internet[112], the ECtHR directly transposed its reasoning from the Delfi judgment[113] to a space of expression with which we are all familiar, in its Grand Chamber judgment, Sanchez v. France in 2023[114]. In this case, the applicant, the holder of a Facebook account for political purposes, had failed in his duties and responsibilities by not removing openly hateful comments posted by contributors on his wall[115]. The ECtHR concluded that, given the control he had, he had a duty to exercise vigilance[116]. Although the owner of the public account in question has an increased duty of vigilance due to his status as a politician[117], this judgment implicitly illustrates that platforms are no longer mere technical supports: they impose accountability on various actors. In other words, the ECtHR recognizes that platforms are not only places of expression[118] but also create obligations, generate normative power, and therefore raise the question of the responsibility of their actors. The Sanchez ruling thus extends Delfi to the era of social media.

This recognition of the normative power of private actors is not unique to the ECtHR. The CJEU's cases law highlight not only Facebook's power to control information[119], but also its structural informational power[120]. More specifically, in the first case, the CJEU ruled that EU law

---

[110] Lorna Woods, "*Delfi AS v Estonia: Grand Chamber Confirms Liability of Online News Portal for Offensive Comments Posted by Its Readers*," *Strasbourg Observers*, 18 June 2015, commentary on ECtHR (Grand Chamber), *Delfi AS v. Estonia*, appl. no. 64569/09, 16 June 2015, available at:https://strasbourgobservers.com/2015/06/18/delfi-as-v-estonia-grand-chamber-confirms-liability-of-online-news-portal-for-offensive-comments-posted-by-its-readers/?utm.

[111] Nathan Capone, "*Delfi v. Estonia: Increased risk of liability for online news portals*", *Fieldfisher – Defamation & Privacy Blog*, 16 July 2015 (commentary on the ECtHR (Grand Chamber) Judgment, *Delfi AS v. Estonia*, no. 64569/09, 16 June 2015), online: https://www.fieldfisher.com/en/services/dispute-resolution/defamation-and-privacy/defamation-blog/delfi-v-estonia-increased-risk-of-liability-for-online-news-portals?utm

[112] European Court of Human Rights (GC), *Sanchez v. France*, no. 45581/15, Judgment of 15 May 2023, §180.

[113] *Delfi AS v. Estonia*, *supra* note 68.

[114] S*anchez v. France*, *supra* note 112.

[115] Ibid. §§140-141, 163-168.

[116] Ibid. §187.

[117] Ibid. §§179-189.

[118] See Chapter 1.

[119] Court of Justice of the European Union, *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd*, C-18/18, Judgment of 3 October 2019 , EU:C:2019:821.

[120] *Meta Platforms Inc. and Others v. Bundeskartellamt*, *supra* note 107.

does not prohibit national authorities from ordering gatekeepers to remove not only the disputed content but also identical or equivalent content. In fact, she considered the regulation in force at the time of the case that : *"Directive 2000/31 (...) does not preclude a court of a Member State from (...) ordering a host provider to remove information (...) or to block access to that information."*[121] It cannot be circumscribed because moderation is extraterritorial and can be applied on a global scale. In other words, the power of moderation extends beyond the territory of the content author or gatekeeper. Furthermore**,** the Meta's ruling[122] recognizes that platforms have a considerable advantage due to the centralization of the data they process. We can deduce that, although the CJEU does not directly address content moderation[123], this structural power of platforms is based on algorithms that establish profiles and organize the dissemination of content, which, as we have seen, determine the visibility of each online expression.

This structural power comes from the fact that *"access to personal data and the fact that it is possible to process such data have become a significant parameter of competition between undertakings in the digital economy."*[124] The control of big data fuels the enormous power of private actors and their dominant positions, the effects of which extend beyond the competitive arena and, as we shall see, have an impact on our freedom of expression.

These two rulings usefully complement the previous analysis: they reveal a technical and algorithmic power that justifies the advent of specific European regulation. Together, the rulings of the European courts highlight the current reality of the technological world: platforms no longer merely host content, but control our freedom of expression through the moderation they operate. In doing so, they set the rules of the game and play a leading role in regulation. Under the guise of hosting conversations, they determine the conditions of access, amplification, and removal, thus assuming a quasi-police function in the digital public space, without the guarantees of transparency, proportionality, or judicial review that normally govern public action[125].

This "freedom of moderation," or freedom of editorial discretion[126], which is an attribute of their private autonomy, therefore comes into conflict with users' freedom of expression, which depends on how these moderation decisions are made and applied.

At this stage, as analyzed by Pierre Auriel and Mathilde Unger[127], the main concern is that the exercise and protection of freedom of expression are being delegated to private actors.

---

[121] *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd*, *supra* note 119.
[122] *Meta Platforms Inc. and Others v. Bundeskartellamt*, *supra* note 107.
[123] The main contribution of the judgment lies in acknowledging that access to a large volume of data may strengthen the dominant position of a network operator.
[124] *Meta Platforms Inc. and Others v. Bundeskartellamt*, *supra* note 107, §51.

[125] See Chapter 1, Section 1.2, on algorithmic influence and visibility as a condition for freedom of expression; and Chapter 1, Section 1.3, on the privatization of filtering mechanisms and the implicit responsibility of platforms.
[126] See, in particular, Jack M. Balkin, "*Free Speech Is a Triangle*," *Columbia Law Review*, 2018.
[127] Pierre Auriel and Mathilde Unger, *supra* note 15.

Because *"beyond this specific case, certain voices—and therefore certain points of view—could be silenced due to arbitrary moderation or moderation motivated not by the pursuit of the public interest or the protection of the rights of others, but by the economic, strategic, or political interests of the companies that own online platforms."*[128]

The question is no longer whether platforms wield power, but how that power should be regulated. What's more, the authors also note that *"in court, users can hardly invoke freedom of expression"*[129] to challenge platform decisions, as these fall under simple contractual relationships between private actors.

This is precisely the logic behind the new European digital law: recognizing the systemic influence of platforms and organizing their responsibility, but without explicitly entrusting them with a public service mission or imposing general control over speech, as the CJEU has warned that the removal obligation does not require the hosting service provider to carry out a general monitoring obligation[130]. The DSA, GDPR, DMA, and AI Act thus form a hybrid set of regulations, oscillating between accountability and democratic caution. It is this framework, and the tensions it reveals, that this subsection proposes to analyze.

2. The European regulatory framework: between accountability and freedom-killing

The phenomenological observation of the benefits and negative impacts of new technologies established in the first chapter, as well as the jurisprudential recognition of the transformation of the role of private intermediaries into true organizers of public debate, brought about, as we have seen, by moderation, algorithmic personalization, and massive data processing, has led the EU to begin constructing a regulatory framework. It is aware that the balance of power between private actors and users is, without euphemism, profoundly unbalanced and asymmetrical.

The DSA, GDPR, DMA, and, more recently, the AI Act form the new regulatory pillars for holding owners of new technologies accountable, indirectly protecting freedom of expression and privacy. The challenge is to regain control over the rules of expression, over which private actors had previously had unlimited power, without democratic oversight. This is an ambitious undertaking, to say the least, in an archaic context where the logic of technological solutionism

[128] Ibid.
[129] Ibid.
[130] *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd, supra* note 119.

still prevails. This concept has been summed up in a phrase attributed to Dennis Gabor and popularized by Marc Dugain and Christophe Labbé, among others: *"Everything that is technically feasible must be done, whether it is considered morally good or reprehensible."*[131] Indeed, the ideology inherited from Silicon Valley in the 2000s is based on the philosophy of moving fast, conquering, and experimenting. The watchwords of the technological era are therefore innovation and gaining an advantage over competitors, regardless of the disastrous social, political, or democratic consequences. Once again, we can take Mark Zuckerberg as an example, who, in relation to Facebook, claimed as his mantra: "Move fast and break things."[132] The dominance of technological solutionism is a result of market logic: innovation has economic value, and massive data collection is the driving force behind digital capitalism.

However, this view is not universally shared, with some criticizing this egocentric maxim that worships technological advancement. Some voices remind us that just because a device becomes technically possible does not necessarily mean it should be used[133]. This is precisely the path that the EU intends to follow: caution in the face of technological advances, ethical oversight without limitation.

But it is not simple. This race, in which too little attention is paid to collateral damage (particularly to freedom of expression), highlights the difficulty of our era and that of the EU: how can we regulate new technologies, digital systems designed specifically to evolve and perform their tasks at an unprecedented speed that exceeds that of the formation of law? What's more, does it tackle the root of the problem, namely the structural change in expression brought about by new technologies, or only its effects and consequences? Does it call into question the economic model of attention capture, algorithmic ranking, the hidden economy behind mass data collection?[134]

In order to determine the effectiveness of the European framework, we will attempt to answer the following questions. How does the DSA respond (or not) to the problem of filter bubbles? Does the GDPR protect against capitalist surveillance? Does European regulation provide a framework for algorithmic governmentality? What proposals are there for democratic governance? The aim will be to evaluate the solutions and propose potential improvements.

---

[131] This idea is commonly attributed to Dennis Gabor, although the wording used here is not a verbatim quotation; see in particular Marc Dugain and Christophe Labbé, *supra* note 6.

[132] Mark Zuckerberg, statements reported, inter alia, in *Wired*, "*Facebook's Hacker Way*," 2014.

[133] See, in particular, Paula Forteza, *L'utilisation des nouvelles technologies par les pouvoirs publics* [*The Use of New Technologies by Public Authorities*], Fondation Jean-Jaurès, 2021.

[134] See Chapter 1, on *surveillance capitalism*, drawing in particular on Shoshana Zuboff, *The Age of Surveillance Capitalism.*

2.1. The Digital Services Act

Firstly, the EU is attempting to respond to this structural change through the Digital Services Act (hereinafter DSA) established by Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19, 2022. Its purpose is to *"contribute to the proper functioning of the internal market for intermediary services by establishing harmonized rules for a safe, predictable, and reliable online environment that facilitates innovation and in which the fundamental rights enshrined in the Charter (...) are effectively protected."*[135]. In other words, it aims to prevent platforms from *"setting the rules of the game on their own"*[136] *by organizing "the information space with clearly defined rights, obligations, and guarantees."*[137]

It is because it directly affects the core of freedom of expression by establishing a parallelism whereby what is illegal offline is illegal online[138] that it should be analyzed first. Although it does not address the root causes, it seeks to regulate the effects of the power held by a few private owners by making them accountable. It also aims to combat the dissemination of illegal or harmful content such as child pornography, disinformation,...[139] The objectives[140] are therefore multiple:

1. protect European citizens online and their fundamental rights;
2. help the smallest businesses in the EU to grow;
3. establish democratic control and oversight of very large platforms;
4. mitigate systemic risks (manipulation of information, …)[141].

Aware of the moderating, hierarchizing, amplifying, or invisibilizing power over the speech of private actors, the EU seeks, through the DSA, to act through the transparency of this "private police force."

This regulation, which came into force on February 17, 2024, applies to *"to intermediary services*[142] *offered to recipients of the service that have their place of establishment or are located in the Union"*[143] *while making a specific distinction for the "very large online*

---

[135] Digital Services Act, Art. 1.
[136] Thierry Breton, "*The Digital Challenges Facing Our Democracies Are Global*," *FigaroVox*, 10 January 2021.
[137] Ibid.
[138] European Commission, *Digital Services Act: Ensuring a Safe and Accountable Online Environment*, 2022, available at: https://www.vie-publique.fr/eclairage/285115-dsa-le-reglement-sur-les-services-numeriques-ou-digital-services-act#quels-sont-les-objectifs-du-r%C3%A8glement-dsa.
[139] Ibid.
[140] Digital Services Act, recital 9: *"This Regulation fully harmonises (...) in the Charter are effectively protected and innovation is facilitated."*.

[141] Ibid.
[142] Digital Services Act, recital 13.
[143] Digital Services Act, art. 2(1).

platforms", while making a specific distinction for "very large online platforms."[144] This includes, in particular: internet service providers (ISPs), cloud computing services, online platforms[145] such as marketplaces, app stores, social networks, content-sharing platforms, travel and accommodation platforms, very large online platforms and very large search engines, used by more than 45 million Europeans per month, as designated by the European Commission[146].
As of April 25, 2023, the largest platforms include: AliExpress, Amazon Store, Apple AppStore, Bing, Booking, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Wikipedia, X (formerly Twitter), YouTube, and Zalando[147].

This horizontal regulation on intermediaries, i.e., it regulates the role of hosting providers, platforms, VLOPs, and VLOSEs, succeeds and complements the e-commerce directive of June 8, 2000[148], by ensuring that the limited liability of platforms[149] is maintained and establishes the principle of prohibiting general surveillance[150]. By directly regulating content moderation, the DSA is the first European text to proceduralize the removal, reduction, and restriction of content, and the first text to impose transparency obligations on private moderators.

It seems that European lawmakers are not removing platforms' power to organize and filter content, but rather are proceduralizing the conditions under which this power is exercised.
More specifically, although the DSA does not directly regulate the relationship between new technologies and freedom of expression, unlike other European responses, its authors originally intended it to ensure the proper functioning of the internal market for digital services[151], and it is useful to this freedom in three ways.

Firstly, Article 16 of the DSA establishes a notification and appeal mechanism called "notice and action" for illegal content. The idea is that when users report content, platforms have an obligation to act "as soon as possible." However, to ensure that there is no arbitrary removal or invisible "shadow banning," this obligation is accompanied by another: the obligation to

---

[144] Digital Services Act, arts. 19 and 33.
[145] Digital Services Act, art. 3(i): : *"'online platform' means a hosting service that, at the request of a recipient of the service (...) and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation;".*
[146] Digital Services Act, arts. 33(1) and (4); see also *Vie-publique*, "*DSA: the Digital Services Act*," explanatory brief:
https://www.vie-publique.fr/eclairage/285115-dsa-le-reglement-sur-les-services-numeriques-ou-digital-services-act#quels-sont-les-objectifs-du-r%C3%A8glement-dsa
[147] European Commission, *Commission designates first set of Very Large Online Platforms and Very Large Online Search Engines under the Digital Services Act*, Press Release, 25 April 2023, online: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.
[148] Digital Services Act, recitals 9 and 10, concerning the partial replacement of Directive 2000/31/EC (*E-Commerce Directive*).
[149] Digital Services Act, arts. 4, 5 and 6.
[150] Digital Services Act, art. 8.

[151] Digital Services Act, art. 1(1).

provide a statement of reasons[152] for each decision. This statement must include information on the legal or contractual basis, the nature of the measure, and the possible remedies. It should be noted that general monitoring is not possible. Finally, the DSA does not specify which expressions should be removed or restricted, but rather organizes how platforms are supposed to handle notifications of illegal content.

These reporting and cooperation obligations did not exist in the era of the e-commerce directive. From now on, with the notice tool, the DSA requires platforms to set up a tool enabling users to report illegal content[153]; once the report has been made, they are obliged to remove this content or quickly block access to it[154]. The DSA has also attempted to rebalance the relationship between private actors and users by creating a new role for "trusted flaggers." Regulators must cooperate primarily with individuals in this role[155]. In this way, the EU is formalizing and systematizing moderation.

The ability for users to report content, or giving so much power to a small group of individuals (trusted flaggers), although it seems essential given the massive amount of content to be analyzed and evaluated, reinforces the privatization of information sorting without any guarantee of neutrality. And that is what is dangerous: the DSA legitimizes the delegation of quasi-public power.

This is not without risk. Several analyses argue that the DSA could not only neutralize the power of private actors but also encourage them to over-censor: to avoid sanctions, platforms could preemptively remove reported lawful content[156]. In fact, in case of serious negligence, *" the very large online platform or of the very large online search engine concerned fines not exceeding 6 % of its total worldwide annual turnover in the preceding financial year.*"[157] The fear of such financial penalties inadvertently encourages platforms to exercise extreme caution, which can have a chilling effect and prompt them to withdraw content as a precautionary measure. Romain Badouard summed this up well when he said: *"The measures adopted are criticized because of the threats they pose to the freedom of expression of Internet users: the pressure exerted on platforms would lead them to over-censor, removing legitimate content for fear of facing financial penalties if they do not comply within the allotted time."*[158] In other

[152] Digital Services Act, art. 17.
[153] Digital Services Act, recital 12.
[154] Vincent Lequeux, "*Digital: What Are the DMA and the DSA, the European Regulations Aiming to Regulate the Internet?*," *Toute l'Europe*, overview article, 5 December 2025. https://www.touteleurope.eu/societe/numerique-que-sont-le-dma-et-le-dsa-les-reglements-europeens-qui-visent-a-reguler-internet/.
[155] Ibid.

[156] Pierre Auriel and Mathilde Unger, *supra* note 15.
[157] Digital Services Act, art. 74(1).
[158] Romain Badouard, "*Ce que peut l'État face aux plateformes*," *Pouvoirs* 177, no. 2 (2021): 49–58, https://droit.cairn.info/revue-pouvoirs-2021-2-page-49?lang=fr.

words, even if well-intentioned, the DSA encourages private actors to remove content too quickly and too often.

The notice and action mechanism could also lead to excessive limits on expression, since ultimately nothing prevents users from reporting content that is not problematic and is protected by the Charter.

Given the massive number of notifications, it may seem appealing to platforms to automate removals in order to remain compliant, and thus favor a categorical algorithm over a human capable of nuance: *"two possible outcomes of how the online content-sharing service providers will retort notice outbursts: 1) to apply automatic content blocking once the user has notified the content; and, 2) to apply algorithmic content moderation regarding the notified content."*[159]

One thing leading to another, an obligation designed to regulate moderation powers may, in fact, create a risk of over-blocking (= excessive algorithmic removal of lawful content), but the installation of notice-and-action mechanisms *"creates a possibility of abusive notifications and subsequent automated content over-blocking."*[160]

Secondly, this regulation also indirectly protects freedom of expression by making platforms accountable through a duty of care. In short, intermediaries must put in place measures to prevent and remove illegal content, ensure the traceability of sellers.

But, in the interests of balance and to avoid preventive censorship, their liability is limited: private owners cannot be held automatically liable a priori for content posted by their users. Once again, the EU is careful not to introduce widespread filtering.

As this limited liability mechanism already exists under the e-commerce directive, the real contribution of the DSA is the addition of a set of procedural obligations to prevent arbitrary decisions by private economic actors: detailed reasoning for decisions, information for users, creation of internal and external appeal mechanisms, increased transparency in the terms of service[161], and the establishment of a public database containing all moderation decisions. Whereas the e-commerce directive was content with a general principle of limited liability, the DSA builds a comprehensive due diligence framework. These two injunctions are essential "*to ensure a safe, predictable, and reliable online environment and to enable EU citizens and others*

---

[159] Stefan Kulk, *Internet and Intermediaries and Copyright Law: Towards a Future-proof EU Legal Framework* (Alblasserdam: Ridderprint, 2018).

[160] Jörg Wimmers, "*The Out-of-court Dispute Settlement Mechanism in the Digital Services Act: A Disservice to Its Own Goals*," *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)* 12, no. 4 (2021): 427.

[161] Digital Services Act, art. 3(u): *"'terms and conditions' means all clauses, irrespective of their designation or form, which govern the contractual relationship between the providers of intermediary services and the recipients of the service."*.

to exercise their fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union, in particular freedom of expression and information."[162]

Thirdly, another new feature of the DSA compared to its predecessor is a requirement for transparency and information regarding the use of algorithms and targeted advertising. This means that targeting individuals based on sensitive data (religion, sexuality, political opinions, health) is prohibited[163], as is targeted advertising aimed at minors[164]. In other words, the recommendation system[165] used by very large platforms/search engines must be explained. And, since profiling is not directly permissible, they must offer an alternative system that is not based on it.

This transparency is not limited to the platform-user relationship. Article 42 requires platforms to publish detailed transparency reports on their moderation activities such as: the human resources that the provider of very large online platforms devoted to content moderation, the number of complaints. Article 40, meanwhile, gives coordinators for digital services in each Member State access to data from very large platforms. This opens up the possibility of scientific monitoring of the impact of their algorithms on the flow of information and public debate.
As emphasized by Tarleton Gillepsie : "*the workings of content moderation at most social media platforms are shockingly opaque, and not by accident*"[166], so, "*the labor, the criteria, and the outcomes are almost entirely kept from the public."*[167] In other words, even when reinforced, transparency remains partial: algorithmic mechanisms escape external control. Indeed, the transmission of such information does not allow us to understand how new technologies actually work: hierarchization, visibility, and so on remain unknown. The DSA is a step forward because it makes procedures more accountable, but it does not make transparency a lever for democratizing the governance of freedom of expression.

Furthermore, with a view to striking a balance between protecting users' fundamental rights and promoting the market, the DSA introduces specific enhanced obligations for VLOPs and VLOSEs. VLOPs/VLOSEs are defined as those with more than 45 million monthly active users[168].

---

[162] Digital Services Act, recital 3.
[163] Digital Services Act, art. 26(3).
[164] Digital Services Act, art. 28.
[165] Digital Services Act, art. 3(s): *" 'recommender system' means a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed;".*

[166] Tarleton Gillespie, *supra* note 5, 199, citing Mikkel Flyverbom, "*Digital Age Transparency*."
[167] Ibid.
[168] Digital Services Act, art. 33.

Article 34 introduces annual risk assessments: they must annually identify, analyze, and evaluate the systemic risks associated with the design or use of their services, such as any negative or foreseeable effects on the exercise of fundamental rights (Art. 34, 1b). They must pay particular attention to structural factors such as the design of recommendation systems, content moderation practices, terms and conditions and their enforcement, advertising systems, and data collection and use practices.

Meanwhile, article 35 requires reasonable, proportionate, and effective risk mitigation measures to be taken, tailored to specific systemic risks. For example, this could involve modifying the design of the interface or adjusting moderation (speed, quality,...)[169]. This article in particular emphasizes the need to take into account the impact of these measures on fundamental rights, demonstrating the importance of protecting them, including freedom of expression. The article 36 which establishes a crisis response mechanism complements it.

Finally, article 37, a requirement for independent audits at least once a year to assess compliance with their obligations under the DSA and their commitments in codes of conduct. They must then implement these recommendations or justify why they are not doing so. Once again, this is a good idea, but it emphasizes procedural compliance rather than genuine protection of freedom of expression: "*The DSA does not set harmonised rules for risk assessments and there is still no consensus on what constitutes a high-quality impact assessment… impact assessments do not become merely a formality*."[170]

Ultimately, "*the set of procedural rules governing the actions of platforms under European law does not prevent their freedom of moderation, encouraged by legislation, from acquiring legal status, at the expense of possible challenges from users." [171]*

In other words, the DSA does not remove platforms' role as "private police" of freedom of expression; it regulates the way platforms moderate, prioritize, and remove content. Admittedly, it makes the decisions of tech giants more visible, more justiciable, and more contestable, but it does not affect the algorithmic architecture built to encourage user engagement, nor does it strip them of their power over freedom of expression.

[169] Digital Services Act, art. 35(1).
[170] European Center for Not-for-Profit Law (ECNL) & Access Now, *Towards Meaningful Fundamental Rights Impact Assessments under the DSA*, Summary (2023), online: https://www.accessnow.org/wp-content/uploads/2023/09/DSA-FRIA-joint-policy-paper-September-2023.pdf.
[171] P. Auriel et M. Unger, *supra* note 15.

2.2. The GDPR

Secondly, the EU has a second lever, this time indirect: the GDPR. This regulation 2016/679, which came into force in 2018[172], aims to establish *"rules on the protection of natural persons with regard to the processing of personal data and rules on the free movement of such data."*[173] The idea is that protecting personal data and privacy is tantamount to protecting freedom of expression, as these rights are interdependent.

In this regard, the CJEU[174] admitted that a norm which aims to 'establish a continuous, non-targeted and systematic surveillance regime' through the processing of data concerning an unselected set of individuals constitutes an interference of a serious 'gravity' with fundamental rights. The CJEU points out that such a measure could only be authorised under very strict conditions, notably: the storage period must not exceed what is necessary for the pursued objective, and the data processing cannot be general but targeted. This reasoning is particularly relevant for what it permits to conclude about ChatControl as it would replicate the measure which was held here by the Court to be incompatible with fundamental rights. More generally, with this reasoning, the CJEU implicitly recognized that surveillance induces chilling effects.

As Mireille Hildebrandt said:*"Privacy is not merely a private interest, but also a public good, and notably for the substance of intellectual privacy that is closely related to the freedom of information, and to the capability to develop a mind of one's own regarding matters of personal and public interest."*[175]

These rights are therefore interdependent because the protection of privacy and personal data is a prerequisite for freedom of expression in the digital age. In other words, this refers back to the idea of the panopticon developed in Chapter 1: if people feel that their data is protected, they will not be afraid to express what they really think. What's more, the protection of personal data limits profiling and manipulation, with targeted advertising allowing for expression that is more faithful to ideals and true values. Consequently, if individuals do not trust private actors' use of their data, if they feel monitored and their data inferred, they will adjust their behavior[176]. As Daniel Solove has shown, "*Whether in public or in private, government surveillance can chill*

---

[172] Vie-publique.fr, *"DSA: the regulation on digital services – objectives and scope"*, *éclairage*, official administrative information site, 4 August 2025, online: https://www.vie-publique.fr/eclairage/285115-dsa-le-reglement-sur-les-services-numeriques-ou-digital-services-act#quels-sont-les-objectifs-du-r%C3%A8glement-dsa.

[173] General Data Protection Regulation, art. 1(1).

[174] Court of Justice of the European Union (GC), *Ligue des droits humains ASBL v Conseil des ministres,* C-817/19, Judgment of 21 June 2022, EU:C:2022:491.

[175] Mireille Hildebrandt, "*Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*," *Theoretical Inquiries in Law* 20, no. 1 (2019): 83–121.

[176] See more Chapter 1.

speech, dissent, and association; it provides great power to the watchers; it can be abused."[177] while Neil Richards reminds us that *"surveillance is harmful because it can chill the exercise of our civil liberties" because "surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues."*[178] In truth, the misuse of data has a direct impact on informational[179] self-determination, which is a prerogative of freedom of expression. However, as the German Constitutional Court stated as early as 1983, *"In the context of modern data processing, the free development of one's personality therefore requires that the individual be protected against the unlimited collection, storage, use and sharing of their personal data.*"[180] Indeed, as Shoshana Zuboff[181] explains, surveillance erodes the possibility of free expression by shaping the conditions under which individuals form beliefs and preferences[182]. Surveillance transforms our thinking, and therefore what we express. Moreover, as privacy is not simply an individual right; it is a structural condition of democratic speech[183], privacy is not only a right interdependent with that protected by Articles 10 of the ECHR and 11 of the CFREU, but it is a structural condition of freedom of expression.[184] As De Hert and Papakonstantinou[185] point out, the GDPR is a cause for celebration for human rights, as it strengthens individual control over personal data and the accountability of data controllers. Thus, it is because it contributes to consolidating the conditions for the effective exercise of fundamental freedoms[186] that the degree of protection it affords to freedom of expression should be assessed.

The GDPR helps in the protection of freedom of expression through several principles : data minimisation[187], transparency[188], and purpose limitation[189] but also through two rights : right to object[190], rights related to automated individual decision-making, including profiling[191].

---

[177] Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (New Haven and London: Yale University Press, 2011), 180.
[178] Neil M. Richards, "*Intellectual Privacy*," *Harvard Law Review* 126 (2013): 1935.
[179] Suzanne Vergnolle, *supra* note 7.

[180] German Federal Constitutional Court (Bundesverfassungsgericht), *Census Act Case* (*Volkszählungsurteil*), Judgment of 15 December 1983, recognising the constitutional right to informational self-determination.
[181] Shoshana Zuboff, *supra* note 3.
[182] Ibid.
[183] Ibid.
[184] Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven and London: Yale University Press, 2012), https://doi.org/10.12987/9780300177930.
[185] Paul De Hert and Vagelis Papakonstantinou, "*The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?*," *Computer Law & Security Review* 32, no. 2 (2016): 179–194, https://doi.org/10.1016/j.clsr.2016.02.006.
[186] Ibid.
[187] General Data Protection Regulation, art. 5(1)(c).
[188] General Data Protection Regulation, arts. 14 and 15.
[189] General Data Protection Regulation, art. 5(1)(b).
[190] General Data Protection Regulation, art. 21.
[191] General Data Protection Regulation, art. 22.

By asking for personal data to be adequate (e.g sufficient to fulfill the specific purpose for which it is being processed), relevant (e.g have a direct connection to the purpose) and limited to what is necessary (e.g the minimum amount of data needed to achieve the purposes for which they are processed), the GDPR reduce the raw material of profiling and of the algorithmic customization[192].

In fact, this principle helps avoid private actors becoming omniscient, thus, data minimization functions as a structural limit on the accumulation of power by data controllers. Without such constraints, informational asymmetries grow, enabling subtle forms of control[193]. This principle protects the autonomy of the functional freedom of expression by constituting a bulwark against algorithmic ingenuity. To sum up we can say that : less data > less targeting > less inferences > less manipulation.

By asking for transparency, as the DSA, does e.g. that individuals can easily locate and understand information that must be provided about their data processing in clear, plain language and in a timely manner, the GDPR to reduce the opacity of the personal data process. In fact, data controllers must inform individuals about notably the data collected, the purposes of the processing, the recipients, their rights. This gives users direct visibility into the effects that new technologies have on the dissemination of their ideas and the visibility of their content. Some even see this principle as a counterweight to the power of private actors, as is the case with O. Lynskey[194], who asserts that data protection law functions as a counterweight to the informational power of digital platforms by forcing them to disclose practices that would otherwise remain invisible[195].

Moreover, transparency is a prerequisite for contestation. Indeed, in order to contest data processing and its effects (targeted advertising,...), one must first be aware that it exists. It therefore becomes a factor that promotes and facilitates recourse for non-compliance with the rights protected by the Charter, from privacy to freedom of expression.

Transparency therefore protects freedom of expression in two ways: it allows users to understand why certain content is shown or hidden from them, thereby reducing invisible information bubbles, a phenomenon described in Chapter 1, and it limits to a certain extent the harmful effects of new technologies, such as surveillance and manipulation. By providing evidence that can be used in legal proceedings, it makes it possible to criticize the practices of platforms.

---

[192] Minimization principle.

[193] Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven and London: Yale University Press, 2012), https://doi.org/10.12987/9780300177930.

[194] Orla Lynskey, "*Complete and Effective Data Protection*," *Current Legal Problems* 76 (2023): 297–343, Advance Access published 10 October 2023, https://doi.org/10.1093/clp/cuad009.

[195] Ibid.

However, the effectiveness of the GDPR in protecting freedom of expression remains debatable, since, like the transparency established by the DSA, that enshrined in the GDPR also remains formal and easily circumvented. It also remains primarily informational and does not explain the algorithmic mechanisms in concrete terms.

It is not only certain principles established by the GDPR that are favorable to expression, but also the right to object and the regulation of profiling and algorithmic personalization. The former allows users to challenge the processing of their data when it is carried out for reasons of public interest or based on the legitimate interests of the controller. On paper, this right is a tool for data protection and therefore indirectly for the protection of expression. Indeed, by being able to prevent certain processing, data subjects can limit advertising targeting, personalization, and profiling, and thus mitigate the influence that new technologies have on information.

Nevertheless, this right is not absolute. The GDPR specifies that this right can only be invoked for reasons related to the specific situation of individuals. It is understood that the individuals concerned must justify the exercise of this right, which is therefore not automatic, limiting the scope of this right. It is common, yet complicated for users to challenge the legitimate interest of a data controller, since, as the doctrine[196] reminds us, the right to object is weakened by the broad margin of appreciation left to controllers invoking legitimate interest. This reinforces the power asymmetry in favor of platforms. This right remains fully enforceable to oppose commercial prospecting. Admittedly, it works on profiling and therefore acts sporadically on it, but that is not enough. This does not prevent intensive profiling or profiling for other purposes, or even profiling of those who do not exercise this right due to ignorance.

Ultimately, the rights to object and restrict processing remain difficult to exercise in practice due to the opacity of processing and the extent of information asymmetries[197]. Admittedly, this right is a step towards better protection of our fundamental rights, but as long as the adage "*If you don't pay for something, you're not the customer, you're the product"* remains true, this protection remains largely theoretical. Indeed, the current framework relies on the responsiveness of individuals, in which it is up to the people concerned to react to the giants of the technological world rather than them changing their strictly economic vision and not abusing the collection and processing of data. Moreover, how can you get a product to react when it doesn't even realize it is a product? How can you stand up to massive, incessant, and not-so-transparent data collection?

[196] Orla Lynskey, *supra* note 194.
[197] See, in particular Paul De Hert and Vagelis Papakonstantinou, *supra* note 185.

There is a clear disproportion between the proposed solution and the problem: individual rights are ill-suited to address systemic harms produced by data-driven platforms[198]. In other words, the GDPR offers a micro tool to respond to a macro problem: the GDPR limits certain excesses, but does not challenge the massive collection of data that fuels the attention economy[199].

One might think that Article 22, by establishing the right not to be subject to a decision based solely on automated processing, including profiling, mitigates the criticism developed above. However, these two limitations significantly reduce its scope. Indeed, such processing can only be challenged when it produces legal effects or similarly significant effects.

The main negative effects of new technologies on freedom of expression are therefore not affected. Ultimately, most algorithmic decisions shaping online environments fall outside the scope of Article 22, despite their profound influence on individuals' opportunities and worldviews, as Teo so aptly summarized: *"social media algorithms that nudge and filter content personalised and tailored to the individual might mean that one is increasingly unable tell whether one is being manipulated[200] nor discern the commercially driven business model behind content curation[201] that increasingly enable the shaping of worldviews."*[202] It is therefore understandable that decisions that shape the visibility of information fall outside the scope of this right.

In addition, what is often overlooked by most, but not by private actors, is that the decision must be fully automated, i.e., algorithmic decision making refers to the use of algorithms to automate choices or recommendations that would otherwise require human judgment. However, platforms are well aware of this and easily circumvent European obligations. As a result, many influential algorithmic systems fall outside the scope of EU regulations because formal minimal human involvement is sufficient to avoid classification as fully automated decision-making. They do this by justifying the processing on the basis of contractual necessity or, strategically, by adding some minimal human intervention ("human-in-the-loop"[203]) to avoid having to answer for this right. Thus, a reading of the entire body of doctrine shows that, in practice, human intervention is largely illusory, as the opacity and

---

[198] See, in particular, Orla Lynskey, *supra* note 194.
[199] Shoshana Zuboff, *supra* note 3.
[200] Daniel Susser, Helen Nissenbaum, and Beate Rössler, "*Online Manipulation: Hidden Influences in a Digital World*," *Georgetown Law Technology Review* 4 (2020).
[201] Shoshana Zuboff, *supra* note 3.
[202] Szu-Yu Teo, "*Artificial Intelligence and Its 'Slow Violence' to Human Rights*," *Human Rights Review* (2024), https://doi.org/10.1007/s43681-024-00547-x.
See also: Seth Flaxman, Sharad Goel, and Justin M. Rao, "*Filter Bubbles, Echo Chambers, and Online News Consumption*," *Public Opinion Quarterly* 80 (2016): 298–320, https://doi.org/10.1093/poq/nfw006.
[203] Rebecca Crootof, Margot E. Kaminski, and W. Nicholson Price II, "*Humans in the Loop*," *Vanderbilt Law Review* 76, no. 2 (2023): 429.

complexity of machine-learning systems render this control ineffective[204]. Even when processing falls within the scope of this right, its impact is limited, as it does not prevent processing but merely imposes safeguards[205].

More generally, the GDPR does not protect against the fiction of consent, meaning, for example, that the practice of dark patterns (= manipulative interfaces) remains commonplace, or that *"Most people do not read privacy notices"*[206]; privacy self-management is an illusion, and consent, presented as free, is ultimately not free. This further diminishes the real impact of this regulation on freedom of expression.

Ultimately, the GDPR is similar to the DSA: neither is sufficient to protect freedom of expression. Admittedly, the transparency they establish makes data controllers procedurally accountable, but they do not address filter bubbles, engagement-based ranking, attention capture, recommendation mechanisms, engagement logic. Nevertheless, it is the most ambitious effort to date in the attempt to rebalance the asymmetrical forces between users and platforms, restoring to individuals a part of their freedom of self-determination.

2.3. The Digital Markets Act

At present, it is appropriate to analyze a third European instrument: the Digital Markets Act, which tackles the very structure of the digital market dominated by major platforms in order to make it fairer and more contestable. The EU therefore has another indirect lever: Regulation 2022/1925. This regulation aims to better frame the economic activities of the largest platforms[207]. These large companies are described as gatekeepers, which *"are large digital platforms providing so-called core platform services, such as online search engines, app stores, and messenger services."*[208][209] More specifically, the DMA lays down a set of clearly defined criteria to identify these "gatekeepers"[210] and then sets out do's (i.e. obligations) and don'ts (i.e. prohibitions) listed in the DMA. Thus, unlike the DSA, it does not regulate content moderation

---

[204] Lilian Edwards and Michael Veale, "*Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*," *Duke Law & Technology Review* 16 (2017): 18–84.
[205] Ibid.
[206] Daniel J. Solove, "*Privacy Self-Management and the Consent Dilemma*," *Harvard Law Review* 126 (2013): 1880–1903.
[207] Digital Markets Act, art. 1(1); see also *Toute l'Europe*, "*Digital: What Are the DMA and the DSA, the European Regulations Aiming to Regulate the Internet?*," 2022, available online: https://www.touteleurope.eu/societe/numerique-que-sont-le-dma-et-le-dsa-les-reglements-europeens-qui-visent-a-reguler-internet/.
[208] European Commission, *Digital Markets Act – About the DMA*, official website of the European Commission, available online: https://digital-markets-act.ec.europa.eu/about-dma_en.
[209] See definition: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (*Digital Markets Act – DMA*), Articles 2(1) and 3.
[210] European Commission, *supra* note 208.

or data processing, but rather the economic practices of private platforms. The DMA is therefore first and foremost an ex ante competition law tool.

However, given that access to information and the main spaces for expression depend on gatekeepers, regulating their economic model is sensible and useful to a certain extent. By contributing to this regulation, the DMA has an impact on the conditions of access and the actual exercise of expression within the spheres of public discourse. The inseparability of this regulation of the economic and informational power of platforms has been highlighted in particular by Tarleton Gillespie. For her, economic dominance enables the latter[211]. Shoshana Zuboff[212], for her part, asserts that the concentration of surveillance assets gives platforms an unparalleled capacity to shape knowledge, opinion, and discourse[213].

Although once again this European response is not purely focused on the relationship between new technologies and freedom of expression, conditioning competition has structural effects on freedom of expression, which is why it is relevant to study it in the context of the relationship between new technologies and freedom of expression.

To this end, we will analyze the main obligations and prohibitions that the DMA imposes on gatekeepers in order to assess the extent to which they promote genuine freedom of expression.

By requiring interoperability of messaging services under Article 7, the DMA indirectly promotes plurality of channels of expression[214]. This obligation means allowing different services to work together. It implies the possibility for internet users to chat across different applications[215]. For example: Instagram to Messenger. This ability to enable dialogue between services that were previously deliberately compartmentalized and closed off makes it possible to counteract the network effect. The idea behind this concept is that the more users a platform has, the more indispensable it becomes, and therefore, not using it means excluding oneself from public and social debate. This idea is well known to tech players, who have exploited it by building closed ecosystems, thereby blocking their dominant position in the market. The Commission has described this strategy as aimed at "preventing the opening up of markets." This article aims to thwart the plans of these few major players and thus reduces dependence on the main platforms. Thus, through this obligation, the DMA has an indirect incidence on freedom of expression by promoting pluralism in information channels. Users have the opportunity to use

[211] Tarleton Gillespie, *supra* note 5
[212] Shoshana Zuboff, *supra* note 3.
[213] Ibid.
[214] Digital Markets Act, art. 7 and recitals 55 and 57.
[215] Mathilde, *Que va changer le Digital Markets Act en pratique ? Passer d'un Mac à un PC tous les jours si je veux*, 23 March 2023, https://next.ink/1221/que-va-changer-digital-markets-act-en-pratique/.

new communication technologies that are healthier, protect their freedom, and have fewer harmful effects[216].

Next, by requiring gatekeepers to provide access to data generated by user companies[217], if requested, and prohibiting them from using that same data, at least data that is not publicly available[218], the asymmetry is rebalanced somewhat. It is no longer the owners of the technology who have access to all of this data without sharing it, but the companies concerned by it. This data relates to transactions, audiences, the performance of their content and/or products, consumer usage, and so on. In this way, the DMA substitutes a small part of the power held by the major economic players and gives control over the visibility of information to those who have a direct use for it. For example, without access to this data, creators (journalists, NGOs, artists, political parties,..) cannot understand why their expression is amplified or made invisible. This limits the opacity of recommendation practices and reduces dependence on an intermediary that presented itself as omniscient. Indeed, informational lock-in, i.e., the lack of access to data, made it impossible to leave the platform without losing one's audience.

The regulation also includes prohibitions that impact freedom of expression. For example, Article 6(5) of the DMA prohibits self-preferencing, meaning that a gatekeeper must not treat services and products offered by itself more favorably than similar services or products of a third party. This practice distorts access to information by directing visibility towards certain content and thus favoring it. By prohibiting this practice, the regulation ensures that expression receives the visibility it deserves. It is clear that the DMA helps to limit the power of digital giants. Thus, by acting on their economic power through competition regulation, the EU is promoting greater freedom of expression. Consequently, any measure that reduces structural dependence on gatekeepers promotes, to a certain extent, greater diversity of spaces and therefore gives people the choice of a wider range of forums in which to express themselves.

Although the DMA acts at the economic level and therefore tackles the root of the problem, its contribution to protecting freedom of expression remains very limited. Four main criticisms can be made:

1. The DMA does not tackle the business model of these tech players, nor does it directly challenge targeted advertising, profiling, engagement-based ranking, or ultimately the problems described in Chapter 1. Finally, as Van Waerdt points out: *"The digital market*

[216] See Chapter 1, Sub-Chapter 2.
[217] Digital Markets Act, art. 6(10).
[218] Digital Markets Act, art. 6(2).

already features exceedingly strong incumbent and first-past-the-post advantages, even without actual anti-competitive conduct."[219]

2. Admittedly, in theory, the DMA should increase the number of competitors and, to the same extent, the forums for expression. In practice, on the contrary, such diversification is not guaranteed.
3. As with the application of the DSA, private actors could ensure formal compliance with their obligations and prohibitions[220], for example, access to data for the companies concerned could be restricted to the bare minimum. Once again, they could circumvent its application via the "human in the loop" mechanism or fail to give competitors a real opportunity to interact with the platform by limiting bandwidth, ultimately neutralizing the possibility through design.

2.4. The AI Act

Fourthly, the EU also has the AI Act as a tool for dealing with new technologies, specifically artificial intelligence and its owners. Regulation 2024/1689 was adopted on March 13, 2024, to promote trustworthy AI[221] that respects the fundamental rights protected by the Charter.

According to Guillaume Avrin[222], coordinator for artificial intelligence, this European response is a "product regulation," meaning that it aims to regulate AI products as they are marketed on the market. As such, like other products belonging to the European market, they must be authorized by obtaining the "CE marking."

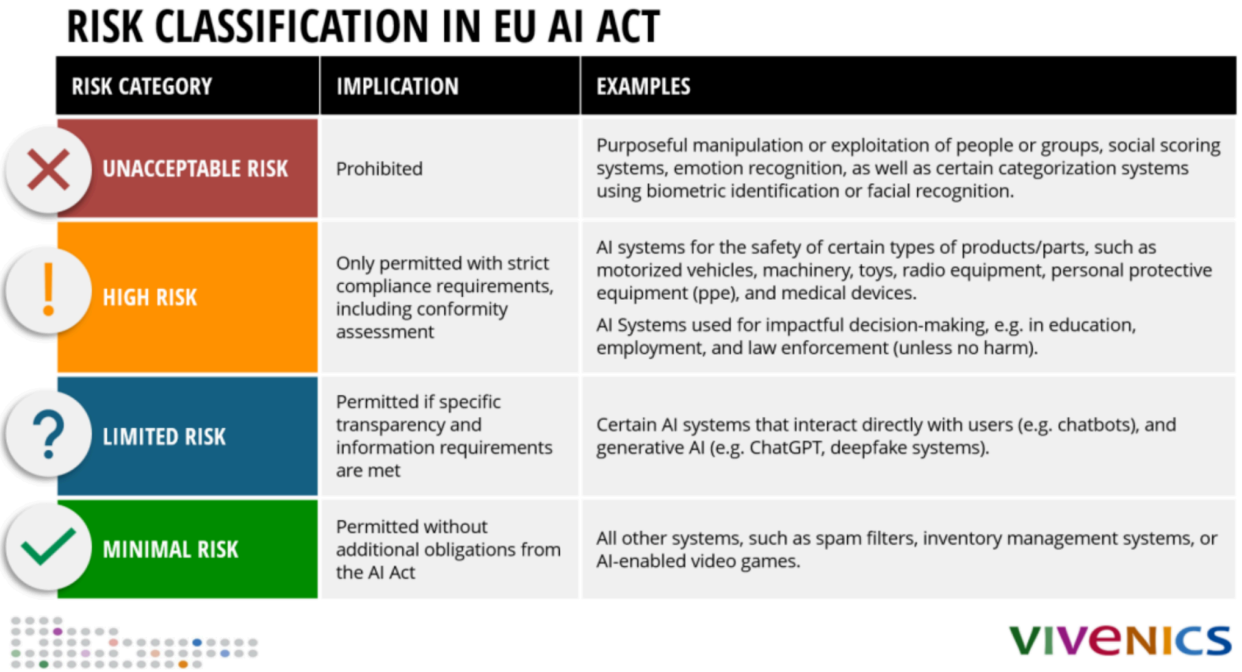
Beyond this framework for securing AI as a product, the AI Act also addresses AI as a modeler of access to expression, algorithmic prioritization, and opinion formation. It therefore also indirectly affects the exercise of freedom of expression and freedom of self-determination. This is why its analysis is relevant and necessary in order to assess the EU's response to the challenges created by new technologies.

---

[219] Peter J. Van de Waerdt, "*From Monocle to Spectacles: Competition for Data and 'Data Ecosystem Building'*," *European Competition Journal* 19, no. 2 (2023): 191–225, DOI:10.1080/17441056.2023.2169366.
[220] The Bundeskartellamt and the Competition and Markets Authority (CMA), notably, have warned of this risk.
[221] See generally Artificial Intelligence Act ; info.gouv.fr, *"Qu'est-ce que l'AI Act ?"*, available online: https://www.info.gouv.fr/actualite/quest-ce-que-lai-act.
[222] Info-gouv.fr, *What Is the AI Act?*, https://www.info.gouv.fr/actualite/quest-ce-que-lai-act.

It is on CE marking that the regulation plays by classifying AI systems according to four levels of risk[223], like the GDPR, the AI Act follows a risk-based approach[224]:

1. Unacceptable risk: these are AI systems used for unconscious manipulation, biometric categorization (based on ethnicity, religion,...), social scoring, and automated content moderation.
2. High risk: such as a resume scanning tool that ranks job applicants.
3. Specific risk: these include systems that interact with individuals, generate content, detect emotions.
4. Minimal risk: unregulated systems, such as spam filters.



Source: Vivenics, *AI Act Risk Assessment*, https://vivenics.com/ai-act-risk-assessment

However, AI systems influence the information visible to each individual by predicting the content that interests them based on the data produced at any given moment and/or personalizing advertisements using the same method.

The aim of the AI Act is *"to increase trust in AI and ensure that this technology is used in a way that respects the fundamental rights and safety of EU citizens."*[225] In fact, AI systems

[223] This four-tier classification primarily stems from doctrinal approaches seeking to provide a pedagogical framework. From a normative perspective, however, the Artificial Intelligence Act is less explicit. It focuses mainly on the most dangerous AI systems. Accordingly, Article 5 prohibits certain AI practices deemed unacceptable, while AI systems classified as high-risk are subject to a specific regulatory regime laid down in Articles 6 to 49 of the Regulation.

[224] Artificial Intelligence Act.

[225] Philipp Hacker, *AI Regulation in Europe: From the AI Act to Future Regulatory Challenges* (2023).

often operate in ways that are opaque, making accountability and contestability difficult. This justifies why the AI Act has to act. Thus, article 5 established a set of prohibitions which are to not exploit vulnerabilities such as those due to age or disability[226], not altering people's behavior through subliminal techniques above a person's threshold of consciousness[227] or, for AI, using deliberately manipulative or deceptive techniques. More broadly, they cannot lead to a significant change in behavior or to an evaluation or classification of individuals based on their social behavior or personal characteristics.

The AI Act prevents AI from surreptitiously influencing what we think and believe and polarizing discourse. It therefore seeks to protect mental autonomy, which we have seen to be a prerequisite for free and genuine expression. Furthermore, by requiring high-risk AI systems to comply with a set of strict obligations, the AI Act seeks to limit the harmful effects they have on fundamental rights. In concrete terms, these systems must comply with cumulative requirements:

1. risk management (identification, analysis, and reduction of risks to fundamental rights);
2. data quality and governance (relevant, representative, limited data to avoid systemic bias);
3. technical documentation and traceability (ability to explain how AI arrives at a certain result);
4. increased transparency (clear information for users on the existence and role of the AI system);
5. human oversight (the ability for a human to monitor, correct, or stop the system).

However, as we have seen, AI systems using algorithms influence the visibility of certain expressions and shape public debate. Therefore, these requirements for data governance and explainability lead to a reduction in arbitrary or discriminatory decisions favored by fully automated processing. In theory, this regulation should break down the opacity of these systems and thus prevent them from acting in the shadows, controlling our rights without anyone noticing.

In addition, the regulation has created another regime alongside that of risk, namely that of foundation models/GPAI. These are general-purpose models trained using big data. Gemini is one example. They are covered by Title VIII, which classifies them into two categories: Ordinary GPAI (general-purpose AI systems) and AI systems with high systemic capabilities (ASIS). There are *"capabilities that match or exceed the capabilities recorded in the most advanced*

[226] Artificial Intelligence Act, art. 5(1)(b).
[227] Artificial Intelligence Act, art. 5(1): "*The placing on the market of an AI system that deploys subliminal techniques beyond a person's consciousness to materially distort a person's behaviour is prohibited.*"

general-purpose AI models."[228] It is these models that are most capable of having a disproportionate impact on information, democracy, security, and freedom of expression because they directly influence the production and circulation of expressions. Their regulation is therefore crucial for freedom of expression. They are subject to specific obligations: systemic risk analysis, documentation, security and robustness, prohibition of manipulative techniques, continuous monitoring.

However, there is a danger that the effectiveness of this regulation could be undermined if "*the AI Act does become a Software Act"*[229] introducing changes that are too technical rather than political. Indeed, as Hacker warns, the AI Act could be too focused on technical compliance, not on substantive protection of fundamental rights[230]. There is a risk that companies will relocate outside the EU, i.e., engage in rational regulatory arbitrage due to the various responsibilities imposed on them by the regulation[231]. The abuses, e.g., the three critical "AI externalities": misinformation, environmental costs, and hybrid threats[232] from AI systems, extend beyond the European framework. The most dangerous effects of AI, i.e., those that alter the information space, are not fully addressed by the AI Act.

Furthermore, one of the major criticisms of the effectiveness of the AI Act's response is that it only includes the most advanced AI models as systemic risks, thereby severely limiting the beneficial effects it could have had. In fact, Article 3(64) defines high-impact capabilities too narrowly, as they are those *"that match or exceed the capabilities recorded in the most advanced general-purpose AI models."*[233] But, given the complexity of these systems, defining them based on training computation thresholds is questionable. For example, the "102 FLOPs" criterion is arbitrary, unstable, and already contested. Therefore, in order to improve the effectiveness of this regulation, its scope should be broadened, and the category of the most dangerous systems should not be limited to only the most advanced AI models: even the least advanced systems can affect freedom of expression on a large scale[234]. Philipp Hacker has outlined regulatory prospects for improving the European response, which would notably involve extending the obligations of the DSA to AI providers[235]. Transparency, audit, and data access obligations would therefore

---

[228] Artificial Intelligence Act, art. 3(64).
[229] Philipp Hacker, *supra* note 225.
[230] Ibid.
[231] Artificial Intelligence Act, art. 3(64).
[232] Ibid.
[233] Ibid.

[234] Philipp Hacker, Atoosa Kasirzadeh, and Lilian Edwards, "*AI, Digital Platforms, and the New Systemic Risk*," September 19, 2025, 30: "*systemic risk ... does not need to be categorically exclusive to the most advanced models – it is enough for them to be significantly more elevated in these than in less advanced models*."
[235] Philipp Hacker, *supra* note 225: *"Expanding DSA duties to AI providers would create a clear and manageable framework, for example by introducing a mandatory notice and action mechanism (Article 16 DSA), and endowing decentralized red teaming with the priority status of trusted flaggers (Article 22 DSA). These measures would*

need to be applied to the AI production chain, not just to platforms. This would help to address one of the blind spots in the regulation, namely the lack of control over the models themselves, by reducing the opacity of AI models, ensuring a certain level of accountability, preventing systemic risks but also by strengthening the protection of freedom of expression. Extending the scope of the DSA to AI would make it possible to address not only its use but also its manufacture, preventing risks to freedom of expression from migrating upstream where regulation is weakest. Thus, "*while the EU's AI Act is a monumental step, it requires further refinement and international cooperation to effectively manage the complex landscape of AI technologies."*[236] AI therefore presents itself as a long-term challenge.

Once again, we see that, like the DSA and the DMA, the AI Act does not challenge engagement-based ranking, does not limit polarization, and ignores algorithmic moderation, even though AI amplifies extreme ideas and ostracizes individuals in their bubbles. Once again, it is possible to apply the obligations set out in the regulation only formally.

After this overview of the various EU regulations in force that directly or indirectly address the relationship between freedom of expression and new technologies, it is clear that the EU has begun a process of making private actors more accountable, proceduralizing their power, and applying the principle of minimization to mass surveillance, thereby increasing visibility... The DSA, GPR, DMA, and AI Act do this through the implementation of transparency, remedies, and the securing of AI systems.

This is why they do not rebalance the relationship between private actors and users, they do not address the sources of power, but only their effects. Thus, the abuses described in Chapter 1 are not sufficiently regulated: from the attention-grabbing model to algorithmic surveillance, the European response is insufficient. The EU is not redefining the boundaries of power for these tech owners. They are effectively becoming the new members of the global government: "the code is law"[237] is clearly a reality.

At the same time, it is understandable why the EU is regulating cautiously, as too much regulation would limit freedom of expression, which is precisely what we are seeking to protect. Indeed, these regulations lead states to request the removal of content, which can put pressure on digital companies, which may tend to over-censor. However, this balance is particularly difficult[238] to strike, and the speed of technological innovation does not help: the creation of law is far too slow.

---

decentralise control over AI outcomes, draw on the monitoring resources of civil society, and ensure a safer AI ecosystem."

[236] Ibid.

[237] Lawrence Lessig, *supra* note 25 ; see also, as taken up by Romain Badouard, Mathieu Dugain, and Clément Labbé.

[238] See, in particular, L'Heure des prédateurs, Giuliano da Empoli (Paris: Gallimard, 2025).

The challenge has not really changed from what it was 15 years ago: it is still a question of *"ensuring that the law can adapt appropriately to constant technological advances and striking the right balance between the (necessary) safeguarding of the public interest and the (effective) protection of individual rights."*[239] But, the technologies created in recent years have brought with them even greater dangers, which is why it is urgent and essential to achieve this objective.

The goal is to regulate without limiting freedom of expression. This should not become a mirage, but neither should European regulations be overly ambitious, which could cause countless problems such as increased removal and filtering. In the triangle formed by states, the EU, and platforms/users, public authorities must not forget their role as guardians of fundamental rights and must ensure that intermediaries are held accountable without leading to "delegated censorship." It is a fine line between protection and surveillance, between regulation and freedom-destroying abuses. The EU may have overstepped this objective with the ChatControl project, as may certain national laws such as the Avia law in France. Under the guise of filling a legal void, or protecting against terrorism, in the name of combating hate speech, EU regulations must not themselves become censors of freedom of expression.

In fact, although the Chatcontrol project has been abandoned, its aim was to combat online child pornography. To this end, the European Commission proposed to authorize or even impose the automatic "scanning" of all private communications, including encrypted ones, thereby circumventing encryption, which is a security pillar of freedom of expression and privacy in the digital age. In concrete terms, this would have included messages sent to your mother, your lover, and even those written but never sent. It would have clearly established widespread surveillance, which is very dangerous. Access to all this data would have been used to enable AI systems to detect illegal or potentially dangerous content. However, as pointed out by the European Data Protection Supervisor (EDPS), voting yes to this project would have amounted to introducing a general, indiscriminate, and automated analysis of all text-based communications transmitted through number-independent interpersonal communications services[240]. And contrary to the other EU regulations, this one would have not respected the principle of necessity and proportionality as it would have deployed a general and indiscriminate analysis. The fact that the technology which would have been used should have to be limited to the use of "relevant key indicators", does not change that[241]. Especially since the surveillance

[239] Laurence Burgorgue-Larsen*, supra* note 14.
[240] European Data Protection Supervisor (EDPS), *Opinion 8/2024 on the Proposal for a Regulation amending Regulation (EU) 2021/1232 on a temporary derogation from certain ePrivacy provisions for combating CSAM*, 24 January 2024, Section 2 (General Remarks), para. 6.
[241] Ibid.

would have been carried out by AI systems that are far from reliable, potentially leading to significant error rates and, therefore, arbitrary suspicions.

The protection of fundamental rights, such as those that would have been affected here, namely privacy and freedom of expression, must be weighed against the objective of such regulation. It is clear that a less intrusive measure could have been found, such as, at the very least, limiting scanning to individuals already known to the police, or those who have been the subject of one or more complaints relating to a child. The objective could thus be largely achieved by less intrusive means. Generalized surveillance, due to the enormous power it gives to data controllers, and therefore to the owners of the AI systems that carry it out, and also due to the massive amount of data collected and analyzed, cannot be justified. Generalized filtering is explicitly prohibited by European law through its regulations[242] and case law in Scarlet Extended[243] and Sabam/Netlog[244].

It is clear that there are two risks:

1. Under-regulation (DSA, DMA, GDPR, AI Act): platforms retain their structural power over expression itself, its visibility, and information channels;
2. Over-regulation (Chatcontrol, Avia law): the original regulators themselves resort to censorship and surveillance.

In addition to the abuse coming directly from public actors, it can also be indirect, meaning that states and/or the EU can unduly infringe on freedom of expression by delegating to private companies or through them, which can then be referred to as proxy censorship. Thus, states and the EU can be freedom-destroying not only by over-regulating, but also by using the platforms or new technologies of private actors as tools of control, surveillance, and manipulation.

In fact, in a more insidious and secretive manner, certain EU states have attempted to cooperate with tech companies with the Machiavellian aim of using new technologies to, for example: influence public debate in favor of a political party, demonize certain protesters, and even, in some cases, incite war.

---

[242] This obligation was previously governed by Article 15(1) of Directive 2000/31/EC, and is now laid down in Article 8 of the Digital Services Act.

[243] Court of Justice of the European Union, *Scarlet Extended SA v. SABAM*, C-70/10, Judgment of 24 November 2011, §§ 35–40.

[244] Court of Justice of the European Union, *SABAM v. Netlog NV*, C-360/10, Judgment of 16 February 2012, §§33, 37 and 38.
See also: Court of Justice of the European Union, *YouTube LLC and Google Inc. v. Cyando AG*, Joined Cases C-682/18 and C-683/18, Judgment of 22 June 2021.

This also has the effect of recognizing that platforms are no longer simply private actors but governors of public debate, with whom certain states compromise and cooperate. We must therefore be wary not only of tech players but also of state political powers, because although they are intrinsically created to protect the public interest, or even our fundamental rights, they can also be the instigators of certain liberticidal abuses of new technologies.

Poland and Hungary have been investigated for playing such a role. Hungary purchased spyware such as Pegasus, which became a powerful tool for political engineering. Confirmed by Amnesty International, an investigation by the Forbidden Stories consortium of journalists revealed that Hungary[245] had infiltrated the phones of more than 300 Hungarian citizens thanks to Israeli spyware[246] developed by NSO Group. Viktor Orbán's government was reportedly one of their clients. According to the same sources, potential or confirmed targets of the spyware included investigative journalists, lawyers, businesspeople, and Hungarian political opponents[247]. But, Pegasus is not only a tool for ensuring Hungarian national security, it is also an information weapon. It is capable of extracting all data from a phone, remotely activating its camera and microphone, and accessing people's calendars, such as their appointments, contacts, and habits. As noted by the Council of Europe, the use of Pegasus in Hungary has not been aimed at imminent terrorist threats (which would have been the only purpose that could legitimize such surveillance), but at individuals who could potentially be harmful to state policy, raising serious concerns about respect for the rule of law and democratic pluralism[248].

Shutting down public debate through opaque private technology is what Shoshana Zuboff describes as the “instrumentarian power” of surveillance capitalism. By using new technologies, visible violence is no longer necessary to discipline citizens; it is enough to silence certain voices. What's more, by simply renting or buying technologies capable of such deep intrusion, states don't have to manufacture them themselves, something they would find difficult to justify. States win on all fronts: they have secret access to surveillance capabilities designed specifically to avoid detection.

---

[245] Parliamentary Assembly of the Council of Europe, *Pegasus Spyware and Similar Surveillance Software and Secret State Surveillance*, Report of the Committee on Legal Affairs and Human Rights, Doc. 15825, 20 September 2023: In practice, the use of Pegasus has been identified in eleven countries worldwide. As this thesis is situated within a European study, it focuses specifically on Hungary. It is established that Pegasus has been sold to at least fourteen Member States of the European Union, including Belgium, Germany (in a modified version), Hungary, Luxembourg, the Netherlands, Poland, and Spain, as well as to third countries such as Azerbaijan.

[246] Amnesty International, *Pegasus Project: Hungary Allegedly Targeted Journalists and Activists*, 22 July 2021, available online on Amnesty International’s official website: https://www.amnesty.fr/liberte-d-expression/actualites/projet-pegasus-revelations-hongrie-logiciel-espion-nso-group.

[247] Ibid.

[248] Parliamentary Assembly of the Council of Europe, *Pegasus and Similar Spyware and Secret State Surveillance*, Doc. 15827 (2023), in particular the sections relating to Hungary.

The Hungarian example shows what “delegated censorship” becomes in its most radical form: no longer just a request by states to remove content from private platforms, but the purchase by these states of a secret capacity for total espionage. They are thus able to control freedom of expression themselves: restricting it unevenly, directing it, stifling it,... It is no longer just a question of imbalance between platforms and users, but of private government and a Big Brother-style public[249].

In the end, the abuses described in Chapter 1 are far from being prevented by European regulations. Of course, seeking to hold platforms, AI systems, and their private owners accountable is the right path to follow, since they are the ones who currently control all aspects of freedom of expression. However, the EU is hampered by several obstacles. First, it is becoming a censor of expression itself. Second, the rules of the digital game are changing at the rapid pace of creation and refinement of new technologies, and it cannot catch up: the law cannot keep up with the pace set by the tech giants. From now on, the code is law[250]. What's more, with expression becoming tenfold, more numerous, and potentially more visible, regulation and even censorship are multifactorial.

The EU must therefore take an interest in all its authors: tech giants, but also states, gatekeepers, and individuals who organize public discourse. This is why it is important for the EU to clearly define a governance framework and its core values. That is the best it can do.

Sub-chapter 2 - Ethical and Political Issues: Towards Responsible and Shared Governance of Digital Freedom of Expression

As previously analyzed, freedom of expression and privacy are interdependent. Contemporary technological tools for surveillance, profiling, and algorithmic personalization lead to self-censorship (chilling effect) and therefore disregard people's freedom of informational self-determination: what you wrote today on Instagram may be the result of upstream manipulation enabled by the processing of your data. Technology has invaded our minds and interferes with the formation of our thoughts and opinions. It is therefore necessary to put an end to this influence in order to glorify our real freedom of expression. Thus, in the digital age, privacy becomes the primary guarantee of free speech.

Our data is also a valuable commodity/resource because tech owners have turned it into the raw material for a truly lucrative business. The reality does not match our perception of it: services are no longer sold but are free; it is individuals who are the source of profit. The adage

[249] Suzanne Vergnolle, *supra* note 7.
[250] Lawrence Lessig, *supra* note 25.

that “If you don't pay for something, you're not the customer, you're the product”[251] has come to life. Dugain and Labbé summed it up very well with their vivid image: “*That's the price we pay. By joining social networks, we unwittingly seal a kind of pact with the devil: our digital identity in exchange for free, increasingly personalized services.”*[252] And finally, to use their striking metaphor, *“the market value of users is no longer their labor, but their digital identity, which will be resold several times, as was done in slave markets.”*[253]

Before considering a radical transformation of the current economic model, it is necessary to establish a complementary response to existing European regulations: the implementation of polycentric governance in which each regulator of freedom of expression assumes a share of responsibility and must act in accordance with ethical principles. This must be done with the understanding that this ethical and shared governance cannot solve the problem on its own, as long as the economic foundations of society remain untouched.

Given that it is not only platforms that set the rules for expression, and that regulation is no longer solely a public matter, with governments and users also having an impact on freedom of expression, everyone must be made accountable through ethical governance. Indeed, legal scholar Jack Balkin has proposed a model known as the “freedom of expression triangle.”[254] This triangle has three sides, as mentioned above: governments, private companies, and users. Establishing the rules of ethical and accountable governance will make it possible to avoid, as far as possible, security abuses by governments and to combat the total privatization of power by tech giants. It is therefore necessary to establish the rules of algorithmic governance. The EU is already on the right track, having imposed a principle of transparency and systemic risk management obligations.

---

[251] Marc Dugain et Christophe Labbé, *supra* note 6.
[252] Ibid.
[253] Ibid.

[254] Jack M. Balkin, “*The Three Laws of Robotics in the Age of Big Data*” (2017), SSRN:https://ssrn.com/abstract=2890965.

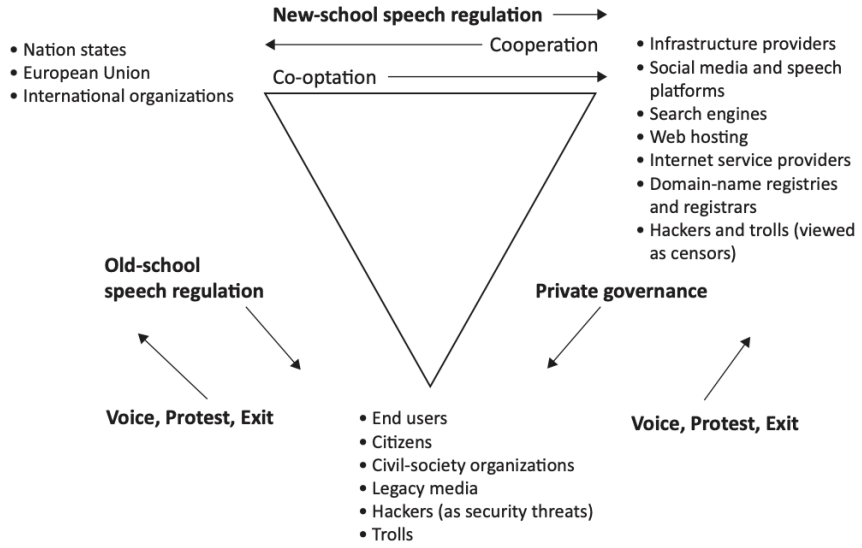


Figure 1. Balkin's (2018b) pluralist model of speech regulation.

Source: Jack M. Balkin, "Free Speech Is a Triangle," *Columbia Law Review*, (2018).

Three scenarios for the evolution[255] of this governance are possible. The first one is Government Regulation - a situation where the government takes the lead in the context of speech regulation - This is the case in China with the Great Firewall, which serves as the clearest example with grave consequences for censorship, transparency, and surveillance. Under the guise of combating dangerous illegal content, particularly terrorism and hate speech, some justify authoritarianism and censorship. The risks of this scenario for the EU are those we criticized in sub-chapter 1 of chapter 2 through a comparison between ChatControl and current European regulations. Government regulation could lead to: loss of transparency, drastic reduction in freedom, increased control leading to over-censorship.

The second one is Walled Gardens - when the private sector (Facebook, Google, ...) takes control - The risks are great: privatization of public discourse, loss of privacy, loss of freedom of informational self-determination, opacity of data processing and the functioning of algorithmic and AI systems, destructive commercial logic.

The last one is Decentralization - Users would regain power, platforms would become public goods, essential services[256]. But this scenario has a capacity limit: users alone cannot manage the regulation of all expressions.

We are clearly moving towards the second scenario. However, the idea that the architecture of digital networks allocates power paints a dangerous reality: power is no longer

[255] Emma Ricknell, "*Freedom of Expression and Alternatives for Internet Governance: Prospects and Pitfalls*," *Media and Communication* 8, no. 4 (2020): 110–120, https://doi.org/10.17645/mac.v8i4.3299.

[256] Ibid. 4(3) : *"As technology advances and human dependence on the Internet increases, the argument is that the Internet should be treated not as a commercial product but as a public utility, controlled by citizens."*

just normative, it has become structural, embedded in the very infrastructures that organize the visibility, prioritization, and removal of content.

Ultimately, none of the three models alone offers satisfactory protection for freedom of expression. They are either unworkable and/or repressive. A digital and technological society governed solely by states would lead to a risk of authoritarianism, but governed by private companies it would result in the trampling of our fundamental rights. Finally, a model governed exclusively by users would be untenable and would lead to mistrust between individuals themselves.

The possible alternative is therefore to consider a hybrid form: co-governance where responsibility is distributed, with each party having a specific role. It is with this in mind that we will attempt to establish a governance profile that is appropriate for today's challenges, by defining the role of the actors in the public discourse.

Firstly, states would still have the role of guaranteeing fundamental freedoms. They would no longer do so through direct control of discourse, but rather by defining the conditions for controlling expression. The complexity and opacity of algorithmic mechanisms require them to shift to oversight of algorithmic systems operated by private actors. They would act as the structural guarantors of the democratic framework. Their role stems from their positive obligation to create a favorable environment for participation in public debate by all concerned persons. Within European regulations, this is reflected in the DSA through procedural obligations, transparency, recourse, and oversight by public authorities. By establishing “shared responsibility,” the DSA makes states the supervisors of platform practices. We can talk about shared responsibility because, for their part, states and the European Commission coordinate and monitor compliance with procedures and audits; they do not control the content itself, but ensure that private algorithmic moderation respects fundamental rights.

But, it is important to remember that their role has significant limitations; they cannot establish measures that implement widespread and indiscriminate surveillance, as this has been prohibited by the DSA and the CJEU[257] in particular.

Furthermore, states and the EU cannot be overly preventive, as the risk of censorship is too great. This is demonstrated by the ChatControl project studied above. This is all the more true given that the CNIL and the European Data Protection Supervisor have pointed out that this could lead to mass surveillance that is incompatible with fundamental rights and the principles established by CJEU case law.

[257] See supra, Chapter II, Sub-chapter 2, 2.1.

In addition to these legal limitations, there are also material capacity limitations. States do not own the new technologies, so they do not have full access to and oversight of algorithmic mechanisms and data processing. They also lack the algorithmic and technological expertise of tech giants to be best placed to determine precisely the balance between technological advances and fundamental rights. Moreover, European States are dependent on technologies created by American CEOs and they do not have sufficient staff and technology to regulate online discourse on their own.

They find themselves irrevocably dependent on private actors and their technology and cannot claim to govern traffic and the visibility of plurality of expression on their own. This is why, for effective co-governance, platforms must respect the principle of transparency so that the functioning and impact of their algorithmic systems are clear to states and the EU, enabling them to articulate relevant rules for moderation. Thus, the role of states and the EU is not marginal: they regulate the regulators of public discourse by guaranteeing democratic principles, fundamental rights, and the conditions for co-governance. They do not act directly on moderation, but rather supervise the delegation of power.

Secondly, he calls for the need for a second pole, as theorized by Balkin: platforms. In the digital age, it is the tech giants that hold the heart and soul of power: they own the information vectors and the tools that structure them by design. Platforms do not just apply the rules established by the EU and states, which provide the main legal basis, they create their own "technical private law of expression". That is why we can talk about private standards since they are formed by private actors in the context of relationships between private individuals, namely the Terms of Service. That is why we can talk about technical standards because moderation is delegated to algorithms and automated. In short, platforms leave little room for states and the EU to act directly on the technical aspects (code) of expression; platforms are both rule-makers and rule-enforcers for online speech[258]. Added to this normative power is an element that multiplies its scope and complicates any challenge to it: its opacity. Consequently, the transparency requirement imposed by European regulations is essential to achieve reliable co-governance. Without access to recommendation, moderation, ranking, and restriction parameters, states cannot effectively regulate the role of platforms.

Thirdly, outside the macro players in Balkin's triangle (EU/States and platforms), part of the regulatory power operates at a more discreet level: that of intermediate gatekeepers. Alongside informal and community practices, EU law has institutionalized a part of these players: the trusted flaggers enshrined in Article 22 of the DSA. It is therefore necessary to examine their role in this ethical and shared co-governance. This status is granted by the Digital

[258] Jack M. Balkin, *supra* note 254.

Services Coordinator of the Member State of establishment only to entities and not to individuals[259]. Trusted flaggers must demonstrate particular expertise and competence in detecting, identifying, and notifying illegal content online, be independent from platforms, and work diligently, accurately, and objectively[260]. Their expertise and the fact that their status is assigned to them places them between the public and private sectors and justifies priority treatment of their notifications. This partial delegation of reporting and moderation to private actors implies digital responsibility, as Goa Kacou[261] argues, i.e., the ethical use of technology and online speech to prevent the fight against abuse from itself becoming an unjustifiable restriction on freedom of expression.

Beyond the advantages (such as faster content processing) offered by the intervention of such actors, risks remain: over-removal, bias of interests[262]. In this sense, it is important that the EU or Member States ensure a certain impartiality on the part of these actors to prevent them from being swayed by commercial, political, or ideological interests and thus arbitrarily censoring content. At this stage, trusted flaggers illustrate the ambivalence of polycentric governance: on the one hand, they can strengthen user protection against clearly illegal content, but on the other hand, they can also contribute to the private and potentially preventive regulation of freedom of expression.

Fourthly, at a relatively lower level than institutionalized gatekeepers, and even as tech giants centralize most of the power, administrators and moderators also shape the contours of our expression. For example, it is the moderator of a YouTuber/Twitch/Discord who has the ability to hide, ban from the channel, or prevent messages from being sent in the public chat.

This creates a pyramid of standards specific to the technological domain, analogous (proportionally speaking) to that developed by Hans Kelsen: European and state regulations > general terms of use and privacy policies of platforms > trusted flaggers > internal rules of certain groups, forums, and online pages.

Through charters, bans, and comment moderation, even without official status, they set internal rules and decide whether or not to apply platform policies in a more or less objective manner, biased by their own perceptions and beliefs.

---

[259] Digital Services Act, recital 61.

[260] European Commission, *Trusted flaggers under the Digital Services Act (DSA)* (last updated 19 December 2025), online: https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa?utm.

[261] Goa Kacou, *supra* note 18.

[262] For more details see not. Jacob van de Kerkhof, "*Article 22 Digital Services Act: Building Trust with Trusted Flaggers*", *Internet Policy Review*14(1) (2025), DOI: 10.14763/2025.1.1828, online: https://policyreview.info/articles/analysis/article-22-digital-services-act?utm.
This study highlights concerns regarding the involvement of trusted flaggers in content moderation from the perspective of freedom of expression. It assesses both the promises and shortcomings of Article 22 DSA in its current implementation and formulates recommendations aimed at ensuring a more effective operationalisation of trusted flaggers while better safeguarding users' freedom of expression.

Furthermore, their role is not only recognized factually, but also legally. The ECHR, through the Sanchez ruling[263], recognized that a local elected official, as the administrator of a Facebook page, had a reasonable obligation to monitor hateful content posted by third parties. The governance of speech is not only carried out through algorithms but also through human decisions, which are sometimes invisible but certainly influential. The lack of visibility and procedural guarantees regarding their role encourages arbitrary decision-making. This is why a scenario in which only users have regulatory power is unsatisfactory.

Finally, for the sake of accuracy, one last actor should be added: individuals who are both regulators and subjects of these regulations—citizens themselves. Balkin's triangle should therefore be divided into two parts:

1. Intermediate gatekeepers: those who have power delegated either directly by the EU or by platforms;
2. Citizens: they have diffuse and highly behavioral power. They constitute the first level of regulation without necessarily being described as moderators.

As Goa Kacou points out, users must exercise their freedom of expression ethically and with digital literacy[264]. Indeed, no regulation, whether legal, technical, or community-based, can be fully effective without individual responsibility on the part of users. As Romain Badouard points out, combining automatic moderation with reporting practices by users themselves can lead to participatory censorship, which in turn can stifle certain forms of expression[265]. The initial steers established by the EU and/or Member States are proving to be all the more necessary. Moderation is therefore not simply vertical (platform > users) but also participatory. For citizens, exercising freedom of expression in a responsible and ethical manner means first and foremost being aware that freedom of expression is not absolute and has many limits that internet users must not ignore[266]. In doing so, it is the responsibility of citizens to know these limits and to restrict themselves ethically, not just out of fear of punishment. They tend to confuse freedom of expression with the right to say whatever they want, including hateful, racist, and illegal comments. It is therefore essential to remind them of the legal, fundamental, and ethical limits such as: respect for pluralism, tolerance, human dignity, the prohibition of hate speech. It is

[263] See Chapter II, Sub-Chapter I, 2.1.1. The new role of platforms: from neutral host to algorithmic censor.
[264] Goa Kacou, *supra* note 18.
See, more recently: Romain Badouard, *Les nouvelles lois du web. Modération et censure*, in *Pauline Brouard* (ed.), *Quaderni* (2025): 147–151, DOI: 10.4000/quaderni.2049, online: https://journals.openedition.org/quaderni/2049?utm; and UNESCO, *Guidelines for the Governance of Digital Platforms* (2023), ISBN: 978-92-3-100620-3.
[265] Romain Badouard, *supra* note 264.
[266] Goa Kacou, *supra* note 18.
See, more recently: Romain Badouard, *supra* note 264.

therefore incumbent upon us to use modern means and/or media of communication intelligently and ethically, and to pursue ethical cybernetics. This ethical cybernetics would not replace the law but would complement it. The establishment of such a framework of values would thus help to prevent the spread of illegal speech and neutralize certain abuses due to new technologies.

This ethics is all the more necessary because it requires each actor to take individual responsibility based on an awareness of the impact of their words and, more broadly, the impact of algorithmic moderation. It is therefore a prerequisite for ensuring that the freedom of some does not oppress the freedom of others: the freedom of expression of one individual in relation to that of another, freedom of expression versus the freedom of platform moderation.

Finally, it is because communication today is no longer merely informative but also persuasive that it is now crucial to address the monetization and modeling of speech by building such ethical co-governance. This is not simply a matter of "good conduct" but a genuine democratic firewall against the freedom-destroying excesses of new technologies and their uses.

But, this ethical and responsible co-governance, however necessary it may be, and current European regulations are not sufficient to properly address the new technological mechanisms that are shaping our society. Indeed, despite how beneficial it may be, it does not affect the structural foundations of power over expression, i.e., the economic roots of global society and the behavioral roots of the actors who hold this power. As long as visibility and the dissemination of speech depend on a model based on capturing attention and exploiting data, as long as we do not become customers again but remain products, freedom of expression will remain structurally limited.

Expression has become a commodity from which tech giants profit. In this context, the use of new technologies is driven by economic objectives: maximizing engagement to obtain as much data as possible, establishing profiles, and being able to influence, even politically, and sell this information. A triptych has been formed: attention becomes a commodity, data becomes a resource, and freedom becomes a product. When we talk about surveillance capitalism, the challenge is not only to retain users, but to get to know them in order to influence them.

As we have already mentioned, Shoshana Zuboff emphasizes that capitalist surveillance does not only seek to predict our behavior, but to modify it, as summed up in this particularly enlightening phrase: "the goal is to automate us." In this context of facilitated manipulation, ethical and polycentric co-governance is not a miracle solution; it would only treat the symptoms, leaving the cause intact.

Ultimately, maximizing the protection of freedom of expression in the digital age is utopian, since the market economy of speech is based on the exploitation of fundamental human instincts: the need for recognition, the attraction to conflict and emotional content, and the need

to belong to a group. Thus, surveillance capitalism works so well because it does not oppose human nature but exploits it. Tech giants have simply industrialized our human mechanisms.

As long as the digital economic model is based on capturing attention and commodifying expression, no legal reform will be able to fully guarantee genuine freedom of expression. The current crisis of freedom of expression is primarily a crisis of the political economy of speech.

CONCLUSIONS

The objectives of this thesis were, first, to highlight the benefits and costs of new technologies in relation to freedom of expression, and then to use this phenomenological observation to fully analyze whether the European legal framework is sufficiently equipped for the technological age.

1. The analysis showed that, contrary to the original opinion on the beneficial contributions of new technologies to the exercise of freedom of expression, recent debates have led a growing number of legal scholars, institutions, and individuals to question the overall effects, with the aim of containing the many abuses that accompany the benefits. A restructuring of speech and how it is exercised is currently underway, driven by the economic and technical motivations of the tech giants. Platforms have simultaneously expanded the capacity for expression, the number of vectors, and the potential visibility of discourse to an unprecedented degree, while shaping this freedom through data collection, algorithmic personalization, and other means. These mechanisms for guiding speech have revealed a new aspect of freedom of expression: the effective ability to participate in public debate, to be truly seen and heard.
2. More specifically, the arrival of new technologies has challenged the traditional definition of freedom of expression and the limits of its protection. This thesis has sought to identify the freedom-destroying abuses brought about by new technologies, highlighting direct, indirect, and structural forms of infringement on freedom of expression. By granting power that goes beyond moderation in the collective interest, structural power to control, monitor, and manipulate discourse, the traditional legal framework for the protection of fundamental rights appears insufficient to fully contain these transformations.
3. Finally, aware that this traditional framework alone is not effective in the face of technological advances and the considerable power they confer on their owners, the EU has developed new instruments such as the Digital Services Act, the GDPR, the Digital Markets Act, and the AI Act. These tools demonstrate a desire to neutralize the negative effects to a certain extent.
4. However, the EU legal instruments do not yet fully guarantee all protected expressions, as several gaps persist. First, the traditional legal framework (article 11 CFREU and article 10 ECHR) does not explicitly protect the second component of freedom of expression, namely the effective right to be heard and to have one's expression visible. In addition, EU regulations do not redefine the limits of the power of digital platforms even though they exercise a real control over visibility, content prioritisation, and have access

to massive amounts of data. At the same time, the EU legal framework does not provide sufficient rights to individuals to face systemic prejudices. Moreover, despite the existing obligation of transparency, algorithmic governance remains largely opaque in practice. The economic model based on capturing attention and exploiting data largely stays outside the scope of regulation even though it structurally shapes the exercise of freedom of expression. More fundamentally, given how harmful new technologies can be for freedom of expression, European regulation would have gained in effectiveness and efficiency if it had not been fragmented but rather contained in a single normative framework specific to the strict relationship between freedom of expression and new technologies. Finally, the EU has empowered private actors but there is a legal vacuum when it comes to State accountability although they also participate in the restriction of freedom of expression.

As blind spots remain, the existing safeguards such as the prohibition of general surveillance, transparency obligations and risk assessment requirements should be complemented by additional measures as those developed in the recommendations.

RECOMMENDATIONS

- **Recommendation 1 - Strengthening the principle of transparency**

As we have concluded, the current European framework that includes transparency and diligence obligations is not sufficient to ensure the effective exercise of freedom of expression.

Articles 14, 17, and 20 of the DSA, and Article 34 for very large platforms, impose a principle of transparency and diligence: definition of clear terms and conditions, provision of a statement of reasons to users affected by a moderation decision, establishment of an internal complaint-handling mechanism, and assessment of systemic risks for VLOPs. Notwithstanding, their fragmentation, the length of the articles, and the repetition of complex wording make them difficult for users to understand and utilize.

This limitation on transparency is not unique to the DSA or to the regulation of new technologies. In French public law, it has been shown that the principle of transparency in administrative decisions, enshrined in Article 15 of the Declaration of the Rights of Man and of the Citizen, when not accompanied by individual procedural rights, does not provide the information and legal tools necessary for effective challenge. This analogy reinforces the relevance of this recommendation.

It could then be considered to supplement the DSA with:

1. an individual procedural guarantee consisting of a personal right to an explanation of the reasons for automated processing to which the person has been subjected, a right to human review to judge whether or not an algorithmic decision to which the person has been subjected is arbitrary;
2. An obligation on the creators of new technologies to list, document, and explain their operating mechanisms and their impact on fundamental rights. This would take the form of standardized fact sheets that are understandable to non-experts. The result would be a public classification of technologies according to their impact on fundamental rights (profiling, personalization, visibility,...).

Such a measure would pursue the legitimate objective of protecting freedom of expression and would respond to the need to correct the asymmetry between platforms and users, while remaining proportionate by limiting itself to procedural and informational obligations.

- **Recommendation 2 - Strengthening shared governance**

The conclusions also highlighted that the current European legal framework is insufficient to effectively protect freedom of expression, as it addresses some risks associated with content moderation but not all, such as algorithmic censorship.

Articles 13 and 34-35 of the Digital Services Act provide for the consideration of fundamental rights and mechanisms to address systemic risks relating to them (for VLOPs).

Nevertheless, the abuses brought about by new technologies could be better contained if the EU established mediation between platforms, public authorities, and users.

This could involve strengthening shared governance by creating an online freedom of expression protection officer, modeled on the data protection officer.

This appointed person would have no power of censorship and would not have the status of a public authority. Their role would be to liaise between platforms, state or European authorities, and users. Similar to a DPO, this commissioner would handle complaints and requests from individuals affected by moderation.

Finally, to avoid preventive censorship of speech, this idea could be coupled with the development of guidelines, discussed jointly with tech players, technical experts, and state and European authorities. These guidelines would aim to define the permissible limits of moderation mechanisms and algorithmic organization of expression.

Such a measure would pursue the legitimate objective of protecting freedom of expression and pluralism. It would respond to the need to rebalance the power relationship between platforms and users and would remain proportionate by creating a coordinating actor similar to those that exist for data protection.

BIBLIOGRAPHY

I. International and European Legal Instruments

1. Universal Declaration of Human Rights, UN General Assembly, 10 December 1948.

2. International Covenant on Civil and Political Rights, UN General Assembly, 16 December 1966.

3. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), 4 November 1950.

4. Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012.

5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4 May 2016.

6. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act), OJ L 277, 17 October 2022.

7. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 (Digital Markets Act), OJ L 265, 12 October 2022.

8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 (Artificial Intelligence Act).

9. UNESCO, *Guidelines for the Governance of Digital Platforms*. Paris: UNESCO, 2023.

II. Case Law

A. European Court of Human Rights

1. *Airey v. Ireland*, no. 6289/73, Judgment of 9 October 1979.

2. *Appleby and Others v. the United Kingdom*, no. 44306/98, Judgment of 6 May 2003.

3. *Ahmet Yıldırım v. Turkey*, no. 3111/10, Judgment of 18 December 2012.

4. *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, Judgment of 1 December 2015.

5. *Delfi AS v. Estonia* [GC], no. 64569/09, Judgment of 16 June 2015.

6. *Dink v. Turkey*, nos. 2668/07 et al., Judgment of 14 September 2010.

7. *Frisk and Jensen v. Denmark*, no. 19657/12, Judgment of 5 December 2017.

8. *Handyside v. the United Kingdom*, no. 5493/72, Judgment of 7 December 1976.

9. *Informationsverein Lentia v. Austria*, nos. 13914/88 et al., Judgment of 24 November 1993.

10. *Lingens v. Austria*, no. 9815/82, Judgment of 8 July 1986.

11. *Magyar Helsinki Bizottság v. Hungary* [GC], no. 18030/11, Judgment of 8 November 2016.

12. *Magyar Jeti Zrt v. Hungary*, no. 11257/16, Judgment of 4 December 2018.

13. *Observer and Guardian v. the United Kingdom*, no. 13585/88, Judgment of 26 November 1991.

14. *Sanchez v. France* [GC], no. 45581/15, Judgment of 15 May 2023.

15. *The Sunday Times v. the United Kingdom*, no. 6538/74, Judgment of 26 April 1979.

16. *Vladimir Kharitonov v. Russia*, no. 10795/14, Judgment of 16 November 2020.

17. *Centre for Democracy and the Rule of Law v. Ukraine*, no. 75865/11, Decision of 3 March 2020.

B. Court of Justice of the European Union

1. *Scarlet Extended SA v. SABAM*, Case C-70/10, Judgment of 24 November 2011.

2. *SABAM v. Netlog NV*, Case C-360/10, Judgment of 16 February 2012.

3. *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd*, Case C-18/18, Judgment of 3 October 2019.

4. *Frank Peterson v Google LLC* and *Elsevier Inc. v Cyando AG*, Joined Cases C-682/18 and C-683/18, Judgment of 22 June 2021.

5. *Poland v. Parliament and Council*, Case C-401/19, Judgment of 26 April 2022.

6. *Ligue des droits humains ASBL v Conseil des ministres*, Case C-817/19, Judgment of 21 June 2022.

7. *Meta Platforms Inc. and Others v. Bundeskartellamt*, Case C-252/21, Judgment of 4 July 2023.

8. *Google LLC and Alphabet Inc. v European Commission (Google Shopping)*, Case C-48/22 P, Judgment of 10 September 2024.

C. National Courts

1. German Federal Constitutional Court (Bundesverfassungsgericht), *Volkszählungsurteil* (Census Act Case), Judgment of 15 December 1983.

2. Tribunale di Roma, *CasaPound Italia v. Facebook*, Judgment of 14 February 2020, no. 80961/19.

3. Supreme Court of the United States, *Packingham v. North Carolina*, No. 15-1194, Judgment of 19 June 2017.

III. Soft Law, Institutional Documents and Reports

1. Amnesty International. *Pegasus: A spyware scandal*. 2021.

2. Amnesty International. *Pegasus Project: Hungary Allegedly Targeted Journalists and Activists*. 22 July 2021.

3. ARCOM and ARCEP. *Référentiel des usages numériques*. Latest edition.

4. Council of Europe. Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries.

5. European Commission. *Digital-Ready Policymaking – Glossary*. Interoperable Europe.

6. European Commission. *Digital Services Act – Explanatory Memorandum*. 2022.

7. European Commission. Press Release, *Commission designates first Very Large Online Platforms and Search Engines under the DSA*, 25 April 2023.

8. European Data Protection Supervisor (EDPS). Opinion 8/2024 on the CSAM proposal, 24 January 2024.

9. Forbidden Stories Consortium. *Pegasus Project Investigation*. 2021.

10. Information Commissioner's Office (UK). *Investigation into the Use of Data Analytics in Political Campaigns*. Report to Parliament, 6 November 2018.

11. OECD. *Emerging Technologies and Their Impact on Society*. 2017.

12. Parliamentary Assembly of the Council of Europe. *Pegasus and Similar Spyware and Secret State Surveillance*, Doc. 15827 (2023).

13. United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Report A/HRC/17/27, 16 May 2011.

IV. Legal Doctrine

A. Books and Monographs

1. Auriel, Pierre, and Mathilde Unger. *La régulation par les plateformes*. Paris: Raison Publique, 2024.

2. Badouard, Romain. *La régulation des contenus sur Internet*. Paris: Presses de Sciences Po, 2020.

3. Cardon, Dominique. *À quoi rêvent les algorithmes*. Paris: Seuil, 2015.

4. Cohen, Julie E. *Configuring the Networked Self*. New Haven: Yale University Press, 2012.

5. Dugain, Marc, and Christophe Labbé. *L'Homme nu*. Paris: Plon, 2016.

6. Guggenberger, Nikola. *The Essential Facilities Doctrine in the Digital Economy*. New Haven: Yale University Press, 2021.

7. Lynskey, Orla. *Information Rights and Platform Power*. Cambridge: Cambridge University Press, 2019.

8. Pariser, Eli. *The Filter Bubble*. New York: Penguin Press, 2011.

9. Solove, Daniel J. *Nothing to Hide*. New Haven: Yale University Press, 2011.

10. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2019.

B. Academic Articles, Chapters, Reviews

1. Badouard, Romain. "Shadow ban. L'invisibilisation des contenus en ligne." *Esprit*, no. 11 (2021): 75–83.

2. Badouard, Romain. “Les nouvelles lois du web. Modération et censure.” *Quaderni* (2025): 147–151.

3. Burgorgue-Larsen, Laurence. “Les nouvelles technologies.” *Pouvoirs*, no. 130 (2009): 65–80.

4. Clucas, Tom. “Don’t Feed the Trolls.” In *Violence and Trolling on Social Media*, edited by Sara Polak and Daniel Trottier. Amsterdam: Amsterdam University Press, 2020.

5. Dacar, R. “The Essential Facilities Doctrine, Intellectual Property Rights, and Access to Big Data.” *IIC* 54 (2023): 1487–1507.

6. De Hert, Paul, and Vagelis Papakonstantinou. “The New General Data Protection Regulation.” *Computer Law & Security Review* 32, no. 2 (2016): 179–194.

7. Dovbysh, Olga, and Esther Somfalvy. “Understanding Media Control in the Digital Age.” *Media and Communication* 9, no. 4 (2021): 1–4.

8. Forteza, Paula. *L’utilisation des nouvelles technologies par les pouvoirs publics*. Fondation Jean-Jaurès, 2021.

9. Guevara-Rosas, Erika. *Tech Made by Palantir and Babel Street Pose Surveillance Threats*. Amnesty International, 21 August 2025.

10. Hildebrandt, Mireille. “Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning.” *Theoretical Inquiries in Law* 20, no. 1 (2019): 83–121.

11. Kacou, Goa. “Problématique de la liberté d’expression à l’ère de la communication numérique.” *Revue ivoirienne des Sciences du Langage et de la Communication* 10 (2016): 243–256.

12. Rouvroy, Antoinette, and Thomas Berns. “Gouvernementalité algorithmique.” *Réseaux* 177 (2013): 163–196.

13. Susser, Daniel, Helen Nissenbaum, and Beate Rössler. “Online Manipulation.” *Georgetown Law Technology Review* 4 (2020).

14. Teo, Szu-Yu. “Artificial Intelligence and Its ‘Slow Violence’ to Human Rights.” *Human Rights Review* (2024).

15. Tinière, Romain. “L’Union européenne et la régulation des plateformes.” *Revue de l’Union européenne*, no. 650 (2021): 413.

16. Vergnolle, Suzanne. “Normalisation de la surveillance et propagation de la manipulation.” In *Nouvelles technologies et droit européen*. Paris: Mare & Martin, 2023.

17. Woods, Lorna. “Delfi AS v Estonia.” *Strasbourg Observers*, 18 June 2015.

V. Press and Online Sources

1. Breton, Thierry. “The Digital Challenges Facing Our Democracies Are Global.” *FigaroVox*, 10 January 2021.

2. Capone, Nathan. “Delfi v. Estonia.” *Fieldfisher Blog*, 16 July 2015.

3. IPS News. “Spain’s Indignados Take to the Streets Again.” 30 May 2012.

4. Lequeux, Vincent. “Digital: What Are the DMA and the DSA?” *Toute l’Europe*, 5 December 2025.

5. Saliou, Mathilde. “Que va changer le Digital Markets Act en pratique ?” *Next.ink*, 23 March 2023.

6. Vie-publique.fr. “DSA: Objectives and Scope.” 4 August 2025.

7. Zuckerberg, Mark. “Speech at Georgetown University.” *Meta*, 17 October 2019.

ABSTRACT

This thesis undertakes to evaluate the EU legal response to the issues that new technologies cause to freedom of expression. It outlines the key phenomena associated with these technologies and their impact on the exercise of this fundamental right, before questioning the adequacy and effectiveness of the EU's legal safeguards. Thus, the aim of this research is to assess to what extent the EU legal tools are capable of protecting the exercise of freedom of expression in a context where new technologies both expand and limit it.

The research finds that current regulatory instruments, including the DSA, the DMA, the AI Act and the GDPR are still insufficient to defend freedom of expression as traditionally guaranteed under the European fundamental rights framework.

It shows that these tools address the effects rather than the underlying causes of the problem and therefore, do not constitute a sufficient protection against limitations imposed by private companies and States. As a result, this analysis points out the need for an ethical and shared governance model to face the structural restrictions that shape freedom of expression.

Keywords : freedom of expression, new technologies, limitations, insufficient legal response, ethical and shared digital governance.

SUMMARY

Title: *New technologies and freedom of expression*

This thesis explores the EU's legal and ethical frameworks addressing the growing challenges to the protection of freedom of expression posed by new technologies. While new technologies were initially perceived as mainly beneficial to freedom of expression, they appear to be vectors of surveillance, manipulation, censorship, and self-censorship, enabling new forms of limitation of freedom of expression by private companies and, more secretly, by States.

The objective is to identify the judicial problems that new technologies raise for the effective exercise of freedom of expression. It analyzes whether the EU's legal framework is adequate to regulate moderation and control powers, evaluates the interdependence between data protection and freedom of expression, and explores the need to complement the EU legal response with an ethical and shared model of digital governance.

This thesis is structured into two main parts. The first chapter provides a phenomenological context of transformations brought by new technologies, highlighting both their benefits and their risks, and examining how they have reshaped the traditional framework for protection of freedom of expression. The second chapter delves into the EU legal response, analysing strengths and limitations of existing regulatory tools, and identifying governance approaches capable of better assuring pluralism, individual autonomy, and democracy.

Through a comprehensive analysis that connects societal problems with legal reasoning, evaluates current EU legal instruments, and identifies existing regulatory gaps, the research concludes, as it stands, the EU is insufficiently prepared to ensure genuine protection of freedom of expression in this digital era. Despite the strong foundation for fundamental rights protection, the recent tools remain largely indirect, fragmented and ineffective. Therefore, the thesis also explores the need for a governance model which would contribute to addressing technical and economic infrastructures that shape expression.

This thesis concludes with a set of recommendations complementing and perfecting the EU's current approach to the structural issues of the digital era. Thus, the thesis proposed enhancing the principle of transparency and strengthened shared governance aiming to ensure a greater fairness, accountability, and respect for fundamental rights.