COMPARATIVE LAW REVIEW

# Comparative Law Review

VOL. 17 · N. 1 · 2026

SPECIAL ISSUE

## European Law and Digital Technologies

ISSN
2038 – 8993

OPEN ACCESS JOURNAL

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com



Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
VOL. 17/1 – 2026

SPECIAL ISSUE

European Law and Digital Technologies

*Edited by Federica Giovanella*

# INTRODUCTION TO THE SPECIAL ISSUE "EUROPEAN LAW AND DIGITAL TECHNOLOGIES"

*Federica Giovanella*

## I. INTRODUCTION

This Special Issue "*European Law and Digital Technologies*" collects the papers presented during the *Young Scholars' Workshop* of the same title held in Udine on September 4-5, 2025[1].

The starting point of this workshop is the increasing number of Directives and Regulations adopted by the EU in recent years, aimed at governing various digital technologies and introducing new principles, liability rules, classifications, and more.

It is well known that, in doing so, the EU seeks to position itself as a leading legal system—a model for other jurisdictions to consider when deciding whether and how to regulate technological innovation. It is also well known that, according to the now famous "Brussels Effect" formula coined by Anu Bradford[2], the EU has indeed managed to present itself, if not as a model, at least as a source of inspiration for numerous regulatory innovations beyond its borders. This represents yet another illustration of the theory of the circulation of legal models, a theme cherished—though debated—among comparatists.

Building on these considerations, the workshop aimed to explore the role of the EU in regulating digital technologies—past, present, and future—through the methodological tools of comparative law. As could be anticipated, most of the contributions address data protection, Artificial Intelligence (AI), or a combination of the two. From a comparative perspective, alongside the classical EU–US juxtaposition, some contributions focus on China. The interest in this system shows how younger scholars are well aware of the

---

[1] The papers were selected through a Call for Abstracts with a peer-review process that took place in the spring of 2025, and the drafts were discussed during the aforementioned workshop under the guidance of experienced scholars. The suggestions and comments received were then incorporated into the final versions of the papers, published here after a double-blind peer-review process. Given the excellent quality of the submitted abstracts, in addition to the papers selected for the event, other papers were accepted solely for publication in this issue.

I would like to express my gratitude to those who deserve it. The organization of the workshop could not have been possible without the support received by the University of Udine that funded the project "*Tecnologie digitali e legislazione europea*" ("Digital technologies and European law" - PSD WP2 2022-2025). The support of the administrative staff of the Department of Legal Sciences was invaluable before, during and after the workshop.

I take the chance to thank once again the brilliant colleagues who accepted to act as discussants for the papers presented during the workshop. To *Federico Costantini* (University of Udine), *Ivana Kunda* (University of Rijeka), *Rossana Ducato* (University of Aberdeen) and *Sophie Weerts* (University of Lausanne) goes my gratitude.

A big "thank you" also to the attendees of the workshop: it was a real pleasure to meet them and to see their passion for research!

[2] A. Bradford, *The Brussels Effect*, *107 Northwestern University Law Review 1* (2012); the Author later developed her study in a monograph: *The Brussels Effect: How the European Union Rules the World*, Oxford, 2019.

potential of studying a framework that is poised to become a leader not only in technological advancements but also in their regulation.

Data protection is the focus of the contribution by *Alessandro Catano*, titled "*Data protection at the gate: personal data of third-country nationals in the EU Entry/Exit System*". The paper examines the relationship between the Entry/Exit System and the most significant and impactful EU regulations on digital technologies, such as the General Data Protection Regulation (EU) 2016/679 (GDPR), the Law Enforcement Directive (EU) 2016/680 (LED), and the Artificial Intelligence Regulation (EU) 2024/1689 (AI Act). It also provides an analysis of the systems currently in use and highlights the risks that the introduction of the EES poses to the fundamental rights of third-country nationals, particularly with regard to privacy and equal treatment.

*Sara Garsia* and *Bilgesu Sumer*'s article, "*The European digital identity wallet as a tool to increase individual autonomy: from theory to critical reality*", questions digital identity management systems from the perspective of individual autonomy as a core objective of privacy and data protection, particularly in light of the GDPR and the EU Charter of Fundamental Rights. The contribution examines Self-Sovereign Identity (SSI) models and the EU's regulatory response through eIDAS 2.0, which requires Member States to issue European Digital Identity (EUDI) wallets. In concluding their analysis, the Authors highlight the risks of disproportionate data processing and surveillance in increasingly digitalised societies.

The paper "*Transatlantic debate on AI-powered facial recognition technologies: EU and US regulatory models*" by *Giulia Formici* examines the risk-based approach adopted by EU legislators in both the GDPR and the AI Act with regard to biometric surveillance technologies. It also analyzes the US framework, where biometric technologies have largely been regulated at the local or state level in the absence of comprehensive federal rules. By comparing the two scenarios, the paper highlights the main differences and similarities between the two regulatory models and assesses their ability to safeguard human identity and emotions from private and public interferences enabled by AI.

In the paper "*Affective computing-based attention monitoring in AI education: a comparative analysis of children's biometric data protection in China and the EU*", *Xiatong Bing* and *Anne Oloo* also examine biometric data protection. The study focuses on the use of AI in children's education, comparing the approaches of the EU and China and highlighting how the differences between them reflect distinct social, political, and economic contexts. At the same time, the two approaches share similarities, as both require heightened protection. Nonetheless, the Authors conclude that neither regulatory framework provides sufficient safeguards for children's fundamental rights.

The Chinese context is also examined by *Sonia Sforza* in the article "*Central bank digital currencies and privacy: a comparative analysis of regulatory approaches in the EU and China*". The Author explores the complex issues arising from the introduction of the digital euro and the e-Chinese yuan at the intersection of individual data protection, public interest, and state oversight. The paper compares the privacy frameworks of the EU and China, reflecting their different legal traditions, sociocultural contexts, and societal priorities.

Understanding these frameworks is essential for developing common standards that will enable cross-border payments and support the success of central bank digital currencies.
*Raffaele Ambrosino*'s article addresses the "*Governance profiles of the secondary use of health data in the EHDS*". The Author focuses on the European Health Data Space, approved in 2024, and its provisions concerning the secondary use of health data for research, innovation, policymaking, regulatory purposes, and personalised medicine. This secondary use may prove particularly challenging not only in light of the GDPR's application but also because healthcare is largely regulated at the national—and in some cases regional—level. The paper therefore examines the frameworks of selected Member States to clarify whether, and to what extent, the classification of health data may hinder the functioning of the EHDS.
*Gioia Codognotto*'s paper, "*Contradictions of Twin Transitions: The Environmental Impact of AI Systems from the European Union Perspective*", focuses on the tension between two major objectives pursued by the EU. The article outlines the environmental impact of AI—one of the most significant digital innovations—and explains how such impact could jeopardise the green transition. It analyses the existing legal tools available at the European level that could help mitigate the negative effects of the twin transitions, while also considering the potential of AI to address the very problems it creates.
The contribution "*Through the Artificial Intelligence Act: cross-sectional study on a pro-innovation law*" by *Gabriele Franco* offers an in-depth examination of the AI Act to determine whether it supports or, conversely, hinders innovation. While it is often argued that the AI Act constrains digital development, the Author identifies several tools within the Act that are instead designed to foster innovation in both business and workplace contexts. To this end, the Author classifies these tools as "explicit innovation measures" and "implicit innovation measures" and evaluates the effectiveness of both categories.
"*AI regulatory sandboxes as legal transplants: governance, regulatory learning and legal-technical interaction*" by *Fabio Seferi* provides a detailed analysis of the regulatory sandboxes introduced by the AI Act. The article adopts an innovative perspective by conceptualising sandboxes as legal transplants and identifying three key factors for their successful implementation: governance, regulatory learning, and legal-technical interaction. Sandboxes can function as learning tools, enabling regulators to adapt rules and best practices through experimentation, thereby acting as vectors of legal transplantation.
The use of AI by public administrations is examined in *Giulia Fantoni*'s "*The Right to Good Administration and Foundation Models: A European Governance Perspective and Best Practices*". The paper investigates how the Right to Good Administration, guaranteed by the EU Charter of Fundamental Rights, is—or may be—affected by the adoption of Generative AI within public administrations. How are key principles such as transparency, fairness, and impartiality influenced by GenAI, and to what extent? The analysis considers not only the EU legal framework but also the practical implementation of these principles in national guidelines issued by several Member States. The ultimate aim is to outline how policymakers can develop robust, rights-aligned regulatory frameworks for the use of GenAI.
*Giovanni Chieco*'s contribution, "*AI in the Legal Market: Addressing Legal Ambiguity Through a Consumer-Centric Lens*", examines the use of AI in the legal field. The Author seeks to clarify

whether LegalTech tools should be classified as products or services, given that the applicable regulatory framework—and consequently the liability regime and consumer protection rules—would differ. The article argues that a use-based, consumer-oriented approach offers the most coherent and protective framework. Despite the absence of a clear categorisation and a sector-specific regulatory regime, the paper proposes an approach that enhances legal certainty and consumer protection.

*Beatrice Marone*'s contribution, "*Escaping the regulatory lasagna: how the AI liability legislation must molt to survive*", addresses the complex issue of AI liability. The withdrawal of the proposal for the so-called "AI Liability Directive" in February 2025 has further fueled debates on how to regulate liability in the context of AI. The Author attempts to untangle this puzzle by calling the AI Act into play, while also questioning the EU's increasing reliance on regulations that, in practice, resemble directives.

In their paper "*Tokenising property*", *Veronica Zerba* and *Edoardo David Martino* focus on blockchain technologies, non-fungible tokens, and real-world asset tokenisation. The Authors show that blockchain effectively creates property rights despite—and in contrast with—traditional legal requirements. Through an economic analysis of law, the paper demonstrates that blockchain technology should be regulated to ensure consistency between tokenised property and the broader legal system.

All in all, this Special Issue brings together excellent papers addressing highly topical issues and examining technologies that, despite their side effects, are here to stay and have the potential to considerably improve our lives.

# DATA PROTECTION AT THE GATE
## PERSONAL DATA OF THIRD-COUNTRY NATIONALS IN THE EU ENTRY/EXIST SYSTEM

*Alessandro Catano*

TABLE OF CONTENTS:


*Migration management has become a central issue for developed countries. In recent years, especially due to terrorism and the breaking out of new wars, the European Union (EU) has undertaken the fundamental task of effectively implementing digital technologies to control the flow of third-country nationals within its territory.*
*There is a growing body of legislation that strives to regulate each aspect of migration with the objective of coordinating freedom of movement and security. Within this hive of laws, back in 2017 the EU adopted Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES) to register entry and exit data and refusals of entry of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes.*
*The aim of this essay is to explore how the newly operational EES impacts on the data protection framework outlined by the EU and on the main principles therein, in connection with the fundamental rights of third-country nationals.*
*The paper begins by exploring the main novelties introduced by the EES Regulation, first of all clarifying the role and scope of the EES with respect to the systems already in use (such as the EURODAC, the VIS, and the SIS II) and then dissecting its main contents. It will then go on to analyse the compliance of the EES with EU data protection law, diving into the consequences on the access to and processing of personal data. Given these insights, the essay will assess the limitations set by the new large-scale IT system to the main principles of data protection, especially investigating whether the EES creates the grounds for a violation of purpose limitation, the rights to information, access and transparency as well as the mandate of data accuracy.*
*The significance of the study cannot be underestimated, as it poses fundamental questions on the future of smart borders initiatives featuring mass data processing activities, the direction of EU law with respect to the rights of third-country nationals and the porous boundaries between the administrative and criminal sphere.*

**Keywords**: Persona data ─ data protection ─ GDPR ─ migration ─ Entry/exit System ─ fundamental rights ─ purpose limitation ─ transparency ─ data accuracy ─ large-scale IT systems

### I. INTRODUCTION

Typing a search query on a search engine in 2025 generates two particular phenomena. As for the first, it is very likely that an AI stemming from the search engine will automatically attempt to give a complete response to the question. The user may, however, decide to resort to the traditional list of websites recommended by the search engine. The second phenomenon unravels as soon as the user clicks on a specific website, as a banner will pop up asking for permissions. In order to access the information or the services provided by the website, the window will ask users to select whether they accept to relinquish the data

processed by the website, whether they would prefer the processing to be limited to the necessary data or whether they reject a collection whatsoever.

More and more frequently, this situation is mirrored at the borders of the richest countries in the world. In order to access the foreign territory, travellers are asked to relinquish their personal data to border authorities, with the difference that, in this case, travellers cannot but accept the conditions imposed by the State if they are determined to set foot in the country. In parallel, their actions, routes and information are processed by experimental artificial intelligence tools in order to predict their movements and prevent migratory emergencies.

In the past two decades, the EU has invested in a substantial number of technological projects and has created a handful of digital infrastructures in order to improve migration management and security at the borders. These digital infrastructures are mostly designed to store the personal data of travellers and use it to supplement border authorities in the identification of people on the move and in the prevention of potential threats.

The Smart Borders package[1] of the European Union promoted the implementation of a new Entry/Exit System (hereafter EES) that would collect the personal data of third-country nationals admitted for a short stay to register electronically the time and place of their entry and exit. To this goal, the Regulation (EU) 2017/2226 (hereafter EES Regulation) was adopted in 2017 to facilitate identification tasks, detect overstays and show entry bans connected to the travellers' identities. Almost 8 years after the act, nonetheless, the system has not yet become fully operative. In addition, the package includes the European Travel Information and Authorisation System (ETIAS), which will issue authorisations to visa-exempt third-country nationals planning a stay in the EU, working as a pre-border check to evaluate the existence of any security, high epidemic or illegal immigration risk. Over time, the two measures put together should replace the stamping of passports, aiming at the digitalisation of border controls[2].

The motives of interest related to these initiatives are manifold. Firstly, studying the digital infrastructures applied to migrations allows our society to better comprehend the phenomenon of "datafication" of borders, consisting in an amplified reliance on big data to direct resources for migration management and take decisions on third-country nationals[3]. Secondly, especially since the Snowden leaks, increasing attention has been devolved to the mass data processing activities performed by States, which risk paving the

[1] The initiative came from the Communication of the EU Commission of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security'.

[2] On the digitalisation of borders and bodies see F. Biondi Dal Monte, *Confini digitali e dati dei migranti nel Patto sulla migrazione e l'asilo*, in F. Biondi Dal Monte *et al.* (curr.), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa* (2024).

[3] "Datafication is not simply the process of collecting data about people, but that of transforming bodies, actions, and things into data that can be processed by algorithms" (A. Valdivia *et al.*, *Neither opaque nor transparent: A transdisciplinary methodology to investigate datafication at the EU borders*, in *Big Data and Society*, 9(2), 2 (2022)); see also M. Forti, *Errori algoritmici ai confini: questioni giuridiche e implicazioni politiche*, in F. Biondi Dal Monte *et al.* (curr.), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa*, cit., 109.

way for a new world order characterised by mass surveillance[4]. Thirdly, most scholars share the view that it would be erroneous to conceive large-scale IT systems as mere technical instruments to perform administrative tasks. Rather, databases generate their own semiotics which translates the identities of human beings into digitized figures, flagged and described by their own metrics and, thus, raise new significant political questions[5]. Fourthly, the ancillary yet ubiquitous purposes of law enforcement attached to EU databases speak for the dilution between the administrative and criminal sphere of migration management[6]. "Crimmigration"[7] is a neologism introduced to describe the contemporary geopolitical tendency to presume the foreigner as a source of threat which is due taming with the means necessary. Finally, if data protection can be regarded as non-other than a set of rules for a fair distribution of powers between those who have the authority and power to collect personal data and the people whose data are at stake[8], such asymmetry is all the more visible in the field of immigration, where travellers occupy a position of subordination and dependency towards State authorities and suffer the consequences of their own vulnerability[9]. In light of this asymmetry, the research provides useful evidence to judge whether the EES can be regarded as *proportionate*, in the technical terms developed by the CJEU pursuant to Art. 52 of the EU Charter of Fundamental Rights (EUCFR).

While a growing body of literature has examined most of the databases composing the architecture of the digitized EU borders – including the older European Dactyloscopy (Eurodac), the VISA Information System (VIS) and the Schengen Information System (SIS) –, little attention has been paid to the Entry/Exit System in particular. This study therefore aims to fill the gap in the literature and to contribute to the growing area of European research on digitized borders and data management by exploring the functionalities and the shortcomings of the new EES, in consideration of its start of operations in October 2025. The pages that follow assess the ways in which the EES relates to other databases and to the rest of the data protection framework.

This paper begins by providing the reader with a brief summary of the structure and content of the EES Regulation and a clarification of its role in the complex pool of EU IT systems (Section II). It will then examine the peculiar relationship between the EES

[4] For a thorough analysis of the mass surveillance programs in the EU see D. Bigo *et al.*, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, in *Liberty and Security in Europe*, 62, 1–60 (2013).

[5] On the ontological value of databases see R. Bellanova-G. Glouftsios, *Formatting European security integration through database interoperability*, in *European Security*, 31(3), 454–474 (2022); A. Pelizza-W. R. Van Rossem, *Scripts of Alterity: Mapping Assumptions and Limitations of the Border Security Apparatus through Classification Schemas*, in *Science, Technology, & Human Values*, 49(4), 794–826 (2024).

[6] On the topic, *inter alia*, V. Mitsilegas, *The Digital Border and the Rule of Law*, in M. Bergström-V. Mitsilegas (eds.), *EU law in the digital age* (2025); T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, (2024); D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection* (2019).

[7] J. Stumpf, *The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power*, in *American University Law Review*, 56(2), 367-419 (2006).

[8] T. Naef, *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, vol. XXVIII (2023).

[9] S. Penasa, *Intelligenza artificiale e diritti: verso un diritto "algoritmico" dell'immigrazione?,* in F. Biondi Dal Monte *et al.* (curr,), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa,* cit., 23-25.

and the EU data protection framework (Section III), exploring how the powers of designated authorities shift according to the applicable legislative act and highlighting the fundamental principles underlying the data protection regime. Section IV will assess the principles of data protection in relation to the limitations set by the EES. The main issues addressed in the Section will be: whether the EES creates the grounds for a violation of the purpose limitation principle (a); whether it guarantees the rights to information, transparency and access to the data subject (b); whether it respects the mandate of data accuracy (c). Section V will briefly deal with the potential collision between the EES and the regulation of artificial intelligence and summarise the findings of the research with some final remarks.

## II. THE ENTRY/EXIT SYSTEM

The EES is no lone wolf in the digitalisation process of EU migration management; rather, it is comprised in an intricate web of separate databases, each one provided with an own fundamental purpose (or, more realistically, multiple purposes), but jointly processing the personal data of all non-EU nationals coming to the EU.

The first wave of large-scale IT systems mainly concerned asylum applicants and criminal suspects and led to the creation of the Schengen Information System (SIS) and of the European Dactyloscopy (Eurodac). The SIS has been operative since 1995 and serves both the purposes of border management[10] and police and judicial cooperation in criminal matters[11]; it additionally facilitates the return of illegally staying TCNs[12]. Eurodac, by contrast, was created in 2002[13] as a fingerprint database used to find the Member State responsible for each asylum application but has now been expanded to become the main asylum large-scale IT system in the New Pact on Migration and Asylum[14]. The most recent addition to the EU databases for law enforcement and judicial cooperation is the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN), which should facilitate exchange of criminal records information on people on the move between Member States[15].

A second category of IT systems is mainly involved with supporting border checks, albeit preserving the possibility of law enforcement access as an additional purpose[16]. In 2008

[10] Regulation (UE) 2018/1861.
[11] Regulation (UE) 2018/1862.
[12] Regulation (UE) 2018/1860.
[13] Regulation (EC) 407/2002.
[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum, COM/2020/609 final (23.9.2020).
[15] Regulation (EU) 2019/816.
[16] For an analysis of EU databases as multi-purpose tools, see D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection*, cit.; see also European Union Agency for Fundamental Rights (hereafter EUFRA), *Under watchful eyes: biometrics, EU IT systems and fundamental rights* (2018).

the EU instituted the VISA Information System (VIS)[17] as a tool to share information on applications and previous decisions on short-stay visas and extended its scope to cover long-stay authorisations in 2021[18]. The EES and ETIAS were included in the Smart Borders Package as separated tools created to cooperate and fill the gaps on short stays in the VIS. While the EES records entries and exits in the Schengen Area, stores entry bans and detects overstayers, ETIAS issues pre-border, short-stay authorisations to visa-exempt TCNs based on shared and already available information. Both fill the gap of control over visa-exempt travellers, thereby achieving the registration into a database of every category of travellers coming to the EU.

Driven by the urgency to respond to growing security pressures – or, as Bellanova and Glouftios would refer to these and other causes, *database anxieties*[19] –, the EU opted for abandoning the compartmentalisation of databases and adopt the Interoperability Regulations[20]. Interoperability consists in creating a common portal[21] containing all the existing EU large-scale IT systems, which would be accessible to all the competent authorities based on their permissions related to each system, in order to allow communication among the databases and, hence, improve cooperation and accelerate information exchange.

The Union's EES is a large-scale IT system containing a repository storing the personal data of TCNs authorised for a short stay. It is equipped to record and show their entries and exits and entry bans and to calculate the duration of their stay in the EU, aiming at automatically identifying overstayers and alert authorities about them. The data subjects of the EES are represented by three categories of travellers[22], authorised to stay in the Schengen Area for 90 days within a period of 180 days, i.e. short-stay visa holders, visa-exempt TCNs and family members of EU citizens or citizens of an equivalent country enjoying free movement but not provided with a residence document. The EES automated calculator is not applied to the latter. Access to personal data is provided to national visa, border and immigration authorities determined by each Member State based on their own assessment of necessity and proportionality[23]. In addition, law enforcement authorities (described as designated authorities in the EES Regulation) and Europol may access the database for law enforcement purposes, precisely in relation to terrorist offences or other serious criminal offences[24]. Carriers have access to a separate daily-updated, read-only version of the database in order to verify short-stay visas[25].

It is not entirely clear whether the European Border and Coast Guard Agency (Frontex) will also be able to process personal data. On the one hand, the text of Art. 63(1) EES

[17] Regulation (EC) 767/2008.
[18] Regulation (EU) 2021/1134.
[19] R. Bellanova-G. Glouftsios, *Formatting European security integration through database interoperability*, in *European Security*, cit.
[20] Regulation (EU) 2019/817 and Regulation (EU) 2019/818.
[21] Specifically, the Interoperability Regulations introduce four new tools with the purpose of connecting the existing databases, i.e, the Common Identity Repository (CIR), the Multiple Identity Detector (MID), the Biometric Matching Service (BMS), the European Search Portal (ESP).
[22] Art. 2, Regulation (EU) 2017/2226.
[23] Arts. 9(1) and 10(1), Regulation (EU) 2017/2226.
[24] Art. 1(2), Regulation (EU) 2017/2226 laying down the legal basis for access to national LEAs and Europol.
[25] Art. 13(3), Regulation (EU) 2017/2226.

Regulation allows the agency to consult the data contained in the EES database "solely for the purposes of reporting and statistics without allowing for individual identification" and lists the information that can be transmitted for these exclusive purposes. On the other hand, the same disposition allows Frontex to process data for risk analysis and vulnerability assessments *as referred to* in Arts. 11 and 13 of its own Regulation and the Frontex Regulation includes risk analysis in Art. 11 among the specific activities that allow the Agency to process personal data[26].

The EES applies to all external borders of the EU (air, sea and land) and to some borders within the EU, namely (a) between a Schengen country and a country applying only the EES, (b) between countries applying only the EES and (c) between a Schengen and a non-Schengen country[27].

One of the most relevant and debated aspects of the system concerns which information its repository is going to store. The database distinguishes the information the authorities should collect based on whether or not the TCN holds a visa[28]. Short-stay visa holders will be first required to declare name, nationality, sex and date and place of birth. Secondly, they will provide a document or a travel document to the database, which registers their expiry date as well. Lastly, visa holders are asked to record their biometric data, hence, a facial image. Fingerprints, by contrast, are assumed to be already present in the VIS database; the Regulation therefore prevents the system from reiterating the registration of the same personal data.

Information varies according to the time of registration. At each entry, the authority signals date and time of entry, border crossing point, traveller category (whether family member of a EU citizen, visa-exempt or visa holder), number of entries authorised, duration and visa sticker number. If present, limited territorial validity of the visa, national facilitation programmes and Facilitated Transit Documents are recorded in this phase as well. On exit, by contrast, date, time and border crossing point are considered relevant and registered.

Visa-exempt travellers are required to relinquish the same data as for visa holders except for the additional obligation to provide four fingerprints from the right hand[29]. The temporary impossibility to provide fingerprints for visa-exempt travellers does not determine a refusal of entry, yet it is registered in the EES. The remaining data are registered *mutatis mutandis*, that is without the information deriving from the visa. Further information is specified when the authorisation is extended, revoked or annulled[30], when entry is rejected to the TCN[31] and when the TCN has no file or EES record[32].

[26] Art. 46, Regulation 2016/1624.
[27] Art. 4, Regulation (EU) 2017/2226.
[28] Arts. 16-17, Regulation (EU) 2017/2226. Art. 16 regulates the personal data processed on visa holders while Art. 17 regulates the personal data processed on visa-exempt TCNs.
[29] Art. 17 (1)(c), Regulation (EU) 2017/2226.
[30] Art. 19, Regulation (EU) 2017/2226.
[31] Art. 18, Regulation (EU) 2017/2226.
[32] Art. 20, Regulation (EU) 2017/2226.

Once the entry procedure is completed, the information regarding the stay of travellers is connected to an automated calculator[33]. The calculator informs travellers and the authorities of the maximum or the remaining duration of authorised stay or the number of remaining entries and, on exit, it alerts authorities on overstays[34]. Once the duration of the stay is exceeded, overstayers are automatically identified and inserted in a list which is provided to the competent national authorities of each Member State, including the personal data processed at their entry[35].

Following the principle of storage limitation, the personal data are stored in the EES central repository for a pre-determined period of time depending on the subject and on the registration of an exit[36]. In general, data is retained in the database for 3 years or only one year for family members of EU nationals. Yet, if the EES displays no exit record, the data of the traveller can be retained for 5 years, thus interpreting overstaying as a just cause to prolong the retention of the traveller's personal data.

Responsibilities in relation to the database are shared between Member States and eu-LISA[37]. For data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security and integrity, eu-LISA and Member States have an obligation to keep logs, that is documented information regarding access requests and processing operations performed by authorities[38]. National supervisory authorities and the European Data Protection Supervisor (EDPS) are granted access to the logs to enable them to monitor the processing of data and ensure full compliance with applicable data protection rules[39].

## III. LEGAL REGIMES COLLIDING: THE DATA PROTECTION FRAMEWORK

The emergence of a market of personal data resulted in the attempts of EU lawmakers as well as the CJEU to find the balance between the desire to ensure the free circulation of such data and the need to protect individuals from harm. As far as the CJEU is concerned, the Court has progressively developed its own dynamic scrutiny of proportionality to analyse the balance between the respect for the fundamental rights to private life (Art. 7 EUCFR) and the right to data protection (Art. 8 EUCFR) and objectives of general interest related to security and crime prevention. In several cases[40], the CJEU examined whether the legislative measures restricting data subjects' prerogatives respected the

33 Art. 11, Regulation (EU) 2017/2226.
34 Art. 12(1), Regulation (EU) 2017/2226.
35 Art. 12(3), Regulation (EU) 2017/2226.
36 Art. 34, Regulation (EU) 2017/2226.
37 Eu-LISA is the European agency for the operational management of large-scale information systems in the area of freedom, security and justice, established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council.
38 Art. 46, Regulation (EU) 2017/2226.
39 Arts. 56(3)-59(3), Regulation (EU) 2017/2226.
40 Cf CJEU, joint cases C-293/12 and C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources*, 08.04.2014; CJEU, case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 06.10.2015; CJEU, joint cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson*, 21.12.2016; CJEU, joint cases C-511/18, C-512/18, C-520/18, *Quadrature du Net and Others v Conseil des ministres*, 27.11.2020.

essence of the fundamental rights, the quality of law requirement and could be considered appropriate as well as the least intrusive means for achieving a legitimate objective (*strict necessity*).

As far as legislative measures are concerned, as Art. 16(2) TFEU entitled the EU to legislate on the matter, the EU established a data protection framework as a common substratum shared by the EES Regulation and the regulations of the other migration databases. The framework consists primarily of three acts: the General Data Protection Regulation (Reg. (EU) 2016/679, hereafter GDPR), the Law Enforcement Directive (Dir. (EU) 2016/680, hereafter LED) and the EU Data Protection Regulation (Reg. (EU) 2018/1725, hereafter EUDPR). These legislative acts constitute a bedrock on which the regulations of EU IT systems can thrive in fairness, each act regulating the processing of personal data as performed by different subjects and for different purposes. The GDPR is the main legislative reference in the field of data protection, as it dictates rules on the conduct of controllers and processors to safeguard the rights and interests of data subjects. The LED provides a framework for Member States governing the processing activities carried out by national law enforcement authorities (hereafter LEAs) for tasks related to criminal offences, criminal penalties or threats to public security. The EUDPR serves as data protection regulation for EU agencies, bodies and institutions. Considering its role, its content appears as a bond between the previous two pieces of legislation, setting rules for the general processing of personal data as well as for the processing in the fields of judicial and police cooperation (operational personal data).

The EES Regulation makes reference to each one of these acts in relation to cases not directly handled within its text[41]. Immigration, visa and border authorities will apply the GDPR when processing personal data for the purposes of verifying the identity and previous registrations of the TCNs, verifying whether they fulfil the conditions for their stay, accessing the automated calculator, examining and deciding on visas and national facilitation programmes[42]. The LED, by contrast, will be applied by national LEAs when they process personal data to prevent, detect or investigate terrorist acts or serious criminal offences[43]. For the same purposes, Europol will apply its own recast Europol Regulation[44], which derogates and prevails over the EUDPR as a *lex specialis*. The rules of the EUDPR will therefore only govern the processing of personal data performed by eu-LISA.

The scheme that has been described illustrates the intricacy of such a system, with a variety of standards which apply to specific sets of circumstances to cope with the different tasks and powers of each authority[45]. Interoperability will arguably complicate the picture even

41 Art. 49, Regulation (EU) 2017/2226.

42 Such uses of the EES by each category of authorities are regulated by Arts. 23-29, Regulation (EU) 2017/2226.

43 See Art. 1(2), Regulation (EU) 2017/2226, then specified by Art. 32 of the same Regulation.

44 The main text is Regulation (EU) 2016/794, which was recently modified by Regulation (EU) 2022/991.

45 E. Kosta, *The Proposed Anti-Money Laundering Authority and the Future of FIU Collaboration in Europe*, in M. Bergström-V. Mitsilegas (eds.), *EU law in the digital age*, cit., 126; see also V. Mitsilegas, *The Digital Border,* in M. Bergström-V. Mitsilegas (eds.), *EU law in the digital age*, cit., 363; T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, 178 ff. (2024).

further, by streamlining access to LEAs and other authorities and consequently challenging the permissions given by each Regulation[46].

The data protection framework contains the necessary legal grounds justifying processing activities on such data. The LED requires LEAs to process personal data only when such activity is based on Member State or Union law and it is necessary and proportionate for purposes related to criminal penalties, criminal offences or public threats. The EES Regulation restricts this possibility even further, limiting processing only to terrorist offences or another serious criminal offence and requiring evidence or reasonable grounds that it would contribute to the case.

The GDPR, by contrast, enlists a series of alternative legal grounds for the controller to process personal data legitimately. In particular, the collection of data for the EES is based on the provision of the GDPR which allows authorities to process personal data when it is necessary to perform a task carried out in the public interest or to comply with a legal obligation stemming from EU or Member State law[47] and laying down the purpose of the processing[48].

Considering that the functioning of the IT system is based on the use of fingerprints and facial images, the EES data fits the special categories of personal data, whose processing is only legitimate in the specific circumstances specified by Art. 9(2) GDPR and Art. 10 LED. Art. 9(2)(g) GDPR allows collecting biometric data for reasons of substantial public interest and on the basis of Union law. The LED requires that such data be processed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject and authorised by Union or Member State law.

Furthermore, the data protection framework places the focus on the responsibility of controllers towards data subjects. Controllers are represented by whoever determines the purposes and means of the processing[49] and, in this case, are impersonated by the subjects authorised to access the database by the EES Regulation. Data subjects, who surrender their personal data, are conferred a crucial series of rights, some of which directly exercisable against controllers. The rights of data subjects are mostly rooted in the principle of transparency and entitle the subject to gain information, access data and amend inaccuracies. While the principle of transparency is shared between the general rules of the EUDPR and the GDPR, it disappears in the LED and Chapter IX of the EUDPR, as ensuring transparent access to the information held by LEAs to the individual would disrupt police investigations.

Besides transparency, the framework establishes a common series of principles that are foundational in order to guarantee data protection. LED, GDPR and EUDPR require the processing of personal data to be lawful and fair (lawfulness), limited to a specific purpose (purpose limitation), adequate and relevant (data minimisation[50]), accurate (data accuracy),

---

[46] V. Mitsilegas, *The Digital Border*, in M. Bergström-V. Mitsilegas (eds.), *EU law in the digital age,* cit., 363; T. Quintel, *Data protection: the GDPR, the law enforcement directive and beyond*, cit., 178, 216, 218.

[47] Art. 6(c) and (e), Regulation (EU) 2016/679.

[48] Art. 6(3), Regulation (EU) 2016/679.

[49] Art. 4(7), Regulation (EU) 2016/679.

[50] It is noteworthy that while the principle limits the processing of personal data to what is necessary in the GDPR, it simply invites to a non-excessive processing in the LED.

limited to a specific time period (storage limitation) and secure (integrity and confidentiality) and require controllers to be responsible for compliance with these principles (accountability)[51]. Section IV will explore the tension between these principles and the EES, analysing whether the infrastructure is in fact able to guarantee the respect of data protection principles and the fundamental rights to private life and data protection.

## IV. THE CHALLENGES AHEAD: FUNDAMENTAL RIGHTS AND DATA PROTECTION PRINCIPLES UNDER PRESSURE

This study is unable to encompass the entire list of principles of data protection in connection with the EES Regulation. The analysis of the relationship between the EES and data protection presented here is based on the principles of purpose limitation, transparency and data accuracy, in light of their fundamental role in preserving the integrity of the framework. Subsection (a) considers the implications of a multi-purpose tool uniting law enforcement and migration management objectives on the obligation to connect processing activities to a specified, lawful purpose. Subsection (b) reviews the EES provisions on transparency, the right to information and the right to access, analysing the challenges to their effectivity. Subsection (c) is concerned with the precision of the EES database, aiming to shed light on the progress, inherent obstacles and practical issues to data accuracy. The elements gathered in the analysis of these three principles provide valuable insights into whether the EES would withstand the scrutiny of proportionality stemming from Art. 52 EUCFR.

### a. *Purpose Limitation Principle*

An episode of the TV series "Black Mirror" shows a dystopian future in which government-approved drone insects, which were originally equipped for pollination tasks substituting for extinct real bees, are hacked with the goal of killing targeted people[52]. Halfway through the episode, it is revealed that facial image recognition tools had been secretly installed in each and every high-tech bee for urgent cases undermining national security.

The principle of purpose limitation is on the front line to prevent events of function creep like those described in the episode, i.e. the expansion of a system or technology beyond its original purposes[53]. By introducing purpose limitation, fundamental rights[54] and the EU data protection framework[55] require personal data to be processed for specified, explicit

[51] Art. 4(1)(2), Directive (EU) 2016/680; Art. 5(1)(2) Regulation (EU) 2016/679; Art. 4(1)(2), Regulation (EU) 2018/1725.
[52] Reference is made to "Hated in the Nation", the sixth episode of the third season of Black Mirror, aired for the first time in 2016.
[53] B.J. Koops, *The concept of function creep, in Law, Innovation and Technology*, 13(1), 29–56 (2021).
[54] "[D]ata must be processed fairly for specified purposes" (Art. 8(2), Charter of Fundamental Rights of the European Union).
[55] See Section III.

and legitimate purposes and not be processed in a manner that is incompatible with those purposes[56]. The principle is strictly connected with the mandate to process personal data only when strictly necessary (strict necessity) and only in the relevant and adequate amount (data minimisation), preventing excessive and potentially detrimental processing activities. To the same end, controllers are asked to put in place organisational and technical measures to ensure that the systems exclusively authorise access to designated staff and for predetermined purposes (privacy by design)[57].

As mentioned in Section II, the EES pursues the parallel objectives of improving border management and tackling irregular immigration, on the one hand, and contributing to the prevention, detection and investigation of serious crimes and terrorism, on the other hand[58]. While European Union acts with multiple purposes are not illegitimate, the CJEU clarified that the purposes should be inextricably linked and connected to the appropriate legal bases and the procedures for adopting them should not be incompatible with one another[59]. The legal bases chosen for the EES Regulation are Art. 77(2)(b) and (d), allowing for measures establishing controls for the crossing of external borders, and Art. 87(2)(a) TFEU, allowing for measures concerning police cooperation to prevent and combat crime[60]. While the legal bases and their procedures for adoption are arguably reciprocally compatible, it is questionable whether the law enforcement and migration management purposes exhibit the *inextricable link* required by the CJEU[61]. In any case, the association of these legal bases incarnates the increasing dilution between criminal and migration law.

While the uses of personal data may be justified for administrative purposes, studies show a growing concern that the involvement of LEAs in data management activities would pose significant risks to the individual, causing a spillover effect[62]. To address the issue, the efforts of the EES Regulation are directed at articulating the access permissions of each authority depending on the task they are carrying out and compartmentalising purposes for access in different chapters of the Regulation[63]. The EES Regulation enlists the specific search goals, the authorities authorised to start the search for that goal, the data that can be inserted to start the search and the data that can be consulted as a consequence[64]. Law enforcement access further depends on a written and motivated

---

[56] AG Pitruzzella, Opinion of the Advocate General in *Criminal proceedings against V.S. Request for a preliminary ruling from the Spetsializiran nakazatelen sad.*, 30.06.2022, case C-205/21, para. 56.

[57] Art. 25, Regulation (EU) 2016/679.

[58] Art. 1, Regulation (EU) 2017/2226.

[59] CJEU, *Opinion 1/15* (EU-Canada PNR Agreement), 26.07.2017, paras 77-78.

[60] Surprisingly, the EU lawmakers omitted Art. 16 TFEU despite its compatibility being confirmed by the CJEU in *Opinion 1/15*. The choice reflects the focus of the legal instrument on its components for migration management more than data protection.

[61] *Id.*

[62] D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection*, cit., 28; see also T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit.

[63] Access rules are included in Chapter II (entry and use of data by competent authorities), Chapter III (use of the ees by other authorities) and Chapter IV (procedure and conditions for access to the ees for law enforcement purposes).

[64] Consider, for instance, Art. 27 (Regulation (EU) 2017/2226) firstly specifying authorised staff, data for the search and purpose and then mentioning the information open for consultation.

request sent to an independent access point, although the procedure can be delayed in urgent cases[65].

Despite these procedural barriers, the margins for access to LEAs are so broadly defined by the EES Regulation that they can easily breach the *precise purpose* requirement in data protection law. Consultation of the EES database is granted to LEAs anytime it would contribute to the prevention, detection and investigation of terrorist or serious criminal offences and for identification purposes of unknown suspects, perpetrators or suspected victims related to these cases. On the one hand, the provision does not represent a large step forward compared to the requirements set forth by the LED[66]. In particular, while the Directive calls on Member States to further specify the criminal activities which would justify processing activities, the EES makes reference to serious criminal offences if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years[67]. On the other hand, defining when a purpose is, indeed, *precise* is no straightforward operation[68]. European courts have historically preferred evaluating the specific purposes provided by state authorities rather than dictating how precise the purpose should be formulated ex ante, and Member States have so far received little guidance on the meaning of the requirement[69].

Further questions emerge as to the extent of powers of LEAs after consulting the database. LEAs may reuse the information consulted for different subsequent purposes or store the information on their own national databases, *de facto* prolonging the data retention period. As for the change of purpose, the LED applies "to all the subsequent treatment of data obtained from the EES"[70] and requires the further processing to be necessary and proportionate and the controller to be authorised for the second use[71]. These conditions reverberate the EES Regulation's conditions for first access, with the consequence that, once LEAs are provided access for the first time, they could use the same information for a number of purposes without any additional written request. A deeper interpretation of *reasonable expectation* by the Courts when testing subsequent uses might be necessary to avoid redundancy[72].

As for the transfer of EES data to national databases, the Regulation foresees that the retrieved data may be kept "in national files only where necessary in an individual case, in accordance with the purpose for which they were retrieved […] and for no longer than strictly necessary in that individual case"[73]. Therefore, verifications on whether the strict necessity principle is observed can only be performed *ex post*. In addition, an official

[65] Art. 31, Regulation (EU) 2017/2226.
[66] See Art. 1(1), Directive (EU) 2016/680.
[67] Reference is made to the list of criminal activities in Art. 2(2) of Framework Decision 2002/584/JHA.
[68] R. Te Molder *et al.*, *The principle of purpose limitation in data-driven policing: A guiding light or an empty shell?*, in *New Journal of European Criminal Law*, 14(4), 525 (2023).
[69] *Id.*.
[70] Recital 40, Regulation (EU) 2017/2226.
[71] Art. 4(2), Directive (EU) 2016/680.
[72] R. Te Molder *et al.*, *The principle of purpose limitation in data-driven policing: A guiding light or an empty shell?*, in *New Journal of European Criminal Law,* cit., 529.
[73] Art. 28, Regulation (EU) 2017/2226.

assessment conducted before the publication of the EES Regulation, the Impact Assessment of 2016, justified the transfer of the overstayers' data directly to the SIS, affirming that "it is only further processing of a percentage-wise small amount of the EES data" and that by doing so "overstayers are not criminalised" but remain identifiable to be removed or banned[74]. These arguments cannot but raise concern, because they consciously bypass the purpose limitation test on part of the Regulation and do not consider the chilling effect the transfer might have on travellers. Although the final text of the EES Regulation does not explicitly mention such a provision, it did not sink without trace, as the Regulation foresees the automatic communication to the Member States of the scheduled erasure of data on overstayers three months in advance "in order to enable them to adopt the appropriate measures"[75].

By streamlining access in favour of LEAs, interoperability might endanger the respect of purpose limitation even further, to the point of compromising it. For instance, if responsible agents are aware that additional information is contained in Eurodac, they might infer that the individual is an irregular immigrant or applied for asylum[76]. False information might encourage false suspicions in authorities, which might assume the travellers are trying to deceive them[77]. This risk is particularly tangible after the Interoperability Regulations abolished the cascading system of mandatory checks in national databases[78]. Finally, criticism on the feasibility of interoperability highlights that the project might lead to a circumvention of access rules, a reconceptualization of databases and a frustration of both *ex-ante* and *ex-post* supervisory activities[79].

Even setting aside the impact of interoperability, in spite of declarations not to add any new functionality to the passport checks, the central storing of personal data *per se* implies a risk for the traveller to lose control of their own data, which would not be present for stamped passports[80]. In the history of IT systems so far, function creeps within the single IT systems have already been spotted and compartmentalisation has not been able to contrast their inherent frictions. In 2018 the Fundamental Rights Agency of the EU (EUFRA) stated that the "EU IT systems increasingly serve purposes that were not originally envisaged"[81] and mentioned an Irish case, in which fingerprints were found to be stored in searches carried out during investigations regardless of a suspected involvement in any crime of the immigrant or asylum seeker[82].

---

[74] European Commission, Impact Assessment Report on the establishment of an EU Entry Exit System, 2016, 123.

[75] Art. 34(3), Regulation (EU) 2017/2226.

[76] D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection*, cit., 28.

[77] EUFRA, *Fundamental rights and the interoperability of EU information systems: borders and security*, 95 (2017).

[78] The cascading system represents a procedural barrier to enhance privacy protection. It forces authorities to check the presence of matching data on their own databases before requesting access to the EU IT system. On the importance of the cascading system see EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 67.

[79] T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit.

[80] D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection,* cit., 28.

[81] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights,* cit., 58.

[82] *Id.*, 61.

In sum, a thorough examination of the EES Regulation suggests that the IT system is not orphan of general rules and technical measures to satisfy the corollaries of the purpose limitation principle. Nonetheless, pending questions and grey areas emerge especially as far as access by LEAs is concerned, potentially creating the grounds for a violation of the principle. In addition, attention needs to be paid to the provisions of the Interoperability Regulations, which might disrupt the already unstable equilibrium the EES Regulation was seeking. It will ultimately depend on national and European supervisory authorities to monitor the use of EES data by LEAs and impede any abuse, especially after access has been authorised.

b. *Transparency, right to information and right to access*

Under the data protection framework and the migration databases foreigners approaching the EU for a short stay are categorised as data subjects, as their personal data is collected by national and EU authorities to fill large-scale IT systems. As such, TCNs are entitled to legal protection in the form of rights which they can exercise against the responsible authorities of Member States. The principle of transparency mentioned in Art. 5(1)(a) GDPR is the key to unlock the door of these rights to data subjects, who would otherwise wield a blind power, unaware of who is accessing which of their data and for what reason. The objective of transparency is translated in data protection into the main rights to be informed on the processing activities and to access the personal data held by the controller, in order to request rectifications, erasure, ask to complete incomplete data or restrict the processing.
The EES Regulation is founded on these rights as framed in data protection law and is additionally provided with special provisions that distinguish the rules applying to the database with respect to the general rules. Repercussions based on the application of one or the other legal regime differ considerably, and it is not difficult to get disoriented among the different applicable legal regimes. On the one hand, the GDPR sets out to ensure the highest protection possible at any moment for the data subject, adopting a policy of full transparency. On the other hand, the LED excludes transparency from its principles and provides controllers with more options to conceal the processing activities to the advantage of smoother and undisturbed investigations. This subsection identifies the rules shaping access and information rights of TCNs subject to the EES Regulation and examines some issues concerning the tasks of informing travellers responsibly allowing their access to improve transparency.

Despite the significance of the right of access[83] and its inclusion in the most prominent data protection legislation[84], in practice data entries are rarely challenged[85]. This phenomenon could have several origins, from a disbelief by people on the move on the actual effectiveness of their right, to a lack of interest and a cultural shift waiting to occur or to a simple inefficiency in the information provided by institutions and authorities.

Art. 52 of the EES Regulation allows TCNs to request access to their personal data to the competent authorities of Member States for the purposes of gaining information, restricting the use of their data, rectifying, completing or erasing incorrect data[86]. The responsible Member State shall check the accuracy of the data within 30 days and answer within 45 days from receiving the request, specifying to TCNs the action taken with respect to the data and explaining how to bring an action against their administrative decision. The requests might require fingerprints from the individual in order to identify them and such data must be erased immediately after the procedure. The request is documented by Member States and Europol and is made available to the supervisory authorities within 7 days to facilitate monitoring activities. Moreover, national supervisory authorities may assist and advise the data subject in exercising their rights to rectify, complete or erase personal data or to restrict the processing[87].

The short timing selected for authorities to respond in the EES is in line with many national administrative procedures and more ambitious with respect to the LED or to previous provisions[88]. EUFRA reports that this short deadline might be unrealistic due to heavy caseloads, administrative obstacles, necessary cooperative activities among Member States and doubts on the identity of the applicant too[89]. While requests to the SIS II can take from 10 days to four months to process, the VIS requests have so far taken on average 30-60 days, suggesting that EES requests might follow a similar pattern, with a lengthier timing in the early period of force[90].

While Art. 52 EES Regulation certainly refers to the data registered by visa, immigration or border authorities, its binding force arguably vanishes as soon as the same data comes in the hands of LEAs. Art. 58 EES Regulation governs the protection of personal data accessed by LEAs, specifying that the recast Europol Regulation or the LED might apply alternatively.

---

[83] See D. Dimitrova-P. De Hert, *The Right of Access Under the Police Directive: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, vol. 11079, 111–130 (2018).

[84] The rights of access, correction and deletion of one's own stored data are included in Arts. 15-17 GDPR and Arts. 16 and 17 LED, as well as in Art. 8(2) of the EU Charter of Fundamental Rights, Art. 8 of the Council of Europe Convention No. 108. On this point, see EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 99.

[85] *Id.*, 99-100.

[86] The access right in the EES Regulation refers to the uses in Arts. 15-18, Regulation (EU) 2016/679. The rights to data portability and to object the processing are excluded in the EES.

[87] Art. 53(2), Regulation (EU) 2017/2226.

[88] "Articles 12 and 14 Directive 2016/680 do not impose hard limits on the data controller to respond to a request by the data subject, unlike some AFSJ instruments" (D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 125).

[89] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 103–104.

[90] *Id.*

This architecture is criticised for its complexity due to three issues in particular, i.e. the variety of LEAs processing personal data, the different information systems they operate with and thus the applicability of several legal instruments on data protection[91]. Borrowing an example made for SIS II[92], if, upon request by TCNs, national LEAs disclose information to them, it is not clear whether the disclosure would also comprise the data acquired in the EES for law enforcement purposes or whether the data subject should make an explicit reference in the request. The EUFRA argues that interoperability might solve the ambiguity and simplify the procedure by allowing the data subject to gain access to the links stored in the MID by only applying once[93].

On the one hand, exercising access rights on the basis of the Europol Regulation has been described as a "lengthy and complex procedure"[94]. On the other hand, the LED is considered *prima facie* a progressive and quite protective legal act, a step forward for data protection. However, application of the LED means that the rights of access of the data subject will exhibit considerable variation depending on the Member State[95]. While the main rule in the Directive allows full access to TCNs, national laws will be decisive in providing legal bases for controllers to limit access rights in different forms and deciding when the TCN might only receive confirmation of access by LEAs or exclusively receive instructions on how to lodge a complaint[96]. Furthermore, as the Directive excludes public authorities from the definition of 'recipient', competent authorities might transfer data to migration authorities concealing information about recipients[97]. Moreover, scholars highlight that more often than not the provisions of the LED are less effective in practice than they are in the book[98]. Limitations to information on the processing activities operated by LEAs, together with the low level of expertise and the low probability of reward for lawyers might make lodging a complaint inconvenient, undermining real chances of an effective remedy[99]. Scholars appear further sceptical of the transposition of the LED in national laws. Supervisory authorities are not provided with effective investigatory and sanctioning powers to challenge controllers in national laws, with the consequence of compromising the option of indirect access[100]. Undeniably, the

[91] D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 125.
[92] *Id.*
[93] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 102.
[94] D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 126.
[95] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 100.
[96] Art. 15(3), Directive (EU) 2016/680.
[97] T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 136.
[98] C. M. Feoli - A. D. Modigliani, *Il sis fra trattamento illecito di dati, paradossi applicativi e deficit di tutela*, in F. Biondi Dal Monte *et al.* (curr.), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa*, cit., 69; T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 145.
[99] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 104.
[100] D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 123; T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 145.

circumstances seen so far cause "frictions, which take away from the effectiveness of the right of access"[101].

All this is hardly surprising. The exercise of access rights directly depends on the application of the right of information, and in particular on the capacity of controllers to inform the data subject on their entitlements. As far as the right of information is concerned, Art. 50 of the EES Regulation specifies the detailed pieces of information that are to be given to the TCN prior to data registration. The information provided to the data subjects can be summarised in four main groups. First, travellers are informed of their rights, i.e. the right to lodge a complaint to the supervisory authorities (l)[102], the right to request access for rectification purposes (h) and the right to request erasure from the list of identified persons in case of justified overstay (k). The second group of information includes the travellers' obligations, i.e. the obligation to provide general personal data as well as fingerprints and facial image to access the EU territory (b, c, d, e). Third, the traveller should obtain some pieces of information regarding their stay, e.g. the remaining duration of the stay and any entry ban or refusal of entry (f). Finally, a fourth group concerns information on the life of their personal data, i.e., the data retention period (j), the authorities provided with access and their purposes (a, i), the possibility that personal data are transferred to other parties (g) or automatically transferred to a list of identified persons in case of overstaying (k).

Choosing which pieces of information to provide to the traveller can be a tricky task, especially if priority is given to avoiding confusion more than achieving completeness. Moreover, it is how the message is conveyed which mostly determines efficacy in transparency. The EES Regulation dictates information to be given "in writing, by any appropriate means, in a concise, transparent, intelligible and easily accessible form, and it shall be made available, using clear and plain language"[103]. The information will be made available on the official website of the EES[104] and inserted in a template produced by the EU Commission to facilitate the transmission to Member States[105]. Additionally, information campaigns should be conducted regularly to inform TCNs "about the objectives of the EES, the data stored in the EES, the authorities having access and the rights of persons concerned"[106].

Notwithstanding the responsiveness of the EES, in 2018 the EUFRA revealed a general "dissociation between the duty to inform asylum applicants and how they are informed in practice" and concluded that "[t]his raises the question of how the quality of information affects procedures and on the trust in the system as a whole"[107]. The contribution by the FRA is precious to highlight the practical problems which do not emerge by merely

[101] D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 125.
[102] The letters in the paragraph refer to Art. 50(1), Regulation (EU) 2017/2226.
[103] Art. 50(2), Regulation (EU) 2017/2226. The formulation could already be found in a similar fashion in Art. 12(1), Directive (EU) 2016/680 and Art. 12(1), Regulation (EU) 2016/679.
[104] Art. 50(3), Regulation (EU) 2017/2226.
[105] Art. 50(5), Regulation (EU) 2017/2226.
[106] Art. 51, Regulation (EU) 2017/2226.
[107] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 29.

reading the regulations[108]. For instance, although the information should be shared at the moment in which fingerprints are taken in order to safeguard the TCN's rights, the latter often appear to learn about their rights later on in the procedure in fact. Most TCNs (67%) do not recall receiving any information regarding their personal data and those receiving information were mostly only informed on how data was going to be processed[109]. It should additionally be stressed that people on the move are likely to lack the linguistic and legal skills to autonomously exercise their rights to access, rectification and deletion and might well be oblivious on their existence[110]. Language barriers remain the most difficult to overcome as well as the main reason preventing a complete and clear spread of information [111] and the use of legal jargon often further complicates the content reception[112]. The workload impacts the quality of information too, as the higher the number of TCNs crossing borders is, the more difficult it is to ensure their complete understanding of the procedure[113]. Moreover, research shows that most TCNs ignore the leaflets handed by authorities due to a chronic lack of trust or interest, as they tend to prioritise other matters, are unaware of the consequences of the processing activities on the decision-making or are convinced that the information conveyed by family members or even smugglers might be more trustworthy[114]. The FRA recommended "providing information through the digital application process, in addition to including information on the application form"[115].

In sum, on paper the EES Regulation takes the rights of data subjects very seriously. Yet, its application might amplify the practical problems found in relation to similar migration databases as well as highlight the most problematic aspects with the application of the LED and consequential expansions of the LEAs' powers in the field of migration. In light of these issues, the looming rollout of the Smart Borders package will be useful to assess the readiness of the operators concerned and of the new access and information rules aiming at improving transparency and build reciprocal trust between controllers and data subjects in the migration context.

c. *Data Accuracy*

The EES is part of the vaster phenomenon of digitization of borders and datafication of migration management occurring in the European Union. The driving force behind this change is the political belief (or illusion[116]) that the use of large-scale IT systems leads to

[108] *Id.*, 33.
[109] *Id.*, 38.
[110] C.M. Feoli-A.D. Modigliani, *Il sis fra trattamento illecito di dati,* in F. Biondi Dal Monte *et al.* (curr,), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa*, cit., 84.
[111] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 34.
[112] *Id.*
[113] *Id.*, 32-34.
[114] *Id.*, 41.
[115] *Id.*, 36.
[116] M. Leese-S. Pollozek, *Not so fast! Data temporalities in law enforcement and border control*, in *Big Data & Society*, 10(1), 1–12 (2023).

the facilitation and acceleration of controls and to a consequent quality improvement due to a greater possibility of prioritization. Travellers are embedded within a rigid digital structure based on a predetermined set of information, which is replicable for each of them. Their raw data shape an identifying image carved within a digital system, with the inevitable consequence that the more erroneous the starting data is, the more dissimilar the digital result will be from the actual identity and the more pathological will be the reactions of authorities who base their decisions on such results.

Thus, accurate data is a *conditio sine qua non* for trusting the ability of digital identities to enable authorities to manage flows more efficiently and to allow an intrusion into privacy that would otherwise be futile and deleterious. The principle of data accuracy is an essential part of data protection[117] and of each migration database and sets the objective of eliminating errors and keeping data complete and up to date. Accountability for these tasks is shared between Member States, which have an obligation to ensure the accuracy and quality of biometric identifiers, and eu-LISA, which monitors whether the quality standards are followed[118].

By definition, however, large-scale IT systems, cannot be completely accurate[119]. First, it is noteworthy that the so-called *matches*, enabling the recognition of TCNs crossing the borders multiple times, are the result of a probabilistic process, which can only aim for the lowest error rate possible[120]. Secondly, the two elements of operational speed and data quality tend to be inversely proportional[121]. If, on the one hand, eu-LISA sets the aim of a response time equivalent to one second each 10 million of gallery size for the EES[122]; on the other hand, "large biometric data and low response time often translate into lower accuracy"[123].

Inaccuracies are not acknowledged exclusively in theory. In 2018 the FRA argued that "[m]ore than half of the border guards surveyed indicate that they at least sometimes experienced inaccurate, incorrect or not updated personal data in VIS or SIS II"[124]. In contrast, some experts indicate that encountering mistakes in the underlying databases happens quite often[125] and among responsible authorities "only 5 % had never encountered problems when trying to check fingerprints against VIS in the past 12 months"[126]. In the VIS, "mistakes can occur if, for example, the fingerprints are attached to the wrong person or if there are double registrations of the same person"[127]. In addition,

[117] Both Art. 5(1)(d) GDPR and Art. 4(1)(d) LED mention data accuracy among the main goals of lawful processing.
[118] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 88.
[119] CJEU, Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministers*, 21.06.2022, para. 106.
[120] *Id.*; see also EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 88.
[121] M. Leese-S. Pollozek, *Not so fast! Data temporalities in law enforcement and border control*, in *Big Data & Society* cit., 8.
[122] A. Valdivia *et al.*, *Neither opaque nor transparent: A transdisciplinary methodology to investigate datafication at the EU borders*, in *Big Data & Society*, cit., 13.
[123] *Id.*
[124] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 83.
[125] T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 56.
[126] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 90.
[127] *Id.*, 96.

"persons who should be included in VIS because of having applied for a visa frequently could not be found in the system. More than 60 % of respondents indicate that this happened at least once in […] 12 months"[128].

In considering the relatively small error rates of these databases, it is worth noting that "given the large amount of data stored, even a low percentage of mistakes may affect a significant number of people"[129]. Nevertheless, in 2022 the CJEU argued that, in spite of a substantial number of false positives, databases have proved efficient for the objectives of general interest of the EU, e.g. to prevent terrorist or other serious criminal events[130].

Fingerprints and facial image recognition tools are the most debated technologies in the system[131]. The use of facial images for identification purposes is an innovation of the EES which will be applied to each migration IT system and should ensure the same level of accuracy in spite of reducing the number of fingerprints recorded[132]. The EES Regulation dictates that facial images should be taken preferably live[133], that Member States should prepare yearly reports on the exceptional case of use of e-MRTD images and that the Commission should produce reports on the quality standards of facial images stored in the VIS every two years[134]. Although both fingerprint and facial image recognition tools have made considerable progress in the last decade, the cases of racial or gender discriminations caused by the latter and the impact of the ageing effect on both suggest there is plenty of room for research and improvement[135]. Furthermore, episodes of self-harm lowering the quality of biometrics stress the importance of building reciprocal trust among TCNs and authorities regardless of technical adequacy[136].

Errors are not limited to the automated processing of biometric data *per se*. In their analyses of data temporalities, Leese and Pollozek noticed that the efficiency of databases is influenced by at least three main factors: trade-offs, technological inscriptions and social rhythms[137].

Trade-offs refer to conflicting priorities modulating the efficiency of IT systems. A case in point is the notable difference in accuracy rate between the VIS and the SIS. While

---

128 *Id.*, 83.
129 *Id.*, 88.
130 CJEU, Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministers*, 21.06.2022, para. 124.
131 On the reaction by travellers and society to the use of these data, see European Commission, Joint Research Centre, *Study on face identification technology for its implementation in the Schengen Information System* (2019); see also EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit.
132 Recital 20, Regulation (EU) 2017/2226.
133 The facial images extracted from passports have a lower resolution and might as well belong to someone else. This provision applied Recommendation no. 8, formulated in European Commission, Joint Research Centre, *Study on face identification technology for its implementation in the Schengen Information System*, cit.
134 Art. 15, Regulation (EU) 2017/2226.
135 See Recommendation 12 (Accuracy evaluation across ethnicities and gender) and Recommendation 15 (Corrective measures for the ageing effect) in European Commission, Joint Research Centre, *Study on face identification technology for its implementation in the Schengen Information System*, cit.
136 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 50.
137 M. Leese-S. Pollozek, *Not so fast! Data temporalities in law enforcement and border control*, in *Big Data & Society* cit.

registration in the VIS prioritizes speed over accuracy[138], authorities report being more cautious when recording data in the SIS, as those data relate to a judicial or administrative national decision with respect to a specific person[139]. It does not surprise that cases of mistakes due to insufficient verification before entering data and deficiencies in updating and correcting the data are reported more frequently in the VIS with respect to the SIS[140]. Thus, a relevant factor for data accuracy appears to be linked to the perceived importance of the single IT system. The EES could not only share the same experience of the VIS but also suffer from the higher amount of mistakes originated in that database.

Technological inscriptions refer to how data is organised in the digital spaces (datastructuring), i.e. the intrinsic boundaries and limitations of these systems which influence the outputs of the inserted data, their accuracy and their expansion[141]. The EES automated calculator may exemplify a peculiar functionality potentially leading to inaccurate knowledge. By automatically labelling TCNs exceeding the authorised stay as overstayers and *blacklisting* them, the EES sets irregularity as the rule and consequently marks TCNs as irregulars. As their legitimate reasons for overstaying are only entered *ex post*, the knowledge produced by the automated calculator risks amplifying a smaller issue and reaching the wrong target.

Social rhythms refer to how IT systems come in contact with the sociotemporal ordering of phenomena, in other words how they interact with the contingencies of reality, as only in the abstract can databases guarantee full efficacy[142]. To this category we may ascribe the majority of error sources. Human errors in the procedures typically result from poor guidance or poor training. As alien alphabets and spelling difficulties have a direct impact on data quality[143], training human beings to work at borders does not only imply conveying skills of technological know-how but should also comprehend an effort of cultural mediation[144]. Increased workload and strain on the staff recording and dealing with data[145] represent further factual limitations in border management. A substantial minority of controllers stated that they did not appoint or did not know if a data quality officer was present in their organisation[146]. Travellers may communicate false data on purpose in order

---

138 Eu-LISA promoted a "zero failure to enrol" policy with regard to VIS, preventing fingerprints to be rejected because of lack of quality. See eu-LISA, *Biometrics in Large-Scale IT: Recent trends, current performance capabilities, recommendations for the near future* (2015).

139 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 85.

140 *Id.*, 82.

141 R. Bellanova-G. Glouftsios, *Formatting European security integration through database interoperability*, in *European Security*, cit.; M. Flyverbom-J. Murray, *Datastructuring—Organizing and curating digital traces into action*, in *Big Data & Society*, 5(2), 2018; A. Pelizza-W. R. Van Rossem, *Scripts of Alterity: Mapping Assumptions and Limitations of the Border Security Apparatus through Classification Schemas*, in *Science, Technology, & Human Values,* cit., 794–826.

142 M. Leese-S. Pollozek, *Not so fast! Data temporalities in law enforcement and border control*, in *Big Data & Society* cit., 2.

143 To stress this point, some people on the move have claimed that "when they transited other Member States, they did not have access to an interpreter when stating their name and date of birth, despite being unable to use or understand Latin letters" (EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 96).

144 *Id.*

145 *Id.*, 84.

146 M. Leese-F. Marugg, *Data quality in European law enforcement and border control cooperation: Findings from survey research*, in *CURATE Report no.1,* 9 (2023).

to escape a potential registration in the SIS II or Eurodac[147]. Moreover, mistakes can emerge due to procedural or substantial errors during national administrative or judicial proceedings[148].

In addition, although interoperability might be useful to rectify wrong data, some argue that it is likely to amplify the present flaws of each database[149], such as the massive presence of erroneous data, and therefore have heavier consequences on the fundamental rights of the individuals in question[150].

The EES Regulation adopted a series of measures to apply data accuracy. Member States spotting inaccuracies have an obligation to correct them immediately[151] and to examine the requests of access and rectification by data subjects[152]. Eu-LISA, as data quality observer, is tasked with creating data quality control mechanisms and common data quality indicators using anonymised data[153]. In addition, a Biometric Test Engineer is called to perform local and performance tests and accuracy tests[154].

Some additional legislative measures sharpen the focus on data quality for the rollout of the EES. The European Commission has adopted technical specifications for the quality, resolution and use of the biometric data in the EES, whereby, *inter alia*, ICAO standards are used as a reference for data quality[155]. The Data Quality Roadmap[156] examines the capacity of Member States to feed high-quality data into the relevant EU information systems and the Commission's Implementing Decisions no. 2224 and 2225 of 2021 set the quality standards for the interoperability framework[157].

Measures to improve accuracy also originate from Member States or even local initiatives and some of them can be regarded as recommended practices. In order to lower the volume of transliteration issues, some Member States ask the traveller to cross-check the transcribed personal data, fostering participation and building reciprocal trust[158]. Authorities are then invited to use accurate and transparent tools to quantify the level of uncertainty of a match and to minimise manual entries by using electronic readers and automatic verification against other data entries[159]. At the same time, the subsequent

147 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 77.
148 *Id.*
149 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 105.
150 T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 88.
151 Art. 35, Regulation (EU) 2017/2226.
152 Art. 52, Regulation (EU) 2017/2226.
153 Art. 12, Regulation (EU) 2017/1726.
154 The obligation comes from the tender documents that eu-LISA produced in relation to the creation of the Entry/Exit System: *Annex I. Executive summary LISA/2019/RP/05 EES BMS and sBMS. Contract notice.* Available at https://etendering.ted. europa.eu/cft/cft-display.html?cftId=4802 (last visited July 07, 2025).
155 Commission Implementing Decision (EU) 2019/329; see also European Commission, Joint Research Centre, *Study on face identification technology for its implementation in the Schengen Information System, cit.*
156 Council of the EU, *Roadmap for standardisation for data quality purposes*, 11824/20, Brussels, 11 November 2020, 5.
157 M. Leese-F. Marugg, *Data quality in European law enforcement and border control cooperation: Findings from survey research*, in *CURATE Report no.1,* cit., 18.
158 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 85.
159 *Id.*, 88.

verification of results by non-automated means is essential to ensure the proper functioning of the system[160].

## V. FINAL REMARKS: THE FUTURE OF THE EES

This study set out to explore the relationship between the EES and the principles stemming from the data protection framework. After summarising the features of this new large-scale IT system and comparing it to the structure of the most important pieces of legislation of the EU on data protection, Section IV has identified three main principles which are put under pressure by the system.

The investigation of the purpose limitation principle in the EES has shown the inherent ambiguities of multi-purpose tools, potentially causing spillover effects or function creeps. In spite of the rules separating access authorisations and the procedural barriers of privacy by design, the defective definition of precise purposes and, most of all, the upcoming interconnection among all migration databases constitute a risk for the integrity of the principle. The analysis of the transparency principle revealed that obstacles in conveying information and building trust with non-EU nationals concern both how to inform and what information to share. The exercise of the right to access personal data is obstructed by practical obstacles as well as by complexity in the application of both national and EU law. The findings of the study further suggest that datafication does not mean data accuracy. The contact with reality, technological inscriptions and trade-offs are among the factors impacting on the efforts by the EU to achieve the highest level of data reliability and should be taken into account in the shift towards the digitization of borders.

This paper presented some theoretical criticalities that might be confirmed once data on the rollout of the EES is available. Hence, natural progression of the research should include an examination of the new data coming from surveys at the borders.

Room for further research lies in the relationship between the EES and the newly adopted AI Act. The initial exclusion of migration databases from the scope of the AI Act suggests that functions such as the facial recognition tools are likely to include AI features which the EU is reluctant to sacrifice. The final version of the Act classifies AI tools in migration databases as *high-risk*, thus subjecting their use to specified obligations. AI is likely to add pressure to each one of the principles of data protection mentioned in Section IV. For instance, the CRRS (a component of interoperability) will be able to collect data from the EES and other databases and process it through algorithms to assist the selection of risk indicators, thus expanding the role of EES data beyond its original purpose. The opacity characterising algorithms, which are often described as "black boxes", might be detrimental to the principle of transparency and constitute an obstruction to information duties. Finally, data accuracy will be affected by algorithm biases, which could amplify errors in the databases, foster false suspicions and reinforce discrimination.

This research has provided the opportunity to gain knowledge on the provisions the EES is equipped with to protect personal data. However, these findings suggest that the system

[160] CJEU, Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministers*, 21.06.2022, para. 124.

is far from perfect and highlight the future need to monitor how authorities apply these provisions in practice. The integrity of personal data at the borders will depend on the willingness of institutions to strengthen cooperation with the EDPS, enhance the powers of supervisory authorities and implement good practices to empower TCNs and build reciprocal trust.

# THE EUROPEAN DIGITAL IDENTITY WALLET AS A TOOL TO INCREASE INDIVIDUAL AUTONOMY: FROM THEORY TO CRITICAL REALITY

*Sara Garsia – Bilgesu Sumer* *

TABLE OF CONTENTS:



*With the proliferation of online services, digital identity management (IdM) systems have become essential for both public and private interactions, giving rise to complex ecosystems of personal data. This paper critically examines two key developments in this domain: the rise of Self-Sovereign Identity (SSI) models, which emphasise individual autonomy and identity transportability through digital wallets, and the EU's regulatory response via eIDAS 2.0, which mandates the issuance of European Digital Identity (EUDI) wallets by Member States. While eIDAS 2.0 embraces some SSI principles, our analysis questions whether its implementation truly aligns with the value of autonomy as an objective of privacy and data protection, particularly under the GDPR and the EU Charter of Fundamental Rights. Using autonomy as an evaluative criterion, we investigate whether the promises of SSI have been meaningfully integrated into the regulatory architecture or remain rhetorical. In drawing this cross-domain conceptual comparison between digital identity and privacy/data protection frameworks and to make it more concrete, we explore the implications of the use of the EUDI wallet in two prospective scenarios: the European Health Data Space (EHDS) and Very Large Online Platforms (VLOPs). This exercise led us to further consider the risk that the operationalisation of EUDI wallets blurs the line between legal and non-legal digital identities, potentially enabling disproportionate data processing and surveillance in digital ecosystems.*

**Keywords**: digital identity, legal identity, eIDAS, GDPR, autonomy, Self-Sovereign Identity, European digital identity wallets.

## I. INTRODUCTION

With the widespread use of the internet, digital identity management (IdM) systems have become an indispensable component of daily life. Identity management on the internet is

*This research was supported by the European Union through the project no. 101135927 NOUS and Cybersecurity Research Program Flanders – second cycle funded by the Flemish Government. The presentation of this research at the Young Scholars Workshop "European law and digital technologies" held at the University of Udine on 4-5 September, 2025 has received funding from the Research Foundation Flanders (FWO) travel grant.

*Sara Garsia (sara.garsia@kuleuven.be), Doctoral researcher, Centre for IT & IP Law - KU Leuven University, Belgium*
*Bilgesu Sumer (bilgesu.sumer@kuleuven.be), Doctoral researcher, Centre for IT & IP Law - KU Leuven University, Belgium*

The authors contributed equally to § I, V.I, VI. In a context of mutual contribution to the conception of the paper, Sara Garsia drafted § II.I, II.II, III.I, III.II, IV.II, and Bilgesu Sumer drafted § II.III, IV.I, V.II.

a highly complex topic that spans both the public and private sectors, resulting in enormous personal data ecosystems with numerous players.

Two crucial developments can be observed in this context.

First is the emergence of the Self-Sovereign Identity (SSI) model, which aims to safeguard the autonomy and independence of natural persons from closed silos, i.e. 'transportability'. Digital wallets – essentially software that functions as a personal data store for encrypted data - are the core technical reflection of the SSI theoretical foundations.

The second development took place at the regulatory level. In the European Union (EU), the eIDAS Regulation[1] established a system of cross-border recognition of national digital legal identities, however, limited to public services and voluntary for Member States. In view of granting seamless access to public and private services, the newly approved eIDAS 2.0[2] sets up a European digital identity (EUDI) framework by mandating Member States to issue digital identity wallets. The digital identity wallet is promoted as an empowerment tool for the user/citizen in terms of control over data and privacy.[3]

Existing research has already highlighted the potential and pitfalls of digital wallets.[4] Our study builds on — and diverges from — this research, as our objective is to evaluate the eIDAS 2.0 promises in light of the notion of autonomy that is highly related to the right to personal data protection. In fact, we move from the premise that the SSI ideal is advocated by the eIDAS 2.0. and that autonomy is at the core of SSI principles and is deeply connected to the right to data protection in the General Data Protection Regulation (hereinafter GDPR).[5]

Our research question is: how and to what extent does the eIDAS 2.0 framework reflect the SSI-inspired promises of natural person autonomy and identity transportability, especially in light of the autonomy objectives of the EU privacy and data protection frameworks?

Our analysis involves a cross-domain conceptual comparison, whereby we examine the concept of autonomy within different epistemic frameworks. While the contribution does not undertake a doctrinal comparison of legal frameworks, it adopts a comparative method at the level of legal concepts and underlying normative assumptions. One of these is theoretically foundational in a technological context (e.g., eIDAS' introduction of SSI

[1] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market OJ L 257/73 (hereinafter eIDAS).

[2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework OJ L1/56 (hereinafter eIDAS 2.0.)

[3] EU Digital Identity Wallet Home - EU Digital Identity Wallet - (last visited Jan. 16, 2026).

[4] *Ex multis* B. Lukkien et al., *Barriers for Developing and Launching Digital Identity Wallets*, Proceedings of the 24th Annual International Conference on Digital Government Research, 289–299 (ACM, Gdańsk, 2023); A. Giannopoulou*, Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity,* Digital Society 2(18, 2023); L. Weigl, M. Reysner, *The Governance of the European Digital Identity Framework Through the Lens of Institutional Mimesis*, Regulation and Governance (2025).

[5] B. Sümer*, Can Self-Sovereign Identity (SSI) fit within the GDPR?: a Conceptual Data Protection Analysis (Part I)* (June 3, 2022) available at https://www.law.kuleuven.be/citip/blog/can-self-sovereign-identity-ssi-fit-within-the-gdpr-part-i/ (last visited Jul. 30, 2025); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119/1.

elements and digital identity wallets), while the other is legally embedded (e.g., privacy and data protection). Our comparison shows semantic drifts and normative tensions between the two two conceptions of the concepts (autonomy and transportability, and we also touch upon the potential governance implications of these differences. Our overarching aim is to evaluate how the stated legislative objectives of personal autonomy associated with the EUDI wallet are translated into operational provisions, by looking at the developments in specific contexts and policy areas. While our analysis concludes with recommendatory inputs for future directions for research, it does not provide fully elaborated normative recommendations.

The article is organized as follows.

We will first outline the conceptual foundations of digital identity and the stages of evolution of IdMs up to the SSI and digital identity wallets (§II). Second, we delve into the theoretical model of SSI and we conceptualise its essential properties (§III). Third, we present the baseline EU regulatory framework applying to digital identity wallets, focusing on privacy, data protection and the eIDAS 2.0 (§IV). Finally we assess how the eIDAS 2.0 framework responds to the SSI-inspired promises of natural person autonomy and identity transportability, by exploring the implications of the use of the wallet in two prospective scenarios: the European Health Data Space (EHDS)[6] and Very Large Online Platforms (VLOPs) (§ V). Given that the EUDI wallets are currently not operative,[7] we will conduct our analysis in light of the legislative text and its ongoing operationalisation through Implementing Regulations[8] and technical specifications,[9] included in the Architecture and Reference Framework (ARF).[10]

These two scenarios will allow us to respond to our initial question, by drawing a comparison between the prospective implementation of the SSI-inspired promises of natural person autonomy and identity transportability and the autonomy objective enshrined in privacy and data protection.

By answering the research question, we also incidentally explore whether the implementation of the EUDI wallets risks blurring the lines between digital legal identity and non-legal identities often used online. The lack of conceptual distinction has practical consequences, as it may involve disproportionate personal data processing, which, combined with the evolutionary features of online identification, from age verification, to

[6] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space OJ L 1/96 (hereinafter EHDS).

[7] The deadline for EUDI wallets to be operative is set for December 2026, eIDAS 2.0. art. 5a (1).

[8] The European Digital Identity Regulation - EU Digital Identity Wallet -(last visited Jan. 26, 2026).

[9] In parallel to the eIDAS 2.0. Proposal, the EU Commission published the Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework OJ L 210/51. It consists of a collaboration between the EU Commission and Member States to develop the technical architecture and reference framework (ARF), a non-binding document specifying standards and protocols. The ARF is used a basis for the Implementing Regulations, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Technical+Specifications (last visited Jul. 21, 2025).

[10] Architecture and Reference Framework (ARF) v2.7.3., available at https://eudi.dev/2.7.3/architecture-and-reference-framework-main/ (last visited Jan 15, 2026) (hereinafter ARF v2.7.3.).

gateway to all sorts of online venues, such as VLOPs and Data Spaces, points to increased surveillance.

## II. DIGITAL IDENTITY: FOUNDATIONS AND EVOLUTION

Identity is not easy to define, as it is prominently multi-faceted.[11] The word comes from the Latin *idem*, which means *the same*.[12] ISO/IEC 24760-1 defines identity as a '*set of attributes related to an entity*', regardless of whether it is natural or legal.[13] These attributes should be sufficiently distinguished within their context.[14] Therefore, identity consists of a subset of attributes limited by a framework and recognized by a State or another authority, e.g., a name and national number or an e-mail address associated with a password, with predefined boundary conditions (the context), e.g., a country or a website. This definition appears broad enough to serve as the guiding definition for our analysis. Against this premise, in this section, we will illustrate the conceptual foundations of identity, specifically in the digital dimension, and briefly retrace its main stages of evolution.

### II.1 *Foundations - From Analogue to Digital Identities*

In analogue settings, identification is required to transact only in specific cases, normally determined by the law. Entering into contracts to carry out the vast majority of daily activities does not occur prior to identification (e.g., buying public transport tickets, paying for groceries, etc.). Identification is required to access public services (e.g., healthcare), whereas in the context of private transactions, identification only takes place when it is necessary to ensure that a contract is executed in favour of a specific person and not another (e.g., insurance, banking and financial contracts, air travel). Instead, within the digital domain, users are required to identify themselves according to the variable rules adopted by each domain. This is because internet enables operations at a distance that, in the physical world, are facilitated by face-to-face interactions and require less information to be transferred. For instance, buying a book on Amazon compels users to log in with their 'Amazon identity', consisting of the association between a username and a password, while buying a book in a physical bookstore does not require a comparable check. This continuous detection of the user is fragmented since it occurs according to the different attributes defined by each domain. This is due to the absence of a unifying internet identity

[11] A. Ceyhan, *Technologization of security: Management of uncertainty and risk in the age of biometrics*, Surveillance & Society 116 (5(2) (2008).

[12] See personal identity: "*The sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not something else; individuality, personality.*" Oxford English Dictionary, available at www.oed.com/oed2/00111224 (last visited Jul. 30, 2025).

[13] ISO/IEC JTC 1/SC 27, IT Security and Privacy — A Framework for Identity Management — Part 1: Terminology and Concepts, ISO/IEC 24760-1:2019 (2nd ed. May 2019; amended 2023), § 3.1.1 (Switzerland: ISO, 2019/2023), available at https://cdn.standards.iteh.ai/samples/77582/096db3202a3d43108fee339becdbf3a4/ISO-IEC-24760-1-2019.pdf (last visited July 30, 2025).

[14] ITU (International Telecommunications Union) X.1252: Baseline Identity Management Terms and Definitions 04/202, https://www.itu.int/rec/T-REC-X.1252-202104-I/en, 4. (last visited Jul. 30, 2025).

layer that establishes '*who is connecting with what*'.[15] In this sense, the Digital Identity Guidelines of the National Institute of Standards and Technology of the US Department of Commerce (NIST) specifies that a person has normally multiple digital identities and the real-life identity of the individual behind the digital identity is usually not known. [16]
Another significant difference between analogue and digital identity is the role played by the human factor. After the initial registration of the user in a certain digital identity scheme (enrolment), the user can transact by simply providing the system with the information required, which matches the information registered (authentication).[17] This information constitutes the so-called *transaction identity*, defined as the minimum and mostly static set of identity information necessary to transact.[18] For example, when a local gym issues physical membership cards, it is more difficult to transfer them to someone else, even if it is possible; however, a human must be present for authentication. Online, a person or even a bot can create an account on a gaming platform. The platform then compares two sets of information: it is the information that is crucial for the transaction, rather than the human being.[19] Thus, the information can easily be transferred to someone else than the legitimate user.
In light of the features described, digital identity can be defined as the unique representation of a subject engaged in a specific online transaction, where the uniqueness is relative to the context of the transaction, and the representation may not align with the subject's real-life identity in the physical world.[20] To create a link between a person and their digital representation, the set of information forming the digital identity normally contains a piece of information, commonly referred to as an *identifier*.[21] Technically, it is just a pseudonym,[22] in the form of a data string, associated with the person and attached to the set of information forming the digital identity.

---

[15] K. Cameron, *The laws of Identity* (May 2005) available at www.identityblog.com/?p=352 (last visited July 30, 2025). The IP address can only trace back to the device connected to the network and the holder of the Internet connection, see J. McNamee *et al.*, *How the Internet works*, The Edri Papers, 5 (2012).
[16] NIST, SP 800-63 Digital Identity Guidelines available at NIST Special Publication 800-63-4 (last visited June 13, 2025).
[17] F. Wang, P. De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, Frontiers in Blockchain 7 (2, 2020).
[18] Sullivan refers to this concept in several publications: C. Sullivan, *Digital Identity: an emergent legal concept* (2011), 43; C. Sullivan, *Digital identity and mistake,* International Journal of Law and Information Technology 7 (20, 2012); C. Sullivan, E. Burger, *Blockchain, Digital Identity, E-government* in H. Treiblmaier and R. Beck (eds), *Business Transformation through Blockchain* 237 (2019).
[19] Sullivan, Burger, *Blockchain, Digital Identity, E-government*, 239 (2019).
[20] The definition is derived from the National Institute of Standards and Technology of the US department of commerce (NIST), see Paul A. Grassi et al., Digital Identity Guidelines (NIST Special Publication 800-63-3, 2017), confirmed by the second public draft of the ongoing revision, available at NIST Special Publication 800-63-4 (last visited Jun. 13, 2025). Similarly, A. Jøsang, *Identity Management and Trusted Interaction in Internet and Mobile Computing*, IET Information Security, 70 (8 (2) 2014).
[21] Wang, De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, 2 (2020).
[22] Note that from the EU data protection perspective such an identifier is personal data and it is unlikely to constitute a pseudonym, since 'pseudonymisation' requires that the additional information necessary to trace back the data subject "is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". On the contrary, the

II.2 *Foundations - Digital Legal Identity*

Legal identity, also referred to as *foundational identity,*[23] enables persons in most legal systems to prove their identity based on credentials conferred by the State as proof of identity in an offline (analogous) setting, e.g., a national ID document. In addition to foundational identity systems, States often develop *functional identities* to manage sector-specific cases, e.g., voting, taxation, driving license, etc.[24] However, functional identities often overlap with foundational ones, and these two categories are increasingly used digitally. For instance, in Estonia, the digital identification required for government services sets the norm for private-sector transactions;[25] and civil registration is increasingly becoming essential in accessing even basic needs in life, e.g., registering at a hospital. Still, digital 'platform approved' identities typically do not require legal identification, due to the lack of a unifying Internet identity layer between real-life identities (i.e. legally recognised) and the individual's digital identities.

In light of this, what makes a digital identity legal? A digital identity with legal value, i.e., a digital legal identity, is such only if the association between a *legally identified person* and their *identifier* is *unique*,[26] such that this unique link can be subsequently used to prove legal identity across all digital domains where an *identity check is required.*

This unique link can be set up only *outside* the digital dimension. In practice, digital legal identity is established with an initial registration (i.e., enrolment), which requires an identification *de visu.*[27]

Ensuring trust regarding the association between natural persons and their identifiers requires external intervention. States, directly or by delegation, are in a privileged position, given their role as legal identity providers.

II.3 *The Evolution of Digital Identities towards SSI*

The first-generation IdMs have been silos models, where the association between username (i.e., email address) and password is used to guarantee access to registered users. By the end of the 2000s, identity management had begun to shift towards federated identity management, commonly known as 'Single Sign-On'.[28] It is the case of Apple, Google or Meta allowing their users to sign into third-party services with their existing

function of the identifier in the context of digital identity is precisely that of anchor to a natural person, see GDPR, art. 4 (1) (5).

[23] World Bank, ID4D Practitioner's Guide: Version 1.0 (Oct. 2019), available under Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 217.

[24] The distinction between foundational and functional identity has been traced in the context of development initiatives see World Bank, ID4D Practitioner's Guide: Version 1.0 (Oct. 2019), available under Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 218.

[25] Sullivan, *Digital Citizenship and the Right to Digital Identity under International Law*, Computer Law & Security Review 475 (32, 2016).

[26] Sullivan, Burger, *Blockchain, Digital Identity, E-Government*, 236 (2019); Wang, De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, 3 (2020).

[27] Sullivan, Burger, *Blockchain, Digital Identity, E-Government*, 237-238 (2019).

[28] S. Canard *et al.*, *Identity Federation and Privacy: One step beyond*, Proceedings of the 4th ACM workshop on Digital identity management 25 (2008).

accounts. The inability of silos and federated IdMs to address digital identity fragmentation, coupled with asymmetries in the power held by providers and identity holders, has prompted research into more user-centric IdMs, focused on the properties of user consent and identity interoperability.[29]

In the 2010s, the decentralisation trend, mainly brought about by Distributed Ledger Technologies (DLTs) in the context of cryptocurrencies, has become dominant also in the digital identity debate, laying the foundations for an evolution of IdMs: the so-called self-sovereign identity (SSI), often referred to as decentralised identity.[30] Despite its increasing prominence across EU and non-EU jurisdictions, the term does not carry a single universally accepted meaning: technical definitions vary, and the idea of 'self-sovereignty' can imply different levels of control, governance, and legal entitlement in different socio-technical and legal contexts.[31] The original ideological basis of this model is rooted in the desire to overcome administrative mechanisms in the identification process, such that every individual is the source of their own identity, without the need for registration.[32] However, as an anchoring point, digital wallets are seen as the main determinants of an SSI network's level of decentralisation – that is why most regulatory frameworks and industry adoption of SSI are usually centered on wallets.[33] From a technical standpoint, it is, in fact, possible to imagine a self-sovereignty spectrum and classify digital wallets as an enforcing constraint for SSI.[34]


Figure 1. Evolution of IdMs

[29] C. Allen, *The Path to Self-Sovereign Identity* (April 26, 2016) available at The Path to Self-Sovereign Identity - Life With Alac... (last visited Jul. 23, 2025).
[30] O. Avellaneda *et al.*, *Decentralized Identity: Where Did It Come From and Where Is It Going?,* IEEE Communications Standards Magazine 10 (3(4) 2019).
[31] A. Giannopoulou*, Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity,* Digital Society 5 (2(18) 2023).
[32] https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html (February 15, 2012) (last visited Jun. 30 2025); Doc Searls, *Self-sovereign vs. administrative identity* (March 25, 2012) available at http://blogs.harvard.edu/vrm/2012/03/25/ssi/ (last visited 30 June 2025).
[33] Some even argues that the wallets should be the starting point of explaining SSI. T. Ruff, *When Explaining SSI, Start with the Wallet* (Apr. 21, 2020), available at https://rufftimo.medium.com/when-explaining-ssi-start-with-the-wallet-bee5d2af6696 (last visited July 30, 2025).
[34] While the centralized, siloed storage of identification credentials are a restriction for SSI. L. Weigl et al., *The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility*, Proceedings of the Hawaii International Conference on System Sciences, 2551 (2022). Also see M. Babel et al, *Self-Sovereign Identity and Digital Wallets,* Electronic Markets *28* (2025) 35

## III. THE THEORETICAL MODEL OF SSI

### III.1 *The ten principles of SSI*

There is no formal consensus about the characteristics that a digital identity scheme should have to be qualified as SSI, but the ten principles of self-sovereign identity presented by Christopher Allen in the blog post '*The Path to Self-Sovereign Identity*' have become a *de facto* reference to all the subsequent theoretical and technical developments.[35] These principles are: existence, control, access, transparency, persistence, portability, interoperability, consent, minimalization, protection.[36]

There is a crucial passage in Allen's blog post: '*Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating* user autonomy. *To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale*'.[37] The two key concepts are: true user control resulting in '*user autonomy*', which can be achieved only if the identity is '*transportable*'.

### III.2 *Natural Person Autonomy and Identity Transportability*

Building on Allen's conceptualisation, the two interdependent properties constantly identified by scholars, to achieve 'self-sovereignty' are: i) individual control over one's own identity and ii) independence of identity from closed environments, involving both the record/repository and the usability of identity information.[38]

The notion of 'control' is not limited to the individuals' static control over identity (e.g. refer to, update, hide).[39] It is dynamic, implying the ability to manage the information flow in a safe environment, to decide which data to disclose, to which subjects, in what cases, and with a high level of granularity.[40] Such 'true' control is more precisely defined as *autonomy of the natural person* who is the holder of the identity.[41]

---

[35] Allen, *The Path to Self-Sovereign Identity* (2016). The article is constantly referred to both by legal and ICT scholars when analysing the SSI model, see *infra* note 38 for subsequent references.
[36] *Ibid.*
[37] *Ibid.*
[38] Starting from Allen, these two concepts – with some lexical variation and nuances – are consistently used to explain the SSI model, see A. Tobin et *al.*, *The Inevitable Rise of Self Sovereign Identity*, The Sovrin Foundation 11 (8, 2017); Wang, De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion,* 9-10 (2020); Avellaneda et *al.*, *Decentralized Identity: Where Did It Come From and Where Is It Going*?, 11 (2019); K. Wagner et al., *Self-sovereign identity*, Blockchain Bundesverband, 27 (2018); A. Mühle *et al.*, *A Survey on Essential Components of a Self-Sovereign Identity*, 1 (30, 2018) Computer Science Review; U. Der *et al.*, *Self-sovereign Identity − Opportunities and Challenges for the Digital Revolution*, Arxiv Cornell University, 3 (2017).
[39] Allen, *The Path to Self-Sovereign Identity* (2016).
[40] Wang, De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, 9-10 (2020); Avellaneda *et al.*, *Decentralized Identity: Where Did It Come From and Where Is It Going*?, 11 (2019); Wagner *et al.*, *Self-sovereign identity*, 27 (2018).
[41] Allen, *The Path to Self-Sovereign Identity* (2016).

It can be argued that the property of natural person autonomy encompasses the SSI principles theorized by Allen. In fact, autonomy begins with the establishment of a representation of the natural person in the digital dimension (existence); it requires consent, (static) control, but also granular control over the information flow (minimalisation). Persistence of the identity is also included in autonomy because only ensuring the continuity of self allows the holder to manage their identity, which can evolve but needs to follow the continuity of the human being to which it belongs. Finally, no real autonomy is ensured if individuals' rights and freedoms are not respected: control over the identity data and flow presupposes the principle of protection, which provides for the full enjoyment of human rights.

While autonomy regards directly the prerogatives of the individual, the second property concerns identity data, and particularly their mobility. The identity belongs to the individual and not to a provider, and can be used across all desired domains, thereby overcoming the need for separate enrolments and subsequent authentication processes. Interoperability even when fully provided[42] does not change the fact that identity is held by a certain organisation, which locks the identity in its own site. Interoperability - here intended in the broad technical sense described by Allen as *widest possible usability* of the same identity[43] - enables the seamless movement of identities across silos, but it does not eliminate silos.[44] Instead, SSI addresses this weak spot by shaping a model where identity data are located in open 'containers',[45] connected to an infrastructure that enables the individual to both receive and transmit identity data to third parties.

This crucial passage is behind the idea of digital wallets, resembling the function of physical wallets.

This second property of the SSI model can be regarded as *transportability,* which involves the SSI principles of interoperability, portability, transparency, and access. Indeed, the mobility of identity data starts with wide usability across domains (interoperability) and evolves with independence from a single site (portability). Transportability also explains the principle of seamless access to data, enabled by the absence of a unique service provider and the principle of transparency, which allows the scheme to be open, accountable to operators and users, and independent of specific architectures.

Finally, natural person autonomy and identity transportability are complementary: as Allen points out, autonomy is enabled through transportability.[46] Ultimately, when a specific online transaction requires legal identification, the SSI model is meant to ensure a significant level of independence for the individual in the holding, management, and use of their identity information, specifically through wallets. Natural person autonomy,

[42] In federated systems, the interoperability is not full since it is limited to the members of the federation, see A. Tobin et al., *The Inevitable Rise of Self Sovereign Identity,* 7 (2017).

[43] Allen, *The Path to Self-Sovereign Identity* (2016). Note that interoperability is also a legal requirement of national electronic identity schemes under the eIDAS Regulation, confirmed under the eDAS 2.0. and enabled by common technical standards, see eIDAS 2.0., art. 12. "Seamless interoperability" is also identified in the recitals as a technological goal, see eIDAS 2.0., rec. 15, 19.

[44] A. Tobin et al., *The Inevitable Rise of Self Sovereign Identity,* 9, (2017).

[45] B. Pon et al., *Private-Sector Digital Identity in Emerging Markets*, Caribou Digital Reports 16 (2016).

[46] Note the expression "*to accomplish this"* in the passage reported *supra* in § III.I.

enabled by identity transportability, shapes an infrastructure where the identity is held directly by the individual, who can rely on it through granular disclosures. At first glance, this seems like a privacy-friendly development, but as we will argue, the wallet becoming a foundational identification tool shadows this initial ambition.

## IV. BASELINE REGULATORY FRAMEWORK APPLICABLE TO DIGITAL IDENTITY WALLETS

It is now time to delve into the EU regulatory frameworks shaping the essential features of digital identity wallets. Our legal analysis is not exhaustive, meaning that it does not consider all the possible EU legal instruments potentially applicable to digital identity wallets. Rather it surveys the two pieces of legislation that set up the European digital identity (EUDI) framework and that shape the value of autonomy within the same framework, namely the eIDAS 2.0. and the GDPR. Our selection is justified by a number of reasons. First, our contribution seeks to evaluate how the concept of autonomy is substantiated within the EUDI system, and in this regard the eIDAS 2.0. and the GDPR are the most prominent legal instruments to look at, also in consideration of space constraints. Second, these two norms are currently the ones that exert the most concrete effects on the EUDI system. EU laws that remain outside the scope of this contribution regards prominently the recent EU data regulations, other than the GDPR. Primarily, it is legitimate to question the impact of the Data Governance Act (hereinafter DGA)[47] on the EUDI systems and specifically whether EUDI wallet providers could qualify as data intermediation services[48] under the DGA.[49] However, the issue is doubtful, mainly because the establishment of a *commercial* relationship must be the aim of DGA's data intermediation services, and the requirement is not in line with the aim of the EUDI wallet, at least as an electronic identification means.[50] The ongoing revision of the EU data legislation framework,[51] including the DGA, further complicates the data governance implications of an already complex, multistakeholder system as the EUDI system, which is worthy of dedicated analysis, beyond the scope of this paper.
Therefore, it follows the analysis of the GDPR and the eIDAS 2.0.

---

[47] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) OJ L 152/1.
[48] On data intermediation services see G. Carovano, M. Finck, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy,* in Computer Law & Security Review, 50 (2023); and B. Tervel, V.K. Dessers, C. Ducuing, M. Fierens, A. Palumbo, B. Peeters and L. Stähler, *White Paper on the Definition of Data Intermediation Services* (October 2, 2023). Available at SSRN: https://ssrn.com/abstract=4589987 or http://dx.doi.org/10.2139/ssrn.4589987.
[49] See notably DGA, rec. 30 referring to personal information management systems ("PIMS"), which however do not equate to digital wallets; on PIMS see H. Janssen and J. Singh, *Personal Information Management Systems*, in Internet Policy Review (11 (2) (2022).
[50] On the notion of commercial relationship see Tervel *et al.*, *White Paper on the Definition of Data Intermediation Services* 36 (2023).
[51] The Digital Omnibus Regulation Proposal includes significant modifications to the DGA's regime on data intermediaries, particularly making their registration merely voluntary; see Proposal for a Regulation of the European Parliament and of the Council [...] (Digital Omnibus) COM(2025) 837 final and B. Lazarotto, *The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite* (December 19, 2025) available at The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite - MediaLaws (last visited Jan. 15, 2026).

IV.1 *Autonomy, the right to data protection, and the GDPR*

The evolution of digital identity regulation in the EU reflects a deep-rooted commitment to the European value of autonomy, understood as persons' right to self-determination and control over their personal data. As dissected in the previous section, the identity consists of a collection of personal data. In fact, the definition of personal data is closely intertwined with the definition of *identification*. Hence, digital identity as a regulatory field had been subject to several EU legislations before the GDPR. Each of these legislations appears to be motivated by technological and social developments affecting data protection and privacy. For instance, the advent of the Internet and the widespread use of centralised governmental databases for surveillance after the Second World War sparked the need to provide individuals with more control over their personal data.[52]

The European jurisdiction and legislation have responded to these developments with measures that protect the fundamental rights objective, e.g., the Census decision of the German Supreme Court is a seminal case in this direction.[53] This decision is crucial as it grounds individual autonomy in the control over personal data and affirms that data processing poses threats to the free development of personality.

Since 2009, with the enactment of the Lisbon Treaty, the EU's primary legal basis for personal data protection has been the EU Charter of Fundamental Rights.[54] Article 8 of the Charter has raised the level of personal data protection to that of a fundamental right and provides the main data protection principles, including fair processing, purpose specification, and legitimate basis. The Charter also includes a right to privacy in Article 7, which mirrors Article 8 of the European Convention on Human Rights (ECHR).

The rules and practices in IdM may have severe implications for the fundamental rights and freedoms set out in the EU Charter, particularly the right to the processing of personal data, as outlined in Article 8, which covers any information relating to an *identified or identifiable* individual.[55] Article 52(1) of the EU Charter establishes that limitations on rights must be recognised by law, respect their essence, and be necessary and proportionate. This requirement reinforces that the regulation of technologies, including identity management systems, must also be designed to preserve freedom, dignity, and informational self-determination.

An overview of the case law demonstrates that attributes such as identifiers and credentials qualify as personal data. For instance, in the *Linqvist* Case, the CJEU stated that a natural person's working conditions and hobbies constitute personal data.[56] Similar information is usually kept in digital wallets to create profiles of individuals as a part of their (broader)

[52] P. Hustinx, *European Leadership in Privacy and Data Protection* (2015), available at https://edps.europa.eu/sites/edp/files/publication/14-09-08_article_uji_castellon_en.pdf (last visited Jul. 31, 2025).
[53] G. Hornung, C. Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, Computer Law & Security Review 84-88 (25, 2009).
[54] Charter of Fundamental Rights of the European Union, OJ C 326/391 of 26/10/2012.
[55] GDPR, Article 4(1).
[56] Judgment of the Court of 6 November 2003, *Linqvist,* C-101/0*, EU:C:2003:596*, para 24.

database identity.[57] On the other hand, their credentials typically serve as their transaction identity, i.e., the minimum and mostly static set of identity information necessary to transact.[58]

The Court found in the *Breyer* Case that personal data may consist of several pieces that do not identify an individual separately.[59] The case concerns dynamic IP addresses, which change for every connection; however, this still allows *indirect identifiability* of data subjects by the internet service provider. In the IdM context, for instance, identifiers or credentials themselves alone may not identify an individual. However, the possibility of identifying an individual when they are combined with other identifying data is sufficient for the information to qualify as personal data. In this case, the CJEU also pointed out that identifiability depends on the sources available to the controller, who was defined as '*the natural or the legal person […] alone or jointly […] determines the purposes and means of the processing of personal data […]*'. When the controller (ISP in this case) '*has the legal means which enable it to identify the data subject without additional data,*' this is '*a means likely reasonably to be used to identify the data subject*'.[60] The broad interpretation adopted by the Court points to individual's protection as the focal point in data protection, which enables individuals to exercise control over how their identity is constructed, shared and linked across digital infrastructures. Therefore, autonomy is operationalised by the Court as both a right and a foundational value of the EU legal order.

Similarly, the GDPR has been established on these grounds, as explained by the European Data Protection Board (EDPB), '*the data subject should be granted the highest degree of autonomy as possible with respect to control over personal data within the frames of the legal basis, and to determine the use made of their personal data, as well as over the scope and conditions of that processing*'.[61]

IV.1.1. *Control in relation to Autonomy in SSI and GDPR*

In light of the broad definition of personal data enshrined in the GDPR, in SSI, several actors, such as issuers, verifiers, and SSI technical or governance boards, may assume roles that qualify them as controllers or joint controllers.[62] SSI systems concern *entities* that can be organisations, devices, or software applications.[63] On the other hand, to clearly understand their respective obligations under the GDPR, their relative capabilities, i.e., reasonably likely means available to them to identify natural persons should be assessed

[57] "'*Database identity' comprises all the data and information recorded about an individual in the database/s accessible under the scheme*" C. Sullivan, *Privacy or Identity?*, International Journal of Intellectual Property Management 290 (2, 2008).

[58] See *supra* § II.I. and note 18.

[59] "*There is no requirement that all the information enabling the identification of the data subject must be in the hands of one person*" Judgment of 19 October 2016 *Breyer*, C-582/14, EU:C:2016:779, para.43.

[60] *Breyer*, C-582/14, para 48.

[61] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and Default Version 2.0. (2020), 16-18.

[62] See Article 26 GDPR for joint controllership.

[63] ISO/IEC JTC 1/SC 27, IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts, ISO/IEC 24760-1:2019 (2nd ed. May 2019), § 3.1.1, 24.

carefully.[64] Nonetheless, in some circumstances, a set of attributes related to a non-person entity may still qualify as personal data, for example, a device ID. In such cases, device IDs such as IMEI numbers, IP addresses can be used to re-link user sessions or trace behavioural patterns of users.[65]

Some of the SSI principles closely resemble certain provisions and principles outlined in the GDPR. For example, *control* is mentioned a few times in the GDPR as an overarching objective of the Regulation.[66] More broadly, SSI and the GDPR can be said to have a common purpose: to enhance individual control over personal data. As discussed above, this control can be provided by autonomous choice. The conceptualisation of autonomy in data protection is, however, broader, encompassing empowerment and resistance to power asymmetries.[67] A significant example is the right to portability, which is similarly seen as one of the most important accomplishments of the GDPR (Article 20) and following regulatory instruments such as the Data Act, providing data subjects with a right to move their personal data from one controller to another.[68] As mentioned, SSI promotes transportability through wallets.

Although the GDPR has strengthened the measures in its predecessor directive, its effectiveness is still being questioned.[69] One of the reasons for this is that the GDPR, like its predecessor, is written with centralised databases in mind.[70] However, the technological reality is changing. As a result, the ideal of autonomy in data protection is highly challenged.

---

[64] Judgment of the Court (First Chamber) of 4 September 2025, European Data Protection Supervisor v Single Resolution Board, C-413/23 P ECLI:EU:C:2025:645. Related to this, the Digital Omnibus Regulation Proposal includes significant modifications to the scope of the personal data that should be taken into account when discussing data protection responsibility under the GDPR, see Proposal for a Regulation of the European Parliament and of the Council [...] (Digital Omnibus) COM(2025) 837 final.

[65] The UK GDPR explicitly incorporates the term 'online identifiers' into the definition of personal data. These can include details about the device an individual is using, as well as applications, tools, or protocols. ICO, What Are Identifiers and Related Factors? (Nov. 19, 2024), available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-are-identifiers-and-related-factors/ (last visited July 29, 2025).

[66] GDPR, rec. 7.

[67] F. Ferretti, *A European Perspective on Data Processing Consent through the Reconceptualization of European Data Protection's Looking Glass after the Lisbon Treaty: Taking Rights Seriously*, European Review of Private Law 473-506, (20, 2012).

[68] P. De Hert et *al., The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, Computer law & security review, 193-203 (34(2) 2018); B. Lazarotto, *The right to data portability: A holistic analysis of GDPR, DMA and the Data Act,* European Journal of Law and Technology, (15(1) 2024).

[69] W. Li *et al.*, *Mapping the Empirical Literature of the GDPR's (In-)Effectiveness: A Systematic Review,* Computer Law & Security Review 106129 (57, 2025); C. Prince *et al.*, *Online Privacy Literacy and Users' Information Privacy Empowerment: The Case of GDPR in Europe* Information Technology & People 37 (1 2024).

[70] M. Finck, *Blockchain Regulation and Governance in Europe*, (1st ed. Cambridge University Press, 2018).

IV.2 *The eIDAS 2.0 and its recall to the SSI model*

A single EU digital legal identity scheme is not feasible, as legal identity is a national prerogative.[71] Therefore, the former eIDAS set up a system of cross-border recognition of national schemes. This system proved to be limited due to its voluntary nature and the exclusion of private services.[72] Driven by the digitalisation boost caused by the COVID-19 pandemic,[73] the EU Commission published an amendment proposal in June 2021.[74] The so-called eIDAS 2.0. entered into force in May 2024.

The eIDAS 2.0. has established a 'European Digital Identity Framework', which, despite the terminology adopted, is based on a regime of interoperability among national instruments following common technical standards, aiming at facilitating the proof of digital identity within the EU. Under the eIDAS 2.0, each Member State is required to notify the EU Commission of at least one electronic identification scheme, which is then mutually recognised throughout the EU.[75] Second and most notably, the eIDAS 2.0. introduces the European Digital Identity Wallets (EUDI Wallets).[76] The wallet, whose holder can be a natural or a legal person,[77] must be issued at the national level and can be provided directly by Member States, under a mandate or independently, but with the recognition of the Member State.[78] The wallet has three 'layers': i) it is an electronic identification means, hence containing person identification data (PID); ii) it enables the holder to store, manage, and validate other information related to identity ('attribute')[79]. The attributes issued in electronic form ('electronic attestation of attributes', EAA) can be non-qualified, such as concert tickets, or qualified, such as driving licenses and diplomas.[80] Via the wallet, (Q)EAA can be selected and combined with PID and shared; iii) it allows the holder to sign, by means of qualified electronic signatures or seals.[81] The wallet must be accepted by online public services, private strategic services, and very large online

[71] eIDAS 2.0., rec. 19. However, the assurance levels required for national electronic identification schemes impose considerable constraints on Member States. See eIDAS 2.0. art. 8 (untouched by the amendments) and Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 OJ L 235/7.

[72] eIDAS, art. 6 and ff. and rec. 17.

[73] Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, (3 June 2021) SWD (2021) 124 final, 2.

[74] Proposal for a Regulation of the European Parliament and of the Council amending the Reg. (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (3 June 2021) COM (2021) 281 final.

[75] eIDAS 2.0, art. 6 and ff.

[76] *Id.*, art. 3(42) and art. 5a.

[77] Note however that for legal persons, both business and public sector bodies, the European Commission has published a separate legislative proposal on the establishment of European Business Wallets, that if approved, will substitute the EUDI wallet for legal persons, see Proposal for a Regulation of the European Parliament and of the Council on the establishment of European Business Wallets (19 November 2025) COM(2025) 838 final.

[78] eIDAS 2.0., art. 5a (2).

[79] *Id.*, art. 3 (43).

[80] *Id.*, art. 3 (44) (45).

[81] *Id.*, art. 3(42) and art. 5a.

platforms (VLOPs), while other private services remain free to not accept it.[82] The EUDI wallet is free of charge for natural persons and voluntary.[83]

The preparatory documents and the legislative text advocate the SSI model between the lines. The Explanatory Memorandum refers to a new market orientation towards the provision and use of specific attributes related to identities, instead of rigid digital identities.[84] The Impact Assessment report recognizes that society is already dealing with a '*paradigm shift*', whereby users expect '*a self-determined environment*', the so-called '*self-sovereign app-based wallets*', which allows managing person identification data, such as a national eID and other attributes under their full control.[85] The eIDAS 2.0. constantly refers to the principle of user control - in some cases accompanied by the adjectives 'full' or 'sole' - over their online identity and data,[86] and demands the selective disclosures of data and technical safeguards against tracking, correlations, and linkability of users' behaviour and data.[87]

We argued that SSI, with its properties of natural person autonomy and identity transportability, provides for a desirable model for the digital conversion of identity, including legal identity. Against the references made by the EU legislators, it is therefore relevant to consider whether and how the eIDAS 2.0. has implemented the SSI model *in concreto* and whether this implementation aligns with the concept of autonomy in the EU data protection framework.

[82] *Id.*, art. 5f. Those who rely on the EUDI wallet to provide their services are defined as "relying parties", see *id.*, art. 3(6) and 5b.
[83] *Id.*, art. 5a(13)(15).
[84] eIDAS 2.0 proposal *supra* n. 74, 1.
[85] Impact Assessment Report of eIDAS 2.0. proposal *supra* n. 73, 3.
[86] eIDAS 2.0, rec. 2, 3, 4, 13; rec. 5 and 15 (which use the expression "sole control"); art. 5a(14) stating that "Users shall have full control of the use of and of the data in their European Digital Identity Wallet".
[87] *Id.*, art. 5a (4)(a) and (16).

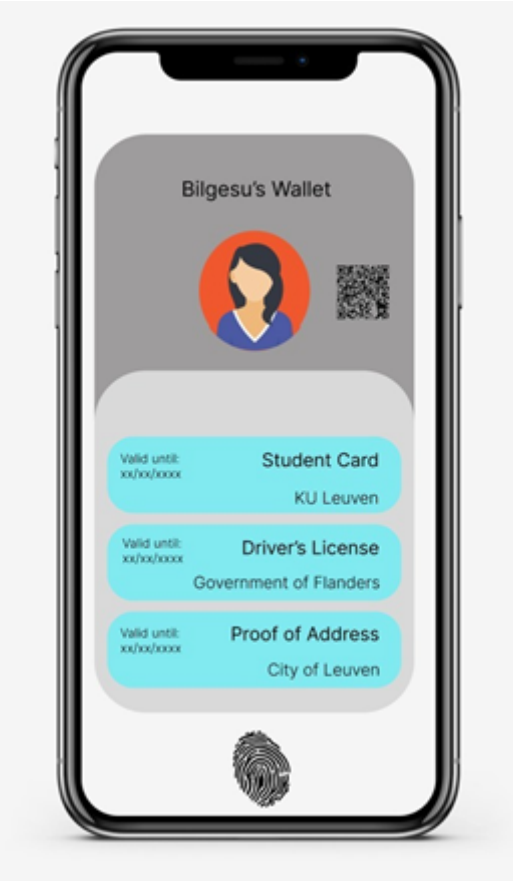



Figure 2. Representation of a digital identity wallet

## V. REALITY CHECK: EUDI WALLETS AND DEBUNKING THE BIG PROMISES

### V.1 *Testing Promises – EHDS and VLOPs*

In this section, we assess how the eIDAS 2.0 framework responds to the SSI's two primary promises: enhancing the autonomy of natural persons and the transportability of identity. We will provide prospective scenarios based on two contexts of use: the European Health Data Space (EHDS)[88] and Very Large Online Platforms (VLOPs).[89] We decided to focus on these two contexts of use since they respectively represent typical legal and non-legal identification scenarios.

The EHDS is a regulatory-technical project that led to the adoption of Regulation (EU) 2025/327, situated within the broader EU efforts to secure data sharing and harness the assumed economic, scientific, and informational value of data.[90] Specifically, the EHDS governs the cross-border access to health data both for use by patients, their

[88] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space OJ L 1/96. Hereinafter EHDS.
[89] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (DSA) OJ L 277/1, art. 33. Hereinafter DSA.
[90] EU Commission, *A European strategy for data,* COM(2020) 66 final.

representatives, health professionals, and healthcare providers (i.e., primary use)[91] and for secondary uses in view of public interest or research objectives (i.e., secondary use).[92] The intersection between the EHDS and the eIDAS framework prominently concerns the first case,[93] whereby patients are granted the right to access their personal electronic health data.[94] Member States will be responsible for establishing health data access services, and patients are entitled to rely on eIDAS for online identification. [95] The prospective use of the EUDI wallet for the overall management of health-related documents seems to be in the intentions of the EU legislator,[96] as showcased by the eIDAS 2.0 large-scale pilot dedicated to ePrescriptions, [97] launched in parallel as an electronic cross-border health service under the eHealth Digital Service Infrastructure (eHDSI).[98]

As for VLOPs, they are defined as those with more than 45 million users per month in the EU in Article 33 and Recital (76) of the Digital Services Act (DSA).[99] VLOPs that require user authentication to access their online services must support and accept EUDI Wallets for this purpose.[100] It means that VLOPs, as Meta, Amazon, and Google,[101] are required to integrate the EUDI wallet as an option for logging in, identity verification (e.g., age verification), and verification of customers' identity (so called Know your Customer "KYC" standards) for marketplaces.

V.1.1. *Natural Person Autonomy*

In line with SSI, the EUDI wallet should equip users with autonomy over their digital identity. We assess three key features of eIDAS 2.0 in light of their impact on autonomy: (i) the circulation of identifiers; (ii) the extent to which individual wallet use is externally observable; and (iii) whether wallet use remains genuinely voluntary.

Overall, the eIDAS 2.0. addresses these potential concerns to autonomy respectively by demanding (i) the 'selective disclosure' of data by the wallet; (ii) 'the unlinkability' of

[91] EHDS, art. 2 (2)(d).
[92] EHDS, art. 2 (2)(e).
[93] On the connections between Data Spaces and eIDAS Regulation, see Centre of Excellence for Data Sharing and Cloud, *Impact of eIDAS revision and EU Digital Identity landscape on data spaces* (2024).
[94] EHDS, art. 3.
[95] EHDS, art 4 and 16 and eIDAS 2.0., art. 5f.
[96] J. S. Marcus *et al.*, *The European Health Data Space,* Study Requested by the ITRE committee 25 (2022) and P. Terzis, *Compromises and Asymmetries in the European Health Data Space*, European Journal of Health Law 349, (30 (3) 2022).
[97] ARF v2.7.3., 2.6.6.1 and <ePrescription - Potential - For European Digital Identity> (last visited Jul. 21, 2025).
[98] As initiated by Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare OJ L 88/45, art. 14; see also EHDS, art. 23 and https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en (last visited Jul. 21, 2025).
[99] Also see: *Digital Strategy Europe Press Release, Digital Services Act: Commission starts collecting platform's user numbers and consults on its monitoring and investigatory procedures*, available at https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-starts-collecting-platforms-user-numbers-and-consults-its (17 February 2023) (last visited Jan 31, 2026)
[100] eIDAS 2.0., art. 5f(3).
[101] https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (last visited Jul. 31, 2025).

person identification data and other attributes every time the identification of the user is not required; (iii) the principle of voluntary use of the wallet, such that access to services, to the labour market and the freedom to conduct business is not impaired by the choice not to use the wallet.[102] In particular, how do these principles appear to be enacted in the prospective uses of the EUDI wallet?

Preliminarily, it should be pointed out that even if, in principle, the selective disclosure of data by the wallet and the unlinkability of legally identifying person identification data with other attributes are two separate properties, they are both conceptually and functionally meant to prevent the tracing of the digital life of wallet holders. Therefore, at the implementation level, it is hard to trace a dividing line between the two.

As for the selective disclosure, art. 5(4) of the Commission Implementing Regulation on the protocols and interfaces to be supported by the eIDAS Framework mainly restates the eIDAS 2.0. text.[103] The ARF specifies the standards that can be followed to ensure selective disclosure.[104] The issue of the circulation of the identifier seems to be explicitly tackled by the implementing rules addressing the unlinkability of wallet activities. The principle is implemented in the ARF with reference to the so called 'relying parties', i.e., those who accept the wallet as a gateway for the provision of their services,[105] but no guarantees are posed with regard to the wallet provider. To conceal identifiers, the use of Zero-Knowledge Proofs (ZKP) by the EUDI wallet as privacy-enhancing technologies (PETs) is promoted.[106] ZKP is a process that only discloses a cryptographic proof of a valid signature, without revealing the original key. Thus, original keys cannot be easily linked back to a specific data subject. However, different ZKP constructions offer varying levels of identifiability, and so far the ARF has not promoted a specific type of ZKP. [107]

By contrast, transaction logs, which constitute personal data from the perspective of the wallet providers, are accessible by wallet providers, provided that the access is necessary for the provision of wallet services and that the user gives their explicit consent,[108] arguably two very weak conditions to effectively safeguard unlikability.

It is then legitimate to wonder how these concerns arise in the context of the EHDS, whereby the EUDI wallet stands as a gateway for the digital interaction of the patient with health professionals and healthcare providers, given that it is likely[109] and in any case possible that the wallet provider will be a private entity.[110] It is true that the use of the wallet remains voluntary, but strong campaigns have been put in place to maximise its

---

[102] eIDAS 2.0., art. 5a (4)(a), art. 5a(16)(b), art. 5a(15). Note that art. 5a(16)(b) has a typo, where "*unlikeability*" is actually "*unlinkability*".

[103] Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 OJ L 1/7.

[104] ARF v2.7.3, 5.3.

[105] ARF v2.7.3., 7.4.3.5.2. See eIDAS 2.0., art. 3 (6) for the definition of "*relying party*".

[106] ARF v2.7.3., 7.4.3.5.3.

[107] L. Zhou *et al.*, *Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities,* Journal of Information Security and Applications 80, (103678, 2024); ARF v2.7.3., 7.4.3.5.3.

[108] Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 OJ L 1/14, art. 9(5).

[109] K. Degen, T. Teubner, *Wallet Wars or Digital Public Infrastructure? Orchestrating a Digital Identity Data Ecosystem from a Government Perspective*, Electronic Markets 20 (34, 2024) .

[110] eIDAS 2.0., art. 5a(2)(c).

adoption, [111] while the EHDS delegates the recognition of the right to opt out in primary use to Member States.[112]

As for VLOPs, the recent introduction of the age-verification obligation by DSA for adult websites demonstrates that the voluntariness of the wallet might not be applicable in every case. Users can opt for either their biometric data to be processed or use the EUDI wallet for age verification. France, for instance, now requires adult websites to implement age verification using methods such as biometric video selfies, credit card, or legal identity scanning. [113] VLOPs will thus enable their users to authenticate via EUDI wallets, based on attributes related to their legal identity, as wallets are inherently connected to this foundational identity established by governments, as will be further elaborated in V.1.2. below.

Therefore, we observe that the EUDI wallet and its technical specifications aim at introducing significant improvements in terms of autonomy for self-managing digital identities. However, the granular pieces of digital identities, i.e., personal data, can still be tracked and matched by wallet providers and online private services within this identity management network.

### V.1.2. *Identity Transportability*

One of the most challenging aspects of digital identity management to ensure identity transportability is (i) the location of the repository necessary to perform the identity check and the verification of other attributes, as these determine the primary interoperability and portability of the scheme. During the operational phase, (ii) malfunctions of the system or other critical scenarios test the system's actual ability to maintain its transportability. The eIDAS 2.0. only partially engages with these profiles.

As for repositories, the Regulation is silent, except for mandating that attributes issued on the basis of '*authentic sources*', i.e., original repositories of official information, are verifiable against those sources. [114] The Implementing Regulation on the integrity and core functionalities of European Digital Identity Wallets requires wallet providers to use secure cryptographic devices (WSCDs) to manage critical assets, such as identifiers and attributes, and to perform authentication functions.[115] The ARF specifies that the WSCD can be

---

[111] G. Comandè, M. Varilek, *The Many Features Which Make the eIDAS 2 Digital Wallet Either Risky or the Ideal Vehicle for the Transition to Post-Quantum Encryption*, Computer Law & Security Review 8, (54, 2024).

[112] EHDS, art. 10.

[113] Reuters, *Five EU States to Test Age Verification App to Protect Children* (July 14, 2025), available at: https://www.reuters.com/sustainability/boards-policy-regulation/five-eu-states-test-age-verification-app-protect-children-2025-07-14/ (last visited July 30, 2025); The Guardian, *Pornhub Owner to Suspend Site in France in Protest at New Verification Law* (June 3, 2025), available at: https://www.theguardian.com/world/2025/jun/03/pornhub-france-id-verification (last visited July 30, 2025).

[114] eIDAS 2.0., art. 45e and art. 3(47) for the definition of authentic sources.

[115] Implementing Regulation (EU) 2024/2979, art. 4(1), see also Z. Ebadi Ansaroudi *et al.*, *Secure and Reliable Digital Wallets: A Threat Model for Secure Storage in eIDAS 2.0* in S. Katsikas, B. Shafiq (eds), *Proceedings of Data and Applications Security and Privacy XXXIX: 39th IFIP WG 11.3 Annual Conference on Data and Applications Security and Privacy, Norway,* 271 and ff. (June, 2025).

either remote, local, or hybrid.[116] This raises security concerns, due to the likely delegation of the repository to the mobile operating systems manufacturers [117] or other third parties, such as cloud providers, in the absence of a proper threat model in the development of the ARF.[118]

In the context of the EHDS, this translates into a similar concern for secure electronic health data repositories.[119] The central interoperability platform MyHealth@EU is being set up through implementing acts, [120] with no guarantee that the 'repository problem' will be addressed, while the EHDS refers specifically to eIDAS identification and authentication mechanisms to facilitate '*the transferability of personal electronic health data in a cross-border context*'.[121]

In the context of VLOPs, the current ecosystems of repository-based digital identities are built on proprietary systems that collect and manage extensive user's data. The EUDI wallets are unlikely to render these underlying infrastructures obsolete. For the sake of existing business models, VLOPs are likely to retain their current digital identity management systems, which will be linked to the wallets, representing the legal identity of individuals. As there is no regulation preventing the link between the existing accounts and wallet authentication, this is a practical likelihood.

As for the operational phase, EUDI wallets can be temporarily suspended by Member States in cases of security breaches or withdrawn when the severity of the breach justifies it – without more specific indications in the law. [122] This means that all wallets of a certain type will be affected by such decisions. However, the wallet provider, which may also be a private entity,[123] is entitled to revoke the so-called Wallet Unit Attestation (WUA), a piece of information that essentially makes the wallet operational.[124] Similarly, providers of PID and of EAA are also entitled to revoke them. [125] Surprisingly, the Implementing Regulations entrust wallet, PID and EEA providers with specifying the conditions and timeframe for revocation in their own policies, without providing further guidance.[126] This represents a significant weakness of the eIDAS 2.0 framework, which does not address this point at the legislative level, *de facto* accepting the risk that providers revoke individual wallets or the essential information forming the individual digital identity (i.e., PID and EEA) at their discretion, with even major impacts when access to health files is prevented.

---

116 ARF v2.7.3., 4.5.

117 Jaromil (D. Roio), *The Seven Sins of European Digital Identity (EUDI)* (Jan. 9, 2025), available at https://news.dyne.org/the-problems-of-european-digital-identity/ (last visited July 21, 2025) .

118 See Z. Ebadi Ansaroudi et al., *Secure and Reliable Digital Wallets: A Threat Model for Secure Storage in eIDAS 2.0,* 271 and ff. (2025).

119 R. Raab et al., *Federated Electronic Health Records for the European Health Data Space*, Lancet Digit Health e841, (5, 2023).

120 EHDS, art. 23(4).

121 EHDS, art. 16(2).

122 eIDAS 2.0., art. 5e and Commission Implementing Regulation (EU) 2025/847 of 6 May 2025 OJ L1/10.

123 eIDAS 2.0., art. 5a(2)(c).

124 Implementing Regulation (EU) 2024/2979, art. 2(8) and 7; ARF v2.7.3., 4.6.3.

125 Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 OJ L1/10, art. 5.

126 See *supra* n. 123 and 124.

V.1.3. *Preliminary conclusions*

As a preliminary result of our analysis, we contend that the ambitions of the initial SSI idea have not been fully achieved.

First, we showcase that the linkability of users' behaviors by wallet providers and a wide wallet adoption – possibly leading to a network effect[127] overcoming voluntary use - hinders the promise of natural person autonomy.

Second, we argue that the promise of transportability may not be a realistic ideal, because of the likely delegation of the repository of people's attributes to the mobile operating systems manufacturers or other third parties, such as cloud providers. Meanwhile, online platforms will likely not alter their existing identity management structures.

Third, and specifically in the context of VLOPs, we observe how the current promotion of the eIDAS 2.0 framework risks linking legal identities to the identities created to access online platforms, as regulations for these platforms increasingly require strong authentication, facilitated by the reliance on government-backed ID wallets. This unavoidable emergence of 'hybrid foundational identities' appears as a consequence of the fact that the eIDAS framework directly challenges and transforms the traditional model of fragmented, non-legal identities by creating a legally grounded identity layer for the Internet. Although this is not immediately apparent, the wallet holder authentication is tied to a verified and consistent identity, based on a device binding technique, which, even if not always mandatory, is recommended or, in any case, possible, pursuant to the ARF.[128] This is a security property within the EUDI architecture that ensures that an identifier is linked to a specific wallet so that it cannot be used independently from that device.[129] For instance, Greece has launched the 'Kids Wallet' app to promote child protection across the EU. Its goal is to verify users' ages to help prevent online addiction among minors. The app uses the Greek digital ID of a parent or guardian.[130]However, security measures based on device binding do not consider that the same device may be used by different people.[131]

Based on the results of our analysis, we caution that extending a digital legal identity scheme without grounds to do so results in a legal identity check that has no equivalent in the physical realm. In essence, the scope of a digital legal identity must be considered with

[127] A.J. Zwitter *et al., Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual*, Frontiers in Blockchain 12 (3, 2020), for more about the network effect. Simliarly, Kaplane underlies how the public and private push to use the wallet "may become irresistible" as non digital authentication proves difficult; see A. Kaplane, *The European Digital Identity Wallet: A New Human Right Unlocked?*, in Nordic Journal of Human Rights, 305, 315, (43(3) 2025).

[128] ARF v2.7.3., 6.6.3.8; see also ARF v2.7.3, 5.3.2. and 5.3.3. on the standards for selective disclosure enabling device binding.

[129] *Ibid.*

[130] Greek City Times , *Greece Launches 'Kids Wallet' App to Push for EU-Wide Child Protection*, (Mar. 14, 2025), available at https://greekcitytimes.com/2025/03/14/greece-launches-kids-wallet-app-to-push-for-eu-wide-child-protection/ (last visited July 30, 2025).

[131] A. Kaplane, *The European Digital Identity Wallet: A New Human Right Unlocked?*, in Nordic Journal of Human Rights, 314, (43(3) 2025).

utmost care, and our analysis indicates that the eIDAS framework is not sufficiently equipped to handle this task.

It is essential to note that we are not arguing that the EUDI wallet is created to control individuals, but rather, we challenge the assumption and promise that it can enhance the autonomy of individuals, in the unfolding of their online identities. Now we proceed with the final step of our assessment, questioning how this preliminary conclusion relates to the data protection principle of autonomy.

### V.2. *Mismatches between eIDAS's SSI-inspired promises and autonomy as the foundation of privacy and data protection*

As explained, autonomy is one of the ultimate objectives of privacy and data protection laws – it enables data subjects to direct the processing of their personal data, and it manifests through auxiliary rights such as the right to erasure. However, the right to data protection is not an absolute right and can be limited by the GDPR or the eIDAS, as mentioned, by the extent provided in Art 52(1) of the EU Charter. However, the limitations shall be strictly necessary, as developed by a strong line of CJEU case law, rather than just being useful or convenient.

The objective of the EUDI wallets is justified as highly general, along the lines of safe, reliable and private identification. Here, first of all, there is no high-level legitimate aim for using a legally established digital identity for online services such as marketplaces. Second, less intrusive alternatives have not yet been investigated. Some techniques are suggested, such as the double anonymity, allowing selective disclosure of personal data.[132] However, it still raises questions about the residual linkability of datasets; the possibility of content providers linking tokens with cookies, which are placed by the platform before or after age verification. As mentioned, device identifiers can act as a link between this metadata. For instance, CNIL (the French Data Protection Authority) suggested to use cryptographic challenges - problems that involve encryption techniques similar to ZKPs - instead of double anonymity.[133] Another possibility is represented by Disposable Identities, designed to allow only temporally defined access, for a specific purpose and under specific circumstances or conditions.[134]

Furthermore, both eIDAS and GDPR safeguards, in addition to technical standards, should be evaluated in terms of their actual impact on the fundamental rights and

---

[132] ARCOM, *Référentiel technique sur la vérification de l'âge pour la protection des mineurs contre la pornographie en ligne (adopté le 9 oct. 2024; en vigueur depuis le 9 janv. 2025),* available at https://www.arcom.fr/sites/default/files/2024-10/Arcom-Referentiel-technique-sur-la-verification-de-age-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne.pdf (last visited July 30, 2025); Décret n° 2021-1306 du 7 octobre 2021 relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique, JORF n° 0235 du 8 octobre 2021 (France), available at https://www.legifrance.gouv.fr/eli/decret/2021/10/7/MICE2110638D/jo/texte (last visited July 30, 2025)

[133] E. Boucher, J. Gorin, CNIL – euCONSENT Speakers (YouTube video published March 2022), available at https://www.youtube.com/watch?v=fHD_sTwnATw (last visited July 30, 2025).

[134] J. Isohanni et al*., Disposable identities; enabling trust-by-design to build more sustainable data driven value*, IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 378-383 (2021).

freedoms. Meanwhile, it would be too naïve to argue that GDPR provisions are fit to achieve the data protection autonomy in the sense enshrined in the Charter.

As per article 6 of GDPR, the legal basis of performance of a contract or compliance with a legal obligation becomes the default for identification procedures. One prominent example of this is the age verification obligation introduced for the VLOPs that host adult content. While important to protect vulnerable individuals such as children, a legal identification obligation based on age verification raises concerns about the expansion of surveillance infrastructure. On the other hand, cybersecurity regulations and trust frameworks are extending such obligatory legal identification or biometric identification.[135] While not the central subject of this study, these type of practices also risks the increased use of sensitive human characteristics, such as biometric data, being used as a foundational identity, similar to the Aadhaar system in India.[136]

Based on the discussion above, we contend that establishing a standard identity layer online, founded on legal identities that permit linking a wallet to multiple relying parties, falls short of achieving autonomy, as a key proxy of privacy. This is mainly because the system is not genuinely user-controlled, as individuals have no actual choice to identify or not in most scenarios online. Legal identification impositions should require a rigorous, evidence-based justification showing that the limitation on the autonomy of individuals is the least harmful way, in accordance with the principle of necessity. In contrast, individuals are nudged to adhere to the rules of the platforms and regulations that steer us away from the initial ambitions of the decentralised internet.

## VI. CONCLUDING REMARKS

As showcased, identity has acquired a central role for digital private and public services. It follows that whoever manages these identities has a privileged view of everyone's choices and, arguably, of everyone's orientation of thoughts. The acquisition of powers by companies and governments extends beyond the function of identity in the analogue world and has given rise to theoretical and technical research on digital identity models that can preserve individuals' prerogatives.

Our study illustrated how similar terminology can conceal fundamentally different normative orientations. We analysed the different conceptions and understandings of the same principle of autonomy in privacy and data protection, as reflected in the SSI theory and its implementation. We concluded that these understandings do not align in their

[135] This approach has also been supported by the CJEU in the recent case Russmedia Digital, in which the CJEU extended online marketplace operators' data protection obligations to include the identity verification of their users. Judgment of the Court (Grand Chamber) of 2 December 2025. X v Russmedia Digital SRL and Inform Media Press SRL Case C-492/23 ECLI:EU:C:2025:935. For cybersecurity regulations, see: E. Kun, *Searching for the Appropriate Legal Basis for Personal Data Processing for Cybersecurity Purposes under the NIS 2 Directive: Legal Obligation and/or Legitimate Interest?*, Computer Law & Security Review 56 (106098, 2025).

[136] Unique Identification Authority of India (UIDAI) available at https://uidai.gov.in/ (last visited July 30, 2025); E.Kun B.Sumer, *Setting the Standard or Breaking the Rules?: European Union Institutions*, Cybersecurity Law and Personal Data Processing (2026, Springer) (upcoming book chapter).

implications, particularly when considering the technical implementation of the SSI concept.

Our observation can also be interpreted as suggesting that digital regulation in the EU might move away from its past objectives. Moreover, the analysis showcases the ongoing configuration of autonomy in European digital governance, where technological implementation risks redefining legal principles rather than realising them. Additionally, in this paper, we argued that the EUDI wallet is inseparably tied to the legal identity of the person - without a state-backed identity as the anchor, the wallet as presented cannot legally function. Thus, the adoption of the eIDAS framework by public services and its expansion to online platforms risk creating a default reliance on legally anchored digital identities. This implies revealing significant insights on a person's online life and connections, specifically from the perspective of wallet providers and identity issuers. Even if it supposedly remains optional, the EUDI wallet should not become the default method of identification for all online transactions.

Therefore, we argue that introducing the EUDI wallet, an architecture established by and connected to legal identities, blurs the line between legal and non-legal forms of identification. This grey area has not yet been fully conceptualised in the scholarship. Further theoretical research, along with the technical implementation of EUDI wallets, should investigate overlaps between legal identification and other forms of online detection and develop a digital identity theory that considers current developments.

Moreover, the proposed system does not challenge the existing power imbalances regarding the collection of personal data by relying parties. Current structures of central management will continue with the additional layer of the EUDI wallet on top, which risks further facilitating surveillance by both public and private organisations. This not only limits control over digital identity but might also create a chilling effect through the over-normalisation of constant online tracking. Without clear limits and safeguards on when and why legal identity must be verified, there is a risk that digital identity becomes a precondition to participate in the public digital sphere, which was originally designed as a free space.

Based on our analysis, legal discourse can move beyond a narrow focus on 'identity' as a static concept and instead engage with how digital systems manage identity-linked relationships as a whole. This perspective is crucial because the governance of digital identity is the first building block that determines power allocation in the digital sphere.

# TRANSATLANTIC DEBATE ON AI-POWERED FACIAL RECOGNITION TECHNOLOGIES: EU AND US REGULATORY MODELS

*Giulia Formici*[*]

TABLE OF CONTENTS:


*AI is a transformative force in the field of biometric technologies, particularly in facial recognition; it has spread rapidly to various sectors and applications. Its rise has also triggered significant risks and concerns, leading to the implementation of different regulatory solutions. This paper focuses on two influential examples: the European Union and the United States. The recently adopted EU AI Act introduced an unprecedented and comprehensive framework for AI governance with specific emphasis on remote identification systems. In the US, the regulatory scenario is fragmented, marked by ongoing debate and varying state and municipal initiatives. In the broader context of AI governance, the two models show differences and similarities. These disciplines reveal a pressing challenge: aligning facial recognition technologies with democratic values and fundamental rights.*

**Keywords**: Facial recognition technologies; biometric data; mass surveillance; artificial intelligence; fundamental rights; USA biometric legislation; AI Act.

## I. 'ALWAYS IN FOCUS, YOU CAN'T FEEL MY STARE' [1] - UBIQUITOUS BIOMETRIC SURVEILLANCE AND FUNDAMENTAL RIGHTS

Facial Recognition Technologies (FRTs) "refer to the application of automatically identifying or verifying a person from face images and videos" [2]. Verification (or authentication) relies on a one-to-one approach, assessing whether different facial images pertain to the same person, whereas identification uses a one-to-many model, comparing a query face against a dataset or watchlist[3].

---

[*] Giulia Formici, Senior Lecturer in Public Comparative Law, University of Parma, giulia.formici@unipr.it.
This paper is an outcome of the research project "AI-Biometric Systems and Fundamental Rights Protection: Legal Challenges and Regulatory Solutions in a Comparative Perspective", coordinated by Giulia Formici, granted by the University of Parma through the Action "Bando di Ateneo 2024 per la ricerca".

[1] The Section titles draw on Judas Priest's song "Electric Eye", which vividly captures the risks and concerns associated with surveillance technologies.

[2] G. Hua, *Facial Recognition Technologies*, in L.A. Schintler, C.L. McNeely (eds), *Encyclopedia of Big Data*, Cham, 475 (2022).

[3] While verification systems answer the question "Are you the one you declared to be?", identification systems respond to the more complex question: "Who are you?". Some Authors also identify a third form of facial processing' technologies, "ones that seek to infer what someone is like, or even how someone is feeling", aimed at inferring emotional states, behavioural intention and specific characteristics connected to gender, age, ethnical origins" (N. Selwyn *et al*, *FRTs. Key Issues and Emerging Concerns*, in R. Matulionyte, M. Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge, 12 (2024). To delimit the scope of this paper, the analysis will focus primarily on identification systems.

These technologies have advanced considerably in recent years, largely due to Artificial Intelligence (AI), deep learning techniques, data computing and sophisticated algorithms[4]. Today, FRTs are not only deployed in controlled environments, e.g. borders, airports and sensitive institutional locations, but also in "uncontrolled environments". They draw on "unconstrained visual sources"[5], including photos and videos uploaded online or captured by surveillance cameras. Such operations can be performed either in *real-time*, capturing, comparing and identifying faces almost instantaneously using live or near-live material[6], or retrospectively (*post*) using photographs in existing databases[7].

Given these technical capabilities, FRTs have become one of the most widely adopted and intensively used AI-powered biometric systems[8]. They are pervasive in everyday life, from authentication tools that secure our smartphones or grant access to specific places (e.g. banks), to large-scale identification systems implemented in train stations, stadiums, public spaces and at national borders[9]. Public and private actors alike have been quick to embrace FRTs, particularly in areas such as security, law enforcement, migration control, prevention of disorder and terrorist attacks, as well as in employee identification and humanitarian operations[10].

However, as FRTs rapidly expand, concerns have mounted. Looking at technical shortcomings, these systems remain fallible, with accuracy strongly dependent on dataset quality, and vulnerable to "face variations"[11]. Many studies have documented algorithmic bias and disproportionate error rates in relation to skin colour and texture, gender and racial/ethnic background[12]. The unique and irreplaceable nature of facial images as biometric data[13] adds further complexity: unlike passwords, facial patterns cannot be altered or replaced in the event of data breaches. Beyond these technical and security

[4] A. Akbari, *Facial Recognition Technologies 101: Technical Insights*, in R. Matulionyte, M. Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition*, quot., 29 ff.

[5] G. Hua, *Facial Recognition Technologies*, quot., 475.

[6] R. Pereira, *Remarks on the Use of Biometric Data Systems (and FRTs) for Law Enforcement Purposes*, in D. Vicente *et al* (eds), *The Legal Challenges of the Fourth Industrial Revolution. The European Union's Digital Strategy*, Cham, 206 (2023).

[7] A.R. Martinez, *The Debiasing Paradox: Facial Recognition Technology and Biometric Identification Systems in the Artificial Intelligence Act*, in C. van Oirsouw *et al* (eds), *European Yearbook of Constitutional Law 2023. Constitutional Law in the Digital Era*, Cham, 147 (2024).

[8] These can be defined as tools able to "identify or verify the identity or a claim of persons on the basis of the automated measurement and analysis of their biological (such as fingerprints and iris) or behavioural (such as signature and voice) characteristics", E.J. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Cham, 1 (2013). Such systems, based on biometric data and biometric datasets, have been integrated, in recent times, with AI. On these tools and the technical impact of AI, see C. Posthoff, *Artificial Intelligence for Everyone*, Cham (2024).

[9] More generally, on AI-powered biometric systems, see M. Smith, S. Miller, *Biometric Identification, Law and Ethics*, Cham, 2021; A.K. Jain *et al* (eds), *Introduction* to *Biometrics*, Cham (2nd ed. 2025).

[10] For an overview of the FRTs uses and market, S.M. Taylor, *FRT in 'Bloom': Beyond Single Origin Narratives*, in R. Matulionyte, M. Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition*, quot., 44 ff.

[11] A.M. Martinez, *Face Recognition, Overview*, in S. Li, A. K. Jain (eds), *Encyclopedia of Biometrics*, quot., 506. On algorithmic bias see FRA, *Bias in Algorithms – AI and Discrimination* (2022).

[12] L. Moy, *Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions*, in 30 William & Mary Bill of Rights J, 337 ff. (2021); E. Haber, *Racial Recognition*, 43 *Cardozo L Rev*, 71 ff. (2021).

[13] "Biometrics include all automated processes used to recognise an individual by quantifying physical, physiological or behavioural characteristics (fingerprints, iris structure, voice, gait, blood vessel patterns, etc.). These characteristics are defined as biometric data, because they allow or confirm the unique identification of that person", EDPB, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, 7 (26 April 2023).

issues, additional risks emerge from function creep, when FRTs are applied beyond their original purpose[14], and from "unintentional collection of additional information"[15].
Thus, the misuse of FRTs may not only affect data protection and privacy but also generate a broader "chilling-effect" on other fundamental rights[16]. Core democratic freedoms, such as freedom of expression and assembly, may be undermined by technologies that foster a constant sense of surveillance[17]. Bulk and indiscriminate processing of biometric data also threatens the presumption of innocence, while opaque and pervasive use of FRTs can erode due-process safeguards[18].
These warnings, coming from different sources, including companies active in the field[19], prompted discussions to establish regulatory frameworks for the governance of AI and/or specifically FRTs, heading to diverse approaches. In recent years, we have witnessed bans, moratoria, but also more comprehensive disciplines in the direction of specific constraints, conditions and limitations of FRTs for various purposes.
Against this backdrop, the present paper examines the different legislatives paths and regulatory solutions adopted to govern FRTs in two influential models: the European Union (EU) and the United States of America (US). In both contexts, widespread use of these technologies – especially by law enforcement authorities – has elicited concern and calls for legislative intervention. Although the case law is still limited on both sides of the Atlantic, regulatory activity has intensified, without yet settling the question. Emerging in democratic systems[20], the EU and US approaches are noteworthy because of their advanced stages of development and because they exemplify the broader challenge of (re)affirming the centrality of fundamental rights and the rule of law in an age of AI-driven surveillance technologies.
Section II explores the EU supranational framework and the recently adopted AI Act[21]. This ambitious act seeks to establish comprehensive governance of AI-systems, with special attention to biometric technologies, including real-time or post Remote Biometric Identification (RBI) systems, among which FRTs.
Section III considers the US context, where the absence of a federal law directly addressing FRTs has led to a fragmented regulatory landscape with various solutions at state and, in some notable cases, even at municipal level.

---

[14] P. Cabana, *Technical and Legal Challenges of the Use of Automated Facial Recognition Technologies for Law Enforcement and Forensic Purposes*, in A. Zavrsnik, K. Simoncic (eds), *Artificial Intelligence, Social Harms and Human Rights*, London, 46 (2023).
[15] i.e. additional medical information or ethnic origin that can be deduced from FRTs.
[16] P. De Hert, *Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Debate*, in P. Campisi (ed), *Security and Privacy in Biometrics*, Cham, 369 ff. (2013); N. Rautenberg, D. Murray, *Making Tangible the Long-Term Harm Linked to the Chilling Effects of AI-Enabled Surveillance: Can Human Flourishing Inform Human Rights?*, in Hum Rights Rev, 293 (1, 2024).
[17] EDPB, *Guidelines 05/2022*, quot.; United Nations High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, UN Doc. A/HRC/44/24, 24 June 2020.
[18] I. Neroni Rezende, *Facial Recognition for Preventive Purposes*, in L. Winter, S. Ruggeri (eds), *Investigating and preventing crime in the digital era*, Cham, 67 ff. (2022); P. Fussey, D. Murray, F*acial Recognition Surveillance. Policing and Human Rights in the Age of Artificial Intelligence*, Oxford, 2025.
[19] IBM, Amazon, Microsoft, as reported by the European Parliamentary Research Service, *Regulation of Facial Recognition in the EU*, Brussels, 2021.
[20] G. Mobilio, *FRTs: Threats or Opportunities for Democracy?*, in N. Menendez Gonzalez, G. Mobilio (eds), *Next Democratic Frontiers for FRT*, Cham, 13 (2025) for reflections on how authoritarian regimes have implemented FRTs as tools of "digital authoritarianism".
[21] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

The final Section takes a comparative perspective, highlighting divergences and areas of convergence as well as trends common to the two legal systems. This analysis is framed in the broader debate on AI governance and democratic values, underscoring the urgent need to align FRTs with the protection of fundamental rights.
As Nobel Laureate in Physics (2024) Geoffrey Hinton warned, AI demands the "urgent and forceful attention of governments and international organizations"[22]. Embodying the promise and perils of rapid technological progress, FRTs encapsulate the broader challenges unleashed by the sudden rise of AI.

## II. 'I AM PERPETUAL, I KEEP THE COUNTRY CLEAN' - EU REGULATORY EFFORTS IN THE FIELD OF BIOMETRIC IDENTIFICATION SYSTEMS: WHEN PROHIBITIONS MEET EXCEPTIONS

In the EU, the main legislative act currently providing a harmonized framework for FRTs is the AI Act.
This Regulation did not emerge in a legal vacuum: earlier safeguards were established by the General Data Protection Regulation (GDPR)[23], the Law Enforcement Directive (LED)[24], as well as rulings by national and supranational Courts and interventions by Member State Data Protection Authorities (DPAs)[25]. These measures identified issues and challenges, enhancing guarantees and limiting indiscriminate and generalized biometric surveillance. Nonetheless, "these various norms, which have different targets and are from multiple sources, create a kind of legal patchwork that could undermine the lawful use of this technology"[26]. Against this background, EU Institutions recognized the need for a

[22] https://www.nobelprize.org/prizes/physics/2024/hinton/speech/ (last visited Sept. 25, 2025).
[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[24] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[25] On the role of Courts, DPAs and the relevant provisions of EU law governing FRTs prior to the AI Act, see, *ex multis*, V.L. Raposo, *(Do Not) Remember My Face: Uses of FRT in Light of the GDPR*, in 32 Inf & Comm Tech L, 45 ff. (1, 2022); M. Qandeel, *FRT: Regulations, Rights and the Rule of Law*, in Front. Big Data, 7:1354659, 2024; C. Pizzolo, *AI, Biometric Data, and the Effective Protection of Fundamental Rights in the Recent ECJ Case-Law*, in Unione europea e Diritti, 1 ff. (1, 2025); N. Menendez Gonzalez, G. Mobilio (eds), *Next Democratic Frontiers for FRT*, quot.; G. Formici, *Put the Genie Back in the Lamp? AI-Based Biometric Systems and Fundamental Rights Protection in the European Union Artificial Intelligence Act* (forthcoming). On the first ruling on FRTs and their legitimacy (*The Bridges* Case in UK), see A. Pin, *A Novel and Controversial Technology. Artificial Face Recognition, Privacy Protection and Algorithmic Bias in Europe*, in 30 William & Mary Bill of Rights J, 291 (2021); L. Woods, *Automated Facial Recognition in the UK: The Bridges Case and Beyond*, 3 EDPL Rev, 455 (2020); on the first case-law of the ECtHR on FRTs (*Glukhin v. Russia*, App. No. 11519/20, 4 July 2023), see M. Zalnieriute, *Glukhin v. Russia App. No. 11519/20 Judgement*, in 4 American Journal of International Law, 699 (2023).
[26] V.L. Raposo, *The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal*, in 29 Eur J Crim Policy Res, 515 (2023); for a critical analysis of the issues and limits linked to the application of GDPR and LED to FRTs, see, amongst the others, J. Purshouse, L. Campbell, *Automated Facial Recognition and Policing: A Bridge Too Far?*, in 42 Legal Studies, 209 ff. (2022); G. Mobilio, *Your Face Is Not New to Me – Regulating the Surveillance Power of FRTs*, in 1 Internet Pol Rev, 1 ff. (2023); E. Kavoliunaite-Ragauskiene, *Right to Privacy and Data Protection Concerns Raised by the Development and Usage of FRTs in the EU*, in 16 J of Human Rights Practice, 658 ff. (2024); M. Zalnieriute, *Beyond Procedural Fetishism: The Inadequacy of GDPR in Regulating Facial Recognition Technologies and Public Space Surveillance*, in M. Ebers, K. Sein (eds), *Privacy, Data Protection and Data-Driven Technologies*, Abingdon, 328 ff. (2025).

dedicated legal framework targeting the technology itself and comprehensively addressing the threats it posed to fundamental rights[27].

The 2024 AI Act therefore tackled this necessity by introducing an ambitious, first-ever, regulatory regime on AI. It established a unified supranational discipline governing the development, marketing, implementation and use of different AI systems, with the dual aim of fostering innovation and safeguarding the internal market, while ensuring strong protection of fundamental rights, democracy and the rule of law[28].

This innovative regulatory instrument that underlines the need for trustworthy human-centric AI, assigns particular attention to AI-driven biometric systems. By applying a risk-based approach[29], several of these technologies are identified as unacceptable AI practices: systems inferring emotions of natural persons in workplaces and education institutions[30], biometric categorization technologies[31], untargeted scraping of facial images[32] and real-time RBI systems in publicly available spaces for law enforcement purposes[33] are explicitly prohibited under Art. 5. Such systems are deemed to pose risks irreconcilable with EU values and principles[34].

Other biometric systems, such as those inferring emotions for medical or safety purposes, post-RBI systems and certain non-prohibited categorization systems, are classified as high-risk under Art. 6 (and Annex III)[35].

Focusing on FRTs, it is worth noting that although the AI Act does not explicitly refer to them, they fall within the broader category of "RBI systems". According to Art. 3 (n. 41), these are defined as "AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database". This formulation evidently covers FRTs as well as voice and gait identification systems[36].

---

[27] See the Resolution of the European Parliament 2020/2016/INI of 6 October 2021, invoking a moratorium on the use of RBI systems (Para. 27). Also the Commission, in the *White Paper on AI – A European Approach to Excellence and Trust*, COM(2020)65 of 19 February 2020, emphasized the importance of a renewed debate on fundamental rights protection imperilled by RBI systems. Several actions were also promoted by civil society organisations, as the "Reclaim Your Face" campaign, promoted by EDRi and supported by almost 200 other NGOs and experts calling on governments to stop facial recognition surveillance.

[28] On the AI Act, see, *ex multis*, G. Cassano, E.M. Tripodi (eds), *Il regolamento europeo sull'Intelligenza Artificiale. Commento al Reg. UE n. 1689/2024*, Rome (2024); C.N. Pehlivan, N. Forgo, P. Valcke (eds), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn (2024); A. Bensoussan, J. Bensoussan, V. Bensoussan-Brulé, *The European AI Act. Summary, Key Points and Article-by-Article Analysis*, Louvain-la-Neuve (2025); D.U. Galetta, L. Hueso Cotino (eds), *The European Union Artificial Intelligence Act*, Naples (2025); G. Malgieri, G. Gonzalez Fuster, A. Mantelero, G. Zanfir-Fortuna (eds), *The EU Artificial Intelligence Act. A Thematic Commentary*, London (2025); A. Mantelero, G. Resta, G. M. Riccio (eds), *Intelligenza Artificiale. Commentario*, Milan (2025); R. D'Orazio, V. Ricciuto (eds), *Il diritto europeo dell'Intelligenza artificiale*, Turin (forthcoming).

[29] P. Dunn, *The AI Act: A Tile in the EU's Digital Risk-Based Approach*, in O. Pollicino *et al* (eds), *La disciplina dell'Intelligenza artificiale*, Milan, 141 ff. (2025).

[30] Art. 5(1)(f). For a definition of these systems, see Art. 3(n. 39).

[31] Art. 5(1)(g). The definition of "biometric categorisation technologies" is provided in Art. 3(n. 40).

[32] Art. 5(1)(e). See also Recital 43.

[33] Art. 5(1)(h) and Art. 5 (2) to (8).

[34] The European Commissions dedicated to these prohibited systems specific Guidelines (*Guidelines on Prohibited AI Practices*, C(2025)884 final, 4 February 2025).

[35] See *infra* in this Paragraph.

[36] N. Menendez Gonzalez, G. Mobilio, *Between Prohibited Risks and High Risk: The Regulation of FRT*, in O. Pollicino *et al* (eds), *La disciplina dell'Intelligenza artificiale*, quot., 65.

In this general framework, the AI Act introduces a further distinction: besides differentiating identification and verification[37], it establishes a novel and highly relevant classification between real-time and post-RBI (Arts. 3 (n. 42) and (n. 43)). The former indicates systems where biometric capture, comparison and identification occur without significant delay, including instant identification and limited short delays[38]. By contrast, post-RBI applies where biometric data has already been captured and comparison and identification occur "after a significant delay", for example by analysis of CCTV footage or pictures or videos from private devices produced prior to use of the systems (Recital 17).

These distinctions, grounded in an assessment of the implications of RBI systems for fundamental rights[39], form the basis of graded risk assessment.

Given its potential for deep intrusiveness, technical inaccuracies, biased outcomes and discriminatory effects (Recital 32), the use of real-time RBI systems is prohibited in publicly accessible spaces[40] for law enforcement purposes[41]. While this first-ever evaluation is a courageous and rigid stand, Art. 5(1)(lett. h) also introduces a significant list of exceptions, only allowing implementation when strictly necessary and for expressly indicated purposes[42].

Paragraphs (2) to (7) of Art. 5, nonetheless, set out specific limitations and requirements governing the above-mentioned exceptional uses. First, deployment must be limited to confirming the identity of a specifically targeted individual, thereby excluding indiscriminate and bulk searches[43] (so-called "fishing expeditions"). Moreover, the nature

[37] The AI Act defines "verification" as "automated one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data" (Art. 3 (n. 36)). Identification, on the contrary is described as "automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person" through the comparison between that biometric data and those stored in a database (Art. 3 (n. 35)). This distinction has clear regulatory impacts: as stated in Annex III, Para. 1 (lett. a), high-risk RBI systems shall not include AI systems used for verification, which are therefore excluded from the set of rules established for high-risk technologies (see also Recital 17).

[38] Recital 17 talks about both live or near-live, "such as video footage, generated by a camera or other device with similar functionality".

[39] While verification systems, including authentication, "are likely to have a minor impact" compared to RBI (Recital 17), real-time systems appear to be "particularly intrusive" if compared to post RBI, to the extent that the first ones "may affect the private life or a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights", Recital 32.

[40] Art. 3 (n. 44). See also some examples at Para. 316 of the European Commission *Guidelines on Prohibited AI Practices*, quot.

[41] Useful definitions are provided in Art. 3 (n. 45) and (n. 46).

[42] Namely: i) targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons; ii) prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack; iii) localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years. The latter condition refers to 32 criminal offences listed in the Council Framework Decision 2002/584/JHA; their level of seriousness has been considered sufficient to justify the profound intrusion represented by real-time RBI systems (Recital 33).

[43] As reported by EDRi, "Emeritus Professor of International Law, Douwe Korff, supports this interpretation on the basis of case law of the Court of Justice of the EU, specifically the PNR (Passenger Name Records) case", https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/ (last visited Sept. 25, 2025).

of the situation – particularly the seriousness, probability and scale of harm that would result from non-deployment – and the impact on rights and freedoms should be considered (Art. 5(2)(lett. a)-b)). Except for cases of urgency, such systems shall undergo a prior fundamental rights impact assessment (Art. 27) and be registered in the EU database established by Art. 49.

National laws, specifying the necessary and proportionate safeguards, including temporal, geographic and personal limitations, as well as the competent authority and the rules governing the authorization procedure (Art. 5(5)), must also be in place. In fact, each exceptional use of real-time RBI systems shall be approved in advance by judicial or independent administrative authority that evaluates necessity and proportionality on the basis of objective evidence or clear indications, ensuring that deployment remains limited in duration and geographic and personal scope to what is strictly necessary (Art. 5(3))[44].

The AI Act thus leaves Member States a significant margin of discretion: they may decide to partially or fully authorize the use of real-time RBI systems for the exceptional cases identified, while remaining free to adopt stricter rules (Art. 5(5)).

By contrast, post-RBI and other potential uses of FRTs are classified as high-risk and are therefore subject to the complex rules of Chapter III, Section 2 and 3 of the AI Act[45]. These provisions cover a wide range of obligations, including risk management systems, record-keeping duties, transparency requirements, human oversight safeguards and specific responsibilities for different actors in the value chain – providers, importers, distributors and deployers. While a comprehensive analysis of these measures is beyond the scope of this contribution[46], Art. 26 – addressing the obligations of deployers of high-risk AI systems – is particularly significant in relation to post-RBI. Specifically, Art. 26(10) requires prior authorisation by a judicial or administrative authority when such systems are used "in the framework of an investigation for the targeted search of a person suspected

[44] To create additional guarantees, national provisions also need to include notification rules (Art. 5(4)); each use of real-time RBI for the abovementioned purposes and conditions should be notified to the market surveillance authority and the national DPA; these authorities are also required to submit to the Commission annual reports of the use of real-time RBI (Art. 5(6)). Based on the data acquired, the Commission shall, in turn, publish annual reports photographing the deployment of these technologies in the EU (Art. 5(7)). Similarly to what affirmed in the GDPR (Art. 22), the AI Act establishes that "no decision that produces an adverse legal effect on a person may be taken based solely on the output of the real-time RBI system" (Art. 5(3)).

[45] Specifically, we refer to post-RBI, non-prohibited biometric categorisation systems and AI biometric systems (and FRTs) aimed to infer emotions for medical or safety purposes (see V.L. Raposo, *Facial Recognition AI Technology in Healthcare and the Law*, in B. Solaiman, I.G. Cohen (eds), *Research Handbook on Health, AI and the Law*, Cheltenham, 41 ff. (2024)), systems covered by Annex III, points 2 to 8 (including a list of high-risk AI systems, according to their uses). Moreover, as noted by L. Escajedo San-Epifanio, *Biometric Recognition in the AI Act: Exemptions, Prohibitions and High-Risks Specialities*, in D.U. Galetta, L. Hueso Cotino (eds), *The European Union Artificial Intelligence Act*, quot., 187, "on the basis of Art. 111 AIA with the addition of Annex X, a specific statute is foreseen for a set of biometric recognition practices which are used in the field of large-scale IT systems established by EU legislation in law enforcement and border control matters. (..) A systematic interpretation of the AIA brings to light a set of biometric recognition systems which, because of the little or no attention they receive in the AIA, seem to be outside its scope or at least in doubt". For these systems, primarily used for border control, the deadline for ensuring compliance with the AI Act is extended until 31 December 2030. This provides a significant amount of time to implement the required safeguards, with potential implications for the fundamental rights of migrants. It is also worth highlighting that in the European Commission *Guidelines on prohibited artificial intelligence practices*, it has been clarified that "most AI systems that fall under an exception from a prohibition listed in Article 5 AI Act will qualify as high-risk" (para. 501).

[46] For an in-depth analysis, see the books indicated *supra* footnote n. 28; see also X. Tracol, *The Use of FRTs by Law Enforcement Authorities in the US and the EU: Towards a Convergence on Regulation?*, in 15 *Tech & Regulation*, 312 (2025).

or convicted of having committed a criminal offence". Emphasis on the *targeted* character of the search is further reinforced by the prohibition against using post-RBI "without any link to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person". As Recital 95 underlines, the intrusive nature of such technologies excludes their use for indiscriminate surveillance or as a means to circumvent the strict conditions that govern real-time RBI[47].

The intricate regulatory framework outlined above, distinguishing different categories of FRTs according to their purposes, field of application, technical features and presumed level of intrusiveness, mirrors the contentious political debate surrounding these technologies. FRTs were in fact among the most disputed AI systems during the legislative process of the AI Act[48], where provisions on biometric technologies underwent multiple revisions reflecting divergent positions among EU Institutions[49].

As a result of political compromise and the inherently controversial nature of FRTs, the final text of the AI Act leaves room for criticism.

Specifically, the broad use of exceptions – particularly regarding real-time RBI for law enforcement – risks neutralizing the effectiveness of existing prohibitions[50]. Interpreted expansively, vaguely worded exemptions can even lead to a "dangerous expansion of [RBI] deployment"[51]. As well, the role of national legislators in disciplining sensitive regulatory

[47] The analysed provision also repeats the necessity for: (i) a documented use of such technologies, with information made available to market surveillance authorities and DPAs upon requests; (ii) a specific obligation for deployers to submit annual reports to those authorities; (iii) a prohibition to negatively affect a person solely on the basis of the post-RBI systems' outputs; (iv) a possibility for Member States to introduce more restrictive laws on the use of such technology. The only exceptional case in which the prior authorisation is not required occurs when post-RBI systems are used "for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence" (Art. 26(10)).

[48] F. Palmiotto, *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*, in 16 Eur J of Risk Reg, 770 ff. (2025); G. Volpicelli, *Forget ChatGPT: Facial Recognition Emerges as AI Rulebook's Make-or-Break Issue*, in Politico, 14 June 2023, https://www.politico.eu/article/facial-recognition-artificial-intelligence-act-ai-issue-european-parliament/ (last visited Sept. 25, 2025).

[49] See the European Parliament Resolution of 6 October 2021, *supra* footnote n. 27 and R.J. Neuwirth, *Prohibited Artificial Intelligence Practices Revisited*, in V.L. Raposo (ed), *The European Artificial Intelligence Act. Promises and Perils?*, Cham, 131 ff. (2025).

[50] It is also worth underlining that, according to Recital 38, the "use (of real-time RBI systems) for purposes other than law enforcement should not be subject to the requirement of an authorisation". On this point see G.M. Diaz Gonzalez, *Prohibited Artificial Intelligence Practices*, in A.J. Huergo Lora (ed), *The EU Regulation on Artificial Intelligence. A Commentary*, Milan, 37 ff. (2025).

[51] A. Giannini, S. Tas, *Much Ado About Nothing? AI Act and the Prohibition of Real-Time Biometric Identification*, in Verfblog, 10 December 2024; similarly underlining critical aspects and issues in the current AI Act discipline, see N. Nikolinakos, *EU Policy and Legal Frameworks for Artificial Intelligence, Robotics and Related Technologies – The AI Act*, Cham, 388 (2023); R.J. Neuwrith, *Prohibited AI Practices in the Proposed EU AIA*, in 48 Comp L & Sec Rev, 1 ff. (2023); N. Lynch, *Facial Recognition Technology in Policing and Security – Case Studies in Regulation*, in 13 Laws 1 (2024); W. Gasparri, F. Tesi, *Artificial Intelligence and AI Act: From the Individual to the Algorithm?*, in 59 Zbornik Radova, 297 (2025); I. Barkane, L. Buka, *Prohibited AI Surveillance Practices in the AI Act: Promises and Pitfalls in Protecting Fundamental Rights*, in V. Galis, H.O.I. Gundhus, A. Vradis (eds), *Critical Perspectives on Predictive Policing*, Cheltenham, 127 ff. (2025); L. Escajedo San-Epifanio, *Biometric Recognition in the AI Act*, quot.; N. Menendez Gonzalez, G. Mobilio, *Between Prohibited Risks and High Risk*, quot.; M. Durovic, T. Corno, *The Privacy of Emotions: From the GDPR to the AI Act, an Overview of Emotional AI Regulation and the Protection of Privacy and Personal Data*, in M. Ebers, K. Sein (eds), *Privacy, Data Protection and Data-Driven Technologies*, quot., 368 ff.; F. Paolucci, *Enhancing Oversight and Addressing Gaps: Assessing the Impact of the AI Act on Biometric Identification Systems*, in N. Menendez Gonzalez, G. Mobilio (eds), *Next Democratic Frontiers for Facial Recognition Technology (FRT)*, quot., 71 ff. Vague definitions and potential implementation issues have been identified also with regards to the discipline and requirements established for high-risks AI systems (e.g. the

aspects such as authorization procedures and competent authorities further increases the risk of fragmentation among Member States[52].

In this context, the scope of application of the AI Act adds another layer of complexity. Art. 2(3) excludes areas outside EU law and preserves Member States competence in matters of national security, irrespective of the entities entrusted with related tasks. This provision revives a longstanding and contentious issue in CJEU case law[53]: the blurred boundary between law enforcement and national security. This distinction is often seen as unclear, raising risks of confusion over security purposes and responsible authorities[54].

Similar concerns arise from the Act's internal definitions and categorizations. The separation between verification and identification systems, as well as the different risk levels attributed to real-time and post-RBI, have been questioned by scholars who doubt the accuracy of such binary distinctions and the reliability of the resulting risk assessment[55].

In conclusion, the AI Act marks a bold and unprecedented attempt to establish a comprehensive, harmonized framework for FRTs, banning uses deemed unacceptable or excessively risky for fundamental rights due to their potential for creating a scenario of pervasive surveillance. Yet the above analysis reveals a mixed picture. The strong prohibition widely advocated by NGOs and civil society has not materialized: FRTs remain permissible in several contexts, subject to specific rules and safeguards. This is particularly evident in the security domain, where post-RBI systems are allowed and exemptions enable certain uses of real-time RBI.

The true impact of the Act will depend on its implementation – both by national legislators and within existing EU[56] and domestic regulatory frameworks[57] – as well as on how private

conditions imposed by Art. 26(10) seem quite vague and unclear—for example the distinction between targeted and untargeted investigations, or the definition of "objective and verifiable facts". As S. Wachter, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, in 26 *Yale J of Law & Tech* 672 ff. (3, 2024), affirmed, more generally, "strong lobbying efforts of big tech companies and member states were unfortunately able to water down much of the AIA. An overreliance on self-regulation, self-certification, weak oversight and investigatory mechanisms, and far-reaching exceptions for both the public and private sectors are the product of this lobbying", 672.

[52] As underlined by the recalled *Guidelines* provided by the European Commission, "only a domestic Member State law that fulfils, in particular, the requirements in Art. 5(2-7) AI Act, can allow the use of real-time RBI, as provided by Art. 5(2)" (para. 326). In the absence of such national provisions, the use of the systems under analysis must be therefore considered prohibited as of 2 February 2025, according to the timeline established by Article 113, AI Act.

[53] i.e. CJEU (Grand Chamber), C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others,* 6 October 2020; on this point, see M. Zalnieriute, *A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union*, in 1 The Modern L Rev, 198 ff. (2022).

[54] On this open and still highly discussed aspect, recently (re)emerged with regards to the data retention regime, see E. Celeste, G. Formici, *Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia*, 25 Germ L J, 427 ff. (2024).

[55] B. Sumer, *The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?*, in 2 EDPL Rev, 150 ff. (2024).

[56] In several cases, the AI Act expressly recall the other data protection legal frameworks, in particular the GDPR and LED. With regards to real-time RBI, it is stated that the AI Act provisions should apply as "lex specialis in respect to the rules on the processing of biometric data contained in Art. 10 of LED" (Recital 38). See G. Mobilio, *Your Face Is Not New to Me*, quot.; R. Soares Pereira, *Remarks on the Use of Biometric Data Systems (and FRTs) for Law Enforcement Purposes: Security Implications of the Proposal for an EU Regulation on AI*, in D. Vicente *et al* (eds), *The Legal Challenges of the Fourth Industrial Revolution*, Cham, 208 ff. (2023).

[57] i.e. the Italian Legislative Decree no. 139 of 8 October 2021, converted in Law no. 205 of 3 December 2021 introducing a moratorium on the installation of video surveillance systems incorporating FRTs in public spaces or areas open to public (the term of the moratorium has been extended until 31 December 2025, by Art. 8-ter, Law no. 87 of 3 July 2023). On the legislative national interventions on the topic, see also N. Menendez Gonzalez, G. Mobilio, *Between Prohibited Risks and High Risk: The Regulation of FRT*, quot.

operators fulfil the significant compliance obligations attached to high-risk systems. These factors will be decisive in shaping the effectiveness and practical consequences of the AI Act for the future development of FRTs.

## III. 'My Tearless Retina Takes Pictures that Can Prove' – Facial Recognition Technologies in the USA: A Fragmented Regulatory Landscape

While the EU struggled to establish a comprehensive framework for biometric data and AI-based biometric systems, leaving space for further development by Member States, the US approach to FRTs is complex, fragmented and multilayered. This Section briefly examines the major regulatory experiences across different levels of governance, highlighting the general landscape, ongoing normative discussions and emerging regulatory trends.

At federal level, no comprehensive federal regulatory framework currently governs biometric data[58] or directly addresses the deployment of FRTs, despite widespread use of biometric technologies by private and public entities[59].

Considering the congressional activity, the debate is still unsettled: various proposals have been introduced, yet none have resulted in enacted legislation. Notable examples include the 2020 *Ethical Use of Facial Recognition Act* that proposed "prohibit(ing) any officer, employee, or contractor of a federal agency from engaging in specified activities with respect to FRT without a warrant until a congressional commission established by this bill recommends rules governing the use and limitations on both government and commercial use of such technology"[60]. In 2022, the *Facial Recognition Act*, designed to restrict use of FRTs by law enforcement agencies, proposed the adoption of transparency measures, annual assessments and required to limit the use of this technology to situations when "a warrant is obtained that shows probable cause that an individual committed a serious violent felony"[61]. The *Facial Recognition and Biometric Technology Moratorium Act of 2023* went further, advocating to prohibit or limit the use of biometric surveillance systems, including

[58] General rules concerning the collection, storage and processing of personal information, also including face images, by federal agencies can be identified in the Privacy Act of 1974 (P.L. 93-579, 88 Stat 1896 (1974)) and in the E-Government Act of 2002 (P.L. 107-347, 116 Statt 2899 (2002)). Nonetheless, as underlined by the Congressional Research Service, *FRT and Law Enforcement: Select Constitutional Considerations*, 2020, "neither act directly addresses FRT or the reliability of algorithms employed to compare compiled photographs", 9. The document also lists applicable but very sectorial and limited federal laws disciplining the collection, use and storage of personal information by private entities (i.e. Driver's Privacy Protection Act or Family Educational Rights and Privacy Act), which may apply to the use of FRTs as well. Still, in C. N. Wright, *Facial Recognition Technology: Federal Agencies' Use and related Privacy Protections*, US Government Accountability Office, 2022, it is highlighted the absence of "federal laws that expressly regulate commercial uses of FRT in particular".

[59] On the vast use of FRTs in the US, see the data provided in US Commission on Civil Rights, *Annual Statutory Enforcement Report on the Civil Rights Implications of the Federal Use of FRTs*, 19 September 2024; M.A. Bigos, *Let's "Face" It: FRT, Police Surveillance, and the Constitution*, in 22 J. High Tech. L., 2021, 52 ff.; Congressional Research Service, *Federal Law Enforcement Use of FRT*, 27 October 2020.

[60] S.3284 - 116th Congress (2019-2020).

[61] H.R.9061 - 117th Congress (2021-2022). On the purposes of this proposal, see https://lieu.house.gov/media-center/press-releases/reps-ted-lieu-sheila-jackson-lee-yvette-clarke-and-jimmy-gomez-introduce (last visited Sept. 25, 2025). On FRTs and the concept of "probable cause", see T.J. Benedict, *The Computer Got It Wrong: FRT and Establishing Probable Cause to Arrest*, in 79 Wash. & Lee L. Rev., 849 ff. (2022).

FRTs, at federal, state and local government levels, while establishing the need for specific legislative intervention by Congress disciplining the use of such technologies[62].
Bill H.R. 3782 of June 2025 intends to prevent federal agencies from using FRT "as a means of identity verification"[63]; the prospects of this initiative remain uncertain, particularly given the persistent lack of bipartisan consensus on the matter, as was the case with previous proposals[64].
In the absence of federal legislation, two main areas of intervention have shaped the debate: initiatives of the executive branch and self-regulation or internal policies adopted by federal agencies.
With regard to executive action directly or indirectly affecting the implementation of FRTs, a relevant measure can be identified in the Executive Order (EO) 14074 of 25 May 2022, issued by President Biden and titled *Advancing Effective Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*. Among other provisions, Section 13(e) mandated the Department of Homeland Security (DHS), the Department of Justice (DOJ) and the White House Office of Science and Technology Policy (OSPT) to evaluate the impact of biometric technologies on privacy, civil liberties and rights, and to "lead an interagency process regarding the use by Law Enforcement Agencies of FRT and other technologies using biometric information". The resulting report, released in December 2024, set out best practices and guidelines for law enforcement agencies[65], while the DOJ tasked the National Academy of Sciences (NAS) with preparing a dedicated study on the implementation of AI-based biometric technologies[66]. While its outcomes in the field of FRTs were confined to reports and soft law guidance centred on accuracy, standards development and anti-discrimination measures, the EO nonetheless played an important role in highlighting the risks and challenges of FRTs and in encouraging debate on appropriate safeguards[67].
Subsequent initiatives, such as the *Blueprint for an AI Bill of rights*[68] and EO 14110 of 30 October 2023, titled *Safe, Secure and Trustworthy development and use of AI*, established

[62] S.681 - 118th Congress (2023-2024).
[63] H.R.3782 - *To prohibit the Federal Government from using facial recognition technology as a means of identity verification, and for other purposes* - 119th Congress (2025-2026). The proposal, only recently submitted, is still at the initial stage of the legislative process. Introduced by Republican Andrew Ogles, it has now been referred to the House Oversight and Government Reform Committee. The text defines FRTs as "contemporary security system that automatically identifies and verifies the identity of an individual from a digital image or video frame".
[64] US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot. includes references to various other proposed federal legislations, especially 89 ff.
[65] US DHS, DOJ, OSTP, *Biometric Technology Report*, December 2024.
[66] National Academies of Sciences, Engineering and Medicine, *FRT: Current Capabilities, Future Prospects, and Governance*, The National Academies Press (2024). This document interestingly provides several recommendations, also prompting the adoption of an EO "on the development of guidelines for the appropriate use of FRT by federal departments and agencies and addressing equity concerns and the protection of privacy and civil liberties" from both private and public actors. It additionally underlines that "in light of the fact that FRT has the potential for mass surveillance of the population, courts and legislatures will need to consider the implications for constitutional protections related to surveillance, such as due process and search and seizure thresholds and free speech and assembly rights", 129.
[67] On the EO, more generally, see C. Sbailò, *Governing Artificial Intelligence: Technological Leadership and Regulatory Challenges in an Era of Exponential Growth*, in *DPCE Online*, 67(SP 3), 275 ff. (2024).
[68] *Blueprint for an AI Bill of Rights. Making Automated Systems Work for the American People*, October 2022, https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/ (last visited Sept. 25, 2025). On this set of guidelines, elaborated by the White House Office of Science and Technology Policies, see E. Hine, L. Floridi, *The Blueprint for an AI Bill of Rights: In Search of Enaction, at Risk of Inaction*, in *Minds and Machines*, 1 ff. (2023).

additional general principles and best practices applicable to AI systems[69], and therefore also to FRTs. In particular, EO 14110 instructed "over 50 federal entities to engage in more than 100 specific actions to implement the guidance set forth across eight overarching policy areas", including measures to address algorithmic discrimination[70]. Importantly, these principles and requirements extended not only to public entities but also to private actors[71].

This ambitious framework was nonetheless superseded by President Trump's approach to AI governance[72]. Although the Trump Administration has so far paid limited attention to regulating FRTs, it has outlined a broader direction for the development and implementation of AI in the EO 14179 of 23 January 2025, *Removing Barriers to American Leadership in Artificial Intelligence*, issued with the declared aim of unleashing AI potential, particularly from an economic perspective. The EO emphasized AI as a national security imperative to achieve and maintain global tech dominance. Consistent with this vision, it adopted a deregulatory approach intended to stimulate industry growth, while criticizing the Biden-era EOs for imposing what has been described as an excessive burden on the private sector[73]. Aligned with this deregulatory orientation, the House of Representatives initially included a 10-year moratorium on state and local governments regulations of AI in the *One Big Beautiful Bill of* 2025[74]. Although this clause was ultimately removed for lack of majority support, thereby preserving the possibility for states to legislate in the field of AI governance, and by extension FRTs, its rationale was clearly to avoid regulatory fragmentation that could limit and harness private initiative in this key sector[75].

---

[69] On the President Biden approach to AI governance, see also N.A. Smuha, *Biden, Bletchley, and the Emerging International Law of AI*, in VerfBlog, 11 November 2023; M. Bassini, *The Global Race to Regulate AI: Biden's Executive Order Spillover Effects on the EU AI Act*, in IEP@BU, 1 December 2023, https://iep.unibocconi.eu/publications/global-race-regulate-ai-bidens-executive-order-spillover-effects-eu-ai-act (last visited Sept. 25, 2025); M. Worsdorfer, *Biden's Executive Order on AI and the EU's AI Act: A Comparative Computer-Ethical Analysis*, in 37 *Phil & Tech*, 74 (2024) (and https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4874592, last visited Sept. 25, 2025).

[70] On the requirements and timeline established by the EO 14110, see Congressional Research Service, *Highlights of the 2023 Executive Order on Artificial Intelligence for Congress*, updated 3 April 2024, https://www.congress.gov/crs_external_products/R/PDF/R47843/R47843.8.pdf (last visited Sept. 25, 2025).

[71] The Office of Management and Budget issued in March 2024 a *Memorandum for the Heads of Executive Departments and Agencies "Advancing Governance, Innovation, and Risk Management for Agency Use of AI"*: this document represents a guidance establishing specific requirements for AI governance, including practices such as AI impact assessment, test of AI performance in a real-world context, monitoring, adequate human training, public notice etc.

[72] In the *Initial Rescissions of Harmful Executive Orders and Actions*, 20 January 2025, https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/ (last visited Sept. 25, 2025), President Trump revoked EO 14110. Consequently, all Agencies are required to "suspend, revise or rescind" all the interventions and actions linked or implementing the Biden EO.

[73] In the EO it is stressed that "certain existing AI policies and directives acts as barriers to American AI innovation" (Sec. 1). More vastly, on the President Trump Administration approach to AI, see V. Lubello, *From Biden to Trump: Divergent and Convergent Policies in the Artificial Intelligence (AI) Summer*, in *DPCE Online*, 1, 2025, 49 ff.; C. Novelli, A. Gaur, L. Floridi, *Two Futures of AI Regulation under the Trump Administration*, 31 March 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5198926 (last visited Sept. 25, 2025).

[74] P. L. 119-21 (2025).

[75] That provision would have therefore led to federal dominance in the field of AI, possibly creating tensions between different levels of AI governance initiatives. On this aspect, see Congressional Research Service, *Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress*, 4 June 2025, https://www.congress.gov/crs_external_products/R/PDF/R48555/R48555.4.pdf (last visited Sept. 25, 2025); C. Novelli, A. Gaur, L. Floridi, *Two Futures of AI Regulation under the Trump Administration*, quot.,

In this broad scenario, where the prospect of federal rules governing FRTs remains uncertain[76], various federal agencies and executive bodies have gradually adopted self-regulatory measures, policies and best practices on AI, and more specifically on FRTs. Focusing on consumer protection, the Federal Trade Commission has issued guidelines addressing privacy risks linked to FRTs since 2012[77]. Since 2017, the National Institute of Technology and Standards (NIST)[78] has developed standards for the accuracy of FRTs and launched the *Face Recognition Vendor Testing Program*, which evaluates algorithmic performance in one-to-one and one-to-many systems[79]. More recently, various agencies have adopted interim policies[80], such as DHS Directive No. 026-11 (2023), *Use of FR and Face Capture Technologies*[81]. This directive requires independent testing of deployed systems, opt-out and alternative processing options and prohibits exclusive reliance on FRT outputs in law or civil enforcement actions, mandating manual review of results. While these non-legislative governance solutions introduce important principles and guarantees, they also contribute to an increasingly fragmented landscape.

Given this evolving federal framework, state and local governments are likewise adopting significant regulatory measures. While several states have enacted biometric data laws, notably the Illinois *Biometric Information Privacy Act* (BIPA) of 2008[82], some state and local

discussing the possible federal intervention in the field of AI governance through "pre-emption" of state law, based on the Supremacy Clause (Federal US Constitution, Art. VI, Clause 2). See also D.J. Mallinson *et al*, *Artificial Intelligence Policy, the Trump Administration, and Federalism*, in 47 Admin Theory & Praxis, 202 ff. (3, 2035). This issue and in particular the need to ensure a national policy framework for AI, avoiding fragmentation resulting from divergent state-level interventions, has been at the centre of the recent Executive Order 14365 of 11 December 2025, adopted by President Trump (see *infra* footnote n. 109 for more details).

[76] Other areas of intervention able to also impact on FRTs are the immigration agenda, currently characterized by an attempt to expand biometric data collection, and the large language models discipline; in this field, and more generally on provisions concerning accuracy of AI outputs, President Trump intervened with EO 14319 *Preventing Woke AI in the Federal Government* of 23 July 2025, affirming the need to "ensure that artificial intelligence (AI) models procured by the Federal government prioritize truthfulness and ideological neutrality" and consequently to protect "Americans from biased AI outputs driven by ideologies like diversity, equity, and inclusion (DEI) at the cost of accuracy" (see Fact Sheet https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-prevents-woke-ai-in-the-federal-government/, last visited Sept. 25, 2025).

[77] Federal Trade Commission, *Facing Facts: Best Practices for Common Uses of FRTs*, 22 October 2012. On the non-binding nature of such provisions as well as for an in-depth analysis of the Federal Trade Commission's actions, based on general consumer protection law principles and affecting private companies producing or applying FR software, see M. Filder, J. Hurwitz, *An Overview of FRT Regulation in the United States*, in R. Matulionyte, M. Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition in the Modern State*, quot, 219 ff.

[78] The NIST is a non-regulatory federal agency, part of the US Department of Commerce, with the mission of "promoting US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life".

[79] This test, periodically revised and updated, sets fundamental benchmarks for industries active in the field of FRTs.

[80] Other federal authorities and agencies adopting internal policies on the implementation and use of FRTs are listed in US DHS, DOJ, OSTP, *Biometric Technology Report*, quot. It is possible to mention DOJ's *Interim Policy and Safeguards for FRT Acquisition and Use*, elaborated in 2023 by the FRT Working Group; Federal Bureau of Investigation's (FBI) *FRT Use Policy Directive* of 2023. Both these policies prohibit the use of results coming from the implementation of FRTs "as the sole basis for enforcement action. Instead, FRT results generate investigative leads that require further investigation to substantiate or invalidate those leads", US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., 43.

[81] This Directive covers all use cases of FRTs, not only law enforcement purposes. For more information, see US DHS, DOJ, OSTP, *Biometric Technology Report*, quot., especially 23 ff.

[82] BIPA § 20, 740 Ill. Comp. Stat. 14/20 (2008). This important and innovative law (for its time and within the US context) established rules governing the collection, use, safeguarding, storage, handling, retention and destruction of biometric identifiers and information for commercial purposes. The Act has also

governments have gone further, adopting rules specifically addressing the deployment of FRTs. These regulatory responses may be classified in three categories[83]: outright bans, temporary moratoria and more nuanced normative frameworks. A recent trend marks a transition from comprehensive bans to more targeted legislation, authorizing use of FRTs for specific purposes, predominantly in the field of law enforcement, while simultaneously introducing safeguards and limitations[84].

Without attempting to cover the entire US landscape, it can be said that some regulatory initiatives stand out by virtue of their significance and rationale. In 2019, San Francisco became the first US city to ban use of FRTs by municipal authorities[85], including the Police Department. This strict measure—grounded in concerns over accuracy, discrimination and human rights—was soon replicated by other city councils, often drawing on the American Civil Liberties Union's (ACLU) model bill[86].

In recent years, however, several jurisdictions have reconsidered the scope and effectiveness of such bans and moratoria: Portland, for instance, adopted a resolution in 2023 that could limit its initial prohibition of 2020[87]. A similar trend is evident in New Orleans, where the 2020 ban was then replaced with a framework permitting use in specific cases (i.e. investigation of violent crimes), subject to prior permission by a superior[88]. States such as Virginia[89], Vermont and California have followed comparable paths: Vermont, the first state to ban FRT for law enforcement, has since introduced exceptions for certain

influenced the implementation of FRTs and served as foundation for significant legal actions, such as *American Civil Liberties Union et al. v. Clearview AI Inc.* before the Circuit Court of Cook County. Under the settlement concluding that case in 2022, the company was prohibited from selling its facial surveillance databases to private entities and was required to allow Illinois residents to request the blocking and deletion of their facial data from Clearview's system (for details and legal documents, see https://www.aclu.org/cases/aclu-v-clearview-ai, last visited Sept. 25, 2025). The BIPA and its underlying principles have also inspired the development of biometric data regulatory frameworks in several other states, such as California (Civil Code 1798.100-1798.199), Texas (Tex. Bus. & Com. Code 503-001), Washington (Wash. Rev. Code 19.375.010-19.375.900). In California, the California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100] also sets some specific obligations and requirements for processing of biometric data. H. Corbit, *Face Value: A Proposal for Federal Regulation of FRT Companies*, in 52 Stetson L. Rev., 779 ff. (2023); C. Sobczak, *BIPA and Article III Standing: Are Notice and Consent More than Bare Procedural Rights?*, in 35 Berkley Technical L. J., 1391 ff. (2020).

[83] C. Rabinowicz, *Approaches to Regulating Government Use of FRT*, in Harvard J of Law & Tech, 4 May 2023.

[84] *Ibid.*; see also X. Tracol, *The Use of FRTs by Law Enforcement Authorities in the US and the EU*, quot.; US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot.

[85] *Stop Secret Surveillance Ordinance*, 190110 – Leg Ver3 of 6 May 2019.

[86] According to the US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., "as of 2023, at least 22 local governments have adopted surveillance technology regulations using the ACLU model as template", 88. The model is based on the campaign *Community Control Over Police Surveillance* (CCOPS) that imposes City Council consent and active role in case police intends to buy new surveillance technologies.

[87] Ordinance adopted by the City Council of Portland (Oregon), on 9 September 2020, banning FRTs "for City Bureaus and in places of public accommodations when owned by private entities". The subsequent *Portland City Council Surveillance Technologies Resolution* has been considered as an "overall policy resolution, reconsidering the initial ban" (as affirmed by X. Tracol, *The Use of FRTs by Law Enforcement Authorities in the US and the EU*, quot., 297).

[88] Ordinance City of New Orleans, 21 July, 2022; see also US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., 32. On recent developments, aimed at expanding the use of real-time FRTs, see ACLU, *ACLU and ACLU of Louisiana Sound Alarm on New Orleans Police Department's Secret Use of Real-Time Facial Recognition*, 19 May 2025, https://www.aclu.org/press-releases/208236 (last visited Sept. 25, 2025).

[89] A. Powers, K. Simon, J. Spivack, *From Ban to Approval: What Virginia's FRT Law Gets Wrong*, in 26 Rich. Pub. Int. L. Rev., 155 ff. (1, 2022). While in 2021 the use of FRTs by local law enforcement and campus police was prevented, in 2022 a law was adopted to allow this technology in specific situations, imposing safeguards such as an accuracy score of at least 98% based on the NIST standards. The 2022 law has been criticised by the Authors as not able to adequately address the unique risks FRTs pose.

crime-prevention purposes under specific safeguards[90]; California enacted a three-year moratorium in 2019 on the use of FRT in body-worn camera footage, but since it expired on 1 January 2023, the implementation of a new regulatory framework is still to be discussed[91].

Several other states have recently introduced targeted regulations with specific safeguards to address the risks of FRTs. In Massachusetts, for example, a written request to the State Police or the FBI is mandatory to use FRTs in certain criminal cases[92], whereas a Colorado Bill imposes notification, accountability reporting, human oversight and a motivated justification for each deployment[93]. Additional safeguards include the requirement of a warrant or court order[94], limiting implementation of FRTs to certain crimes[95], establishing "probable cause to believe an unidentified person in an image committed a serious crime" and prohibiting reliance on FRT results as the sole basis for arrest or search[96].

Similar requirements and conditions have been established through self-regulating polices: in Detroit, wrongful arrests prompted the Police Department to revise FRT policies, explicitly prohibiting them as the sole justification for arrest[97].

Thus, regulatory efforts in the US have been made at multiple levels of governance, reflecting different approaches and ongoing debate[98]. In the resulting complex and fragmented landscape, moratoria and bans coexist with targeted regulations permitting use

[90] 2020 Vermont Acts and Resolves 799 Section 14.

[91] California Assembly Bill 1215, 8 October 2019. In recent times, AB 1814 failed to be approved.

[92] Massachusetts General Law – Part. I, Title II, Chapter 6, Section 220.

[93] Colorado Senate Bill 113 of 8 June 2022. See https://leg.colorado.gov/bills/sb22-113 (last visited Sept. 25, 2025).

[94] As required, for instance, by the Washington Senate Bill 6280 of 31 March 2020.

[95] See Utah Code of Criminal Procedure, Chapter 23e, *Government Use of FRT*, effective from 5 May 2021.

[96] Similarly to what established by the state of Maine, in Title 25 (*Internal Security and Public Safety*), § 6001, Part 14, Chapter 701 (*Facial Surveillance*).

[97] See Detroit Police Department Directive 307.5 on *Facial Recognition*. On the specific case, involving Robert Williams, see ACLU, *Civil Rights Advocates Achieve the Nation's Strongest Police Department Policy on FRT. Press Release*, 28 June 2024. In Miami, Police Department voluntarily adopted FRTs policies, also coordinating with civic organisations and privacy advocates, as reported by the US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., 89. Similar examples can be identified in X. Tracol, *The Use of FRTs by Law Enforcement Authorities in the US and the EU*, quot.

[98] For a broader picture of states and local governments measures on FRTs, see J. Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, in Tech.Policy Press, 6 January 2025, https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/ (last visited Sept. 25, 2025). Although this paper excludes such issues from its scope for reasons of space, it is worth noting that the absence of robust and comprehensive legislative safeguards at the federal level leaves room for debates on the compatibility of FRTs with several federal constitutional provisions. For instance, applying Fourth Amendment protections against unreasonable searches and seizures to FRTs raises complex questions about the continued relevance of the so-called Third Party Doctrine and the reasonable expectation of privacy in public spaces. Similar concerns arise under the Sixth Amendment Confrontation Clause, which guarantees defendants the right to confront and cross-examine witnesses in criminal proceedings, as well as under the Fourteenth Amendment requirement that prosecutors disclose all evidence. On this latter point, an illustrative case is *State v. Arteaga*, 476 N.J. Super. 36, para. 61 (App. Div. 2023), where the Superior Court of New Jersey held that the government has a duty to disclose details about the FRTs employed and their role in the identification of the suspect. On these highly articulated and delicate aspects, see US Commission on Civil Rights, *Annual Statutory Enforcement Report*, quot., 16 ff.; Congressional Research Service, *FRT and Law Enforcement*, quot.; M. Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of FRT*, in 49 Conn. L. Rev., 1591 ff. (2017); S. Nakar, D. Greenbaum, *Now You See Me, Now You Still Do: FRT and the Growing Lack of Privacy*, in 23 B.U. J. Sci. & Tech. L, 93 ff. (88, 2017); M. Simonitis, *FRT and the Constitution*, in 2 Notre Dame J on Emerging Tech, 357 (2, 2021); A.G. Ferguson, *Facial Recognition and the Fourth Amendment*, in 105 Minn. L. Rev., 1105 ff. (3, 2021); E. Ringel, A. Reid, *Regulating FRT: A Taxonomy of Regulatory Schemata and First Amendment Challenges*, in 28 Comm L & Pol, 3 ff. (1, 2023).

of FRTs under specific conditions, particularly in the public security domain. Voluntary schemes, policies, guidelines and self-regulatory initiatives further complicate the picture. While the fate of the federal legislative proposals remains uncertain, states and local government continue to implement rules aimed at setting limits and imposing safeguards on what is increasingly seen as an invasive technology. It remains to be seen if these measures and requirements could be considered as adequate and proportionate and, consequently, in what way FRTs will ultimately be deemed admissible[99], as well as how recent federal moves towards deregulation will influence the multi-level regulatory measures.

## IV. 'I Am Protected Electric Eye' - Different Regulatory Approaches, Similar Challenges: Constitutional Principles in the AI Surveillance Society

As emerged from the previous Sections, the regulation of FRTs in the EU and US is a complex challenge. Although Court action is still limited – in the EU, Data Protection Authorities' measures played a prominent role –, the legislative action recorded on both sides of the Atlantic is quite significant. Considering the peculiarities of the two legal systems[100], there are divergencies and convergencies in the regulatory efforts put in place.
In the EU, a comprehensive approach has been adopted, addressing AI systems as a whole with a focus on fundamental rights through strong and rigorous risk assessment evaluations. In the AI Act, specific provisions dedicated to biometric identification systems and specifically to RBI systems are included; also in terms of potential purposes, this Regulation covers different possibilities of FRT use in fields ranging from law enforcement to health and schools.
In the US, notwithstanding some policies and standards have been set by several federal agencies, states and local government have been more active in regulating FRTs, establishing rules on biometric data collection, retention and processing, as well as explicit implementation of FRTs by private and public entities.
Fragmentation of biometric data protection rules and provisions concerning FRTs *per se* is immediately evident in the US context, due to lack of federal and particularly Congressional intervention so far. In the EU, some level of fragmentation couldn't also

[99] On the need for an "adaptive legal framework" and on the delicate balance between investigative advancements and civil liberties, see P.N. Schuetz, *Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's FRT and the Need for an Adaptive Legal Framework*, in 39 Minn. J. L. & Ineq., 221 ff. (1, 2021); S. Chun, *FRT: A Call for the Creation of a Framework Combining Government Regulation and a Commitment to Corporate Responsibility*, in 21 N.C. J.L. & Tech., 99 ff. (4, 2020). On the need for a legislative intervention of the Congress, also transposing federal agencies policies in binding laws, see J. Zens, *Face It: Only Congress Can Preserve Privacy from the Pervasive Use of Facial Recognition Technology by Police*, in 58 San Diego L. Rev., 143 ff. (1, 2021).

[100] The lack of federal comprehensive laws on data protection – only partly compensated by state's data protection provisions – is one of the relevant aspects differentiating the US and EU regulatory approach towards data protection and new technologies; "the US approach marks (..) a significant departure from the 'regulatory anxiety' of EU lawmakers vis-à-vis disruptive technology and follows the general skepticism in the US legal culture about the role of regulation, most notably when it comes to emerging technologies and possible interferences with human rights", M. Bassini, *The Global Race to Regulate AI*, quot. See also A. Otene, *Two Becoming One: Revisiting the Two Western Cultures of Privacy in Light of Data Protection Laws*, 17 April 2024 (http://dx.doi.org/10.2139/ssrn.5017482, last visited Sept. 25, 2025), recalling the well-known paper by J.Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty,* in 113 *Yale Law J*, 1151 (2004) on the different conception of privacy and data protection on the two sides of the Atlantic. See also L. Barrett, *Ban FRT for Children-And for Everyone Else*, in 26 B. U. J. Sci. & Tech. L., 223 ff. (2, 2020). On the different approaches on AI governance, see R.B.L. Dixon, *A Principled Governance for Emerging AI Regimes: Lessons from China, the European Union, and the United States*, in AI Ethics, 793 ff. (3, 2023).

be excluded. National security exemption and room left to Member States to implement often vague and broad exceptions established by the AI Act could create an uneven landscape, especially when it comes to the use of such AI systems for security purposes. Although the AI Act establishes a stricter framework for FRTs, severely limiting real-time RBI systems for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, its effectiveness and harmonizing capacity remain uncertain. Procedural requirements, along with the designation of national authorities responsible for authorizing real-time RBI technologies for law enforcement uses, are left to national legislators. This could lead to diverging balances between the principles of necessity and proportionality protecting fundamental rights on one hand and security needs on the other. The final outcome will largely depend on how EU-level core principles are transposed into Member State laws concerning implementation of FRTs in the field of public security and on whether procedural safeguards can rationalize and "constitutionalize" the exceptional use of these technologies[101].

In the US, some states and local government, often supported by civil liberties organizations, have adopted moratoria or bans, taking a firm stance against potential or already visible impacts on fundamental rights. More recently, however, this trend has shifted toward nuanced regulatory approaches: specific requirements and limitations are gradually replacing outright prohibitions. At federal level, discussion on bans and moratoria continues, but in many cases these proposed measures serve mainly to halt implementation until Congress enacts binding legislation on allowed uses and safeguards. Despite differing approaches, we can therefore see that the two regulatory landscapes mostly allow use of these technologies under defined limits and conditions. This reflects the longstanding struggle to balance competing interests and rights, and more generally, the difficulty of fully renouncing the potential of new surveillance technologies[102].

The attempt to constitutionalize FRTs by applying constitutional values and principles[103] is still underway and debated, making the future in the EU and US difficult to predict. In the EU, much will depend on the concrete enactment of key rules and the interpretation of important principles and provisions by Member States. The coexistence of stratified regulatory frameworks will also need close monitoring, while the role of Data Protection Agencies and other AI supervisory authorities will be decisive[104]. In other words, the AI Act is a fundamental turning point but not the conclusion of the regulatory debate.

In the US, the next steps of legislative initiatives and the evolving interplay between different levels of governance must be carefully observed: the role of government agencies remains ambiguous, oscillating between policies/guidelines and the call for hard law provisions; also the trend at state and local government level seems to lead to unclear scenarios, while the lack of a uniform approach appears likely to persist, particularly considering the current polarized political debate in the US and the growing predilection for "law and order" policies and legal interventions[105].

---

[101] It is important to recall that, especially when it comes to high-risk systems, the effectiveness of AI Act safeguards and requirements will also highly depend on private actors and their compliance and concrete implementation of the AI Act obligations.

[102] C. Jasserand, *Facial Recognition in Public Spaces and the Principle of Necessity*, in N. Menendez Gonzalez, G. Mobilio (eds), *Next Democratic Frontiers for Facial Recognition Technology (FRT)*, quot., 49 ff.

[103] See, more broadly, E. Celeste, G. Formici, *Constitutionalizing Mass Surveillance in the EU*, quot.

[104] On the role of multiple national and supranational authorities empowered to enforce the AI Act, see H-W. Micklitz, G. Sartor, *Compliance and Enforcement in the AIA through AI*, in 43 Yearbook of EU Law, 2024, 297 ff.; C. Novelli *et al*, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in 16 Eur J of Risk Reg, 566 ff. (2, 2025).

[105] M. Filder, J. Hurwitz, *An Overview of FRT Regulation in the United States*, quot., 224.

This uncertain future is also increasingly influenced by overarching trends tied to the broader discourse on AI governance. Although the fragmented, cross-sector US approach to AI differs greatly from the holistic model promoted by the EU AI Act[106], a shared trajectory of deregulation has recently begun to emerge.

This shift is evident in President Trump's EO 14179 *Removing Barriers to American Leadership in Artificial Intelligence* of January 2025 and *America's AI Action Plan*[107], released in July 2025: both documents emphasize simplification and de-regulation as guiding principles, aiming to revoke "policies and directives that act as barriers to American AI innovation, clearing a path for the United States to act decisively to retain global leadership in AI"[108,109].

In parallel, the EU under the current Von der Leyen Commission also seems to be leaning in a de-regulatory direction[110]. Even if concrete measures remain undecided, the *Portfolio Communication on Implementation and Simplification* adopted by the European Commission as well as the Conclusions of the Council of the EU of 24 June 2025 on *Balancing Regulation and Innovation in the Technology -Driven Economy* reveal similar orientation[111]. Here,

[106] "Unlike the EU's AI Act, which provides a legally binding framework, the US adopts a decentralized, sector-specific regulatory strategy, primarily driven by voluntary commitments from private companies and guided by federal agencies. Additionally, state-level initiatives, often influenced by specific local concerns, contribute to a diverse regulatory environment", T. Davtyan, *The US Approach to AI Regulation: Federal Laws, Policies and Strategies Explained*, in 16 Case W. Res. J.L. Tech. & Internet, 223 (2, 2025).

[107] Available at https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (last visited Sept. 25, 2025).

[108] EO 14179. As affirmed in C. Novelli, A. Gaur, L. Floridi, *Two Futures of AI Regulation under the Trump Administration*, quot., "much of the reasoning favoring deregulation is centred on innovation and ease of business, and a rights-based approach is conspicuous in its absence", 10. Biden's approach, on the contrary, was considered as establishing "unnecessary government control" and "excessively burdensome requirements for companies", Fact Sheet, *President Donald J. Trump Takes Action to Enhance America's AI Leadership*, 23 January 2025, https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/ (last visited Sept. 25, 2025).

[109] Pending the peer-review process, it is worth noting that President Trump adopted EO 14365 "Ensuring a National Policy Framework for Artificial Intelligence" on 11 December 2025, which appears to be fully consistent with the simplification and de-regulation approach characterizing the earlier EOs issued during the Trump Presidency. In particular, EO 14365 recognizes that "US AI companies must be free to innovate without cumbersome regulation. But excessive State regulation thwarts this imperative"; consequently, it establishes that "it is the policy of the United States to sustain and enhance the United States' global AI dominance through a minimally burdensome national policy framework for AI" (Sec. 2). Based on this policy, the EO attributes the Attorney General the duty to establish an "AI Litigation Task Force", "whose sole responsibility shall be to challenge State AI laws inconsistent with the [abovementioned] policy (..), including on grounds that such laws unconstitutionally regulate interstate commerce, are preempted by existing Federal regulations". The Order also introduces a mechanism of evaluation of State AI laws (Sec. 4) as well as restrictions on funding for States with onerous AI laws (Sec. 5). Moreover, Sec. 8 is dedicated to legislation and, specifically, establishes that "The Special Advisor for AI and Crypto and the Assistant to the President for Science and Technology shall jointly prepare a legislative recommendation establishing a uniform Federal policy framework for AI that preempts State AI laws that conflict with the policy set forth in this order". Even if the effects of this recent EO have yet to be fully assessed, they may impact not only on the disciplines on FRTs at the State level, but also on the broader regulatory approach to AI governance in the US, potentially giving rise to tensions between the federal Government and States.

[110] H. Ruschemeier, *The De-Regulatory Turn of the EU Commission*, in VerfBlog, 18 February 2025; R. Csernatoni, *The EU's AI Power Play: Between Deregulation and Innovation*, Carnegie Europe, 2025; L. Lazaro Cabrera, *Europe's Deregulatory Turn Puts the AI Act at Risk*, in Tech Policy.Press, 3 June 2025, https://www.techpolicy.press/europes-deregulatory-turn-puts-the-ai-act-at-risk/ (last visited Sept. 25, 2025).

[111] Pending the peer-review process, the European Commission published, on 19 November 2025, the so-called "Omnibus Package", which includes the *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework,*

simplification increasingly risks overlapping with deregulation in the digital area, i.e. covering data protection and AI rules, making it a central element of the legislative, political – and economic – agenda, while at the same time sparking concern among digital-rights NGOs[112].

Considering these broader shifts, the future of FRTs is even more uncertain on both sides of the Atlantic and thus requires close monitoring. However, it is clear that FRTs have a canary-in-coal-mine role, exposing the risks and unprecedented challenges posed by AI.

The implementation of FRTs and their increasing use by private and governmental actors in public spaces expands surveillance, control and data-mining capacities, altering the relation between individuals and governing powers. The legislative and political debate should focus on how to promote solutions that impose rigid risk assessments and, when the risks are acceptable, establish procedural limits and safeguards, but also encourage a profound and vaster constitutionalisation process, ultimately able to ensure the guarantee of data protection and privacy as well as, more broadly, of fundamental rights, freedom and non-discrimination principle[113]. This process must be accompanied by public awareness, democratic debate and the accountability of private and public actors[114].

Ultimately, the regulation of FRTs is not just a technical and sectorial matter but a challenge intimately linked to the future of democracy and to the balance between power, surveillance and individual freedoms.

---

*and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024* (Digital Omnibus), COM/2025/837 and the *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence* (Digital Omnibus on AI), COM/2025/836. The declared aim of these proposals – consistent with the European Commission's previously illustrated shift towards regulatory simplification – is to introduce "technical amendments to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens alike, and to stimulate competitiveness" (https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal, last visited Jan. 10, 2026) and, with specific reference to the AI governance, to adopt "targeted simplification measures to ensure timely, smooth, and proportionate implementation of certain of the AI Act's provisions" (https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal, last visited Jan. 10, 2026). These proposals therefore intend to amend, *inter alia*, the GDPR and the AI Act, with potential implications also for the regulation of FRTs, especially as regards rules on the processing of biometric data and obligations applicable to high-risks AI-systems. Although the proposals are still at an early stage and have already triggered lively debate (R. Mahieu, *The Ominous Omnibus: Dismantling the Right of Access to Personal Data*, in VerfBlog, 3 December 2025; B. Lazarotto, *The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite*, in MediaLaws – Symposium, 19 December 2025; H. Hofmann, *This Is Not Simplification: How to Simplify the Digital Acquis Without Undermining Rights*, in VerfBlog, 3 January 2026), the legislative process warrants close scrutiny, as it may determine the future trajectory of data protection and AI governance in the EU.

[112] See the *Open Joint Letter against the Delaying and Reopening of the AI Act* of 9 July 2025, https://openfuture.eu/wp-content/uploads/2025/07/250709Open-Joint-Letter-against-the-Delaying-and-Reopening-of-the-AI-Act.pdf (last visited Sept. 25, 2025), signed by numerous NGOs.

[113] A regulatory approach mainly focused on procedural safeguards has also been criticized: M. Zalnieriute, *Beyond Procedural Fetishism,* quot. Bigos considers a nationwide ban of government use of FRTs as the only available option nowadays to effectively protect citizens from surveillance (M.A. Bigos, *Let's "Face" It*, quot.). Similarly, L. Barrett, *Ban FRT for Children-And for Everyone Else*, quot.

[114] K. Lachmayer, *AI, Plurality and Democracy. Reflections on the Impact of Large Language Models like ChatGPT on the Rule of Law and Democracy*, in P. Riberi, K. Lachmayer (eds), *Political Representation, Democracy and the Constitution* (forthcoming).

# AFFECTIVE COMPUTING-BASED ATTENTION MONITORING IN AI EDUCATION: A COMPARATIVE ANALYSIS OF CHILDREN'S BIOMETRIC DATA PROTECTION IN CHINA AND THE EU

*Xiaotong Bing – Anne Oloo*[*]

TABLE OF CONTENTS



*The classroom has become a hub of AI technologies, with affective computing and attention monitoring systems processing sensitive biometric data. This paper examines how the European Union (EU) and China are grappling with the data protection challenges posed by these emerging technologies, particularly when it comes to safeguarding children's rights. We argue that while the legal frameworks in both the EU and China are shaped by different regulatory logics reflecting distinct social, political, and economic contexts, both jurisdictions share some similarities in their approaches. In both jurisdictions, children are singled out as requiring heightened protection, yet both regulatory frameworks struggle to define the bounds of such protection. Our research shows that the use of affective computing and attention-monitoring systems in educational settings reveals fault lines in the current data protection framework, underscoring the need for tailored, child-centric regulations that balance technological innovation and fundamental rights protection.*

**Keywords**: Affective computing, biometric data, AI education, GDPR, AI Act, Civil Code, PIPL, fundamental rights, Brussels Effect, comparative law, China, EU.

## I. INTRODUCTION

The rapid development of affective computing technology, a branch of AI that detects and responds to human emotions and cognitive states, is beginning to reshape educational environments by enabling more emotionally responsive and personalised learning.[1] Affective computing aims to enable machines to recognise and respond to human emotions through techniques such as facial analysis, speech processing, and physiological monitoring.[2] Attention-monitoring is often considered a subset of affective computing,

---

[*] The authors' contributions are described based on the Contributor Roles Taxonomy (CRediT). Both authors were involved in the conceptualisation of the paper. The authors jointly defined the main structure and argument and jointly drafted the introduction and concluding sections. Anne Oloo drafted the sections on the EU Legal Framework and Comparative Insights. The sections on Description of Affective Computing and Attention Monitoring and the Chinese Legal Framework were drafted by Xiaotong Bing. Both authors take responsibility for the final text. We are grateful for the comments received at the European Law and Digital Technologies workshop at the University of Udine, Italy, on the 5th of September 2025. Thank you also to Prof Wouter Vandenhole and the anonymous reviewers for their comments and feedback. Xiaotong Bing is funded by the scholarship programme of the China Scholarship Council [Grant No.202409370002]

[1] A. O. R. Vistorte et al., *Integrating Artificial Intelligence to Assess Emotions in Learning Environments: A Systematic Literature Review*, 15 Frontiers in Psychology 1387089, 9 (2024).

[2] Y. Wang et al., *A Systematic Review on Affective Computing: Emotion Models, Databases, and Recent Advances*, 83–84 Information Fusion 19, 19 (2022).

focusing specifically on tracking students' focus and engagement in real time.[3] This aligns with the connection between one's affective state and ability to focus.[4]

However, their integration has raised urgent questions concerning privacy, ethics, and the governance of sensitive biometric data, especially when applied to minors.[5] In China, the deployment of such technologies in classrooms has often outpaced the development of corresponding legal safeguards, leading to significant regulatory gaps in the protection of minors' biometric data. This approach reflects China's emphasis on a policy-driven and technology-enabled approach to digitizing education, but it has sparked concerns about individual privacy and data protection. In contrast, the European Union (EU) has adopted a more cautious regulatory stance, enacting data protection frameworks that impose limitations on biometric data processing in educational settings, such as the General Data Protection Regulation (GDPR)[6] and the Artificial Intelligence Act (AI Act) [7].

This paper examines the emergence of affective computing and attention monitoring technologies in China's basic education system, focusing on the regulatory implications for children's biometric data protection in China and the EU. Whilst these technologies are far more widely deployed in classrooms in China than in Europe, where uptake is still limited but policy relevant, China's large-scale implementations offer a valuable use case for legal analysis. In anticipating cross-border market and vendor behaviour and considering the EU's role as a normative trendsetter in AI regulation, an EU-China comparison becomes pertinent for assessing the potency of EU rules. The analysis is principally legal; however, the authors acknowledge that affective computing and attention monitoring technologies also give rise to wider social, epistemological and ethical questions[8], such as children's autonomy[9], bias characterised in these systems[10], the validity of inferred mental states[11], as well as shifts in pedagogical authority[12], issues that cannot be fully addressed within the scope of this paper. Accordingly, the paper limits itself to a

[3] Vistorte et al., *supra* note 1 at 10.

[4] Y. Liu, Q. Fu & X. Fu, *The Interaction between Cognition and Emotion*, 54 Chinese Science Bulletin 4102, 4103 (2009); Nesreen Mejbri et al., *Trends in the Use of Affective Computing in E-Learning Environments*, 27 Education and Information Technologies 3867, 3868 (2022).

[5] R. Yuvaraj et al., *Affective Computing for Learning in Education: A Systematic Review and Bibliometric Analysis*, 15 Education Sciences 65 (2025); C. S. Montero & J. Suhonen, *Emotion Analysis Meets Learning Analytics: Online Learner Profiling beyond Numerical Data*, *in* Proceedings of the 14th Koli Calling International Conference on Computing Education Research 165 (2014), https://dl.acm.org/doi/10.1145/2674683.2674699; P. Ceres, *Kids Are Back in Classrooms and Laptops Are Still Spying on Them*, Wired, https://www.wired.com/story/student-monitoring-software-privacy-in-schools/ (last visited Oct. 14, 2025).

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) of 2016, OJ L 119.

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (AI Act) of 2024, OJ L 2024/1689, 12.7.2024.

[8] Montero and Suhonen, *supra* note 5 at 168–169.

[9] Yuvaraj et al., *supra* note 5 at 35.

[10] A. Katirai, *Ethical Considerations in Emotion Recognition Technologies: A Review of the Literature*, 4 AI and Ethics 927, 931 (2024).

[11] G. Mobilio, *When the Kids Aren't Alright: The Use of Facial Recognition Technologies at School*, *in* Digital Governance: Confronting the Challenges Posed by Artificial Intelligence 41 (K. Prifti et al. eds., 2024), https://doi.org/10.1007/978-94-6265-639-0_3.

[12] C. Vidal, *The Convergence of Neurotechnology and Digital Technology in Education: Ethical and Societal Issues*, Inserm, 21 (2024).

legal and regulatory examination while seeking to contribute to and stimulate the broader interdisciplinary discourse on the interplay between technological innovation, regulatory frameworks, and human rights.

## I. FROM POLICY TO PRACTICE: ATTENTION- MONITORING IN CHINA'S SMART CLASS

### I.1. *Affective Computing, Attention Monitoring, and Biometric Data*

Understanding the regulatory implications of attention-monitoring technologies requires clarity about their conceptual and technical underpinnings. AI is a highly interdisciplinary field that integrates computer science, cognitive science, linguistics, psychology, and more. As defined by Russell and Norvig in their authoritative textbook *Artificial Intelligence: A Modern Approach*, AI is "the study of agents that receive precepts from the environment and perform actions," aiming to reproduce intelligent behaviour with a rational basis.[13] Within this broad framework, affective computing has emerged as a distinctive subdomain. Affective computing refers to technologies that enable computers to recognise, interpret, and respond to human emotions.[14] It focuses on systems that can detect emotional states through expressions and behavioural cues, allowing machines to simulate or adapt to emotional intelligence in human–computer interaction.[15]

Affective processes involve the psychological and physiological mechanisms through which an organism evaluates stimuli and generates adaptive responses.[16] Emotion represents a fundamental affective process, manifesting as a short-lived, multi-dimensional reaction to internal or external events relevant to an individual's important concerns.[17] It is dynamic, involving coordinated changes in the body, behaviour, subjective experience, and action tendencies, enabling effective adaptation to environmental challenges.[18] Unlike a simple feeling, which reflects only the conscious experience, emotion encompasses the entire multi-modal, evolving process, combining internal states and outward expressions into a coherent episode.[19]

Attention, in turn, a core cognitive function, regulates the processing of sensory information and plays a central role in controlled processes, ensuring that the pursuit of a goal is protected from interference.[20] Cognitive functions, in general, such as memory, language, problem-solving, and planning, are traditionally contrasted with affective functions, highlighting their reliance on rational, controlled processing rather than emotional evaluation.[21] However, attention is closely linked to affective processes[22]: its dynamics reflect an organism's evaluation of environmental events, prioritisation of salient stimuli, and associated physiological and behavioural responses, as well as subjective

---

[13] S. J. Russell & P. Norvig, *Artificial Intelligence: A Modern Approach*, 1 (Third edition, Global edition ed. 2016).
[14] K. R. Scherer, T. Bänziger, and E. Roesch, *A Blueprint for Affective Computing: A Sourcebook and Manual*, 1 (2010).
[15] H.-C. K. Lin, C.-H. Wu, and Y.-P. Hsueh, *The Influence of Using Affective Tutoring System in Accounting Remedial Instruction on Learning Performance and Usability*, 41 Computers in Human Behavior 514, 515 (2014).
[16] L. Pessoa, *On the Relationship between Emotion and Cognition*, 9 Nature Reviews Neuroscience 148, 148 (2008).
[17] K. R. Scherer, *What Are Emotions? And How Can They Be Measured?*, 44 Social Science Information 695, 697 (2005).
[18] *Id.* at 698.
[19] *Id.* at 699.
[20] Pessoa, *supra* note 16 at 149.
[21] *Id.* at 148.
[22] *Id.* at 158.

experiences such as focus, alertness, and engagement.[23] From this perspective, while attention remains fundamentally a cognitive function, its observable manifestations overlap with emotion, making computational detection of attention a concrete application of affective computing in educational contexts.

Attention monitoring refers to the use of technological means to detect and assess learners' focus levels in real time during classroom or learning activities.[24] Collecting and analysing learners' physiological or behavioural data helps educators understand the distribution and fluctuations of students' attention, enabling timely adjustments to teaching content and methods to enhance instructional effectiveness.[25] The computational feasibility of attention monitoring, like emotion recognition, rests on the collection and analysis of biometric data.[26] Biometric data forms a key technical foundation of affective computing and attention monitoring. Both rely on the analysis of multimodal biometric signals[27] including facial expressions, eye movements, posture, and, in some cases, brainwave activity, to infer internal mental states that are not directly observable.

These data serve as proxies for internal mental states that are not directly observable. They can be broadly categorised into behavioural and physiological signals.[28] Behavioural signals encompass observable characteristics such as facial expressions, speech, body posture, and eye movements that can be captured through cameras or microphones without physical contact.[29] Their non-intrusive nature and relatively low cost make them the dominant mode of data collection in classroom-based emotion recognition.[30] Physiological signals, by contrast, require dedicated sensors to monitor indicators such as electroencephalography (EEG), galvanic skin response, and heart rate variability.[31] These signals tend to reflect more accurately since individuals have limited conscious control over physiological changes.[32] However, the collection of physiological signals is complex, costly, and often requires direct contact with the subject, which may interfere with the learning process.[33] Moreover, emotional and attentional states are inferred probabilistically from these proxy signals, whose quality can vary due to differences in EEG devices, sampling rates, and channel configurations, and are further affected by individual and

[23] A. Ohman, A. Flykt, and F. Esteves, *Emotion Drives Attention: Detecting the Snake in the Grass*, Journal of Experimental Psychology: General, 466 (2001)

[24] Z. Trabelsi et al., *Real-Time Attention Monitoring System for Classroom: A Deep Learning Approach for Student's Behavior Recognition*, 7 Big Data and Cognitive Computing 48, 2 (2023).

[25] D. Durães et al., *Monitoring Level Attention Approach in Learning Activities*, 478 *in* Methodologies and Intelligent Systems for Technology Enhanced Learning, 6th International Conference 33 (M. Caporuscio et al. eds., 2016), http://link.springer.com/10.1007/978-3-319-40165-2_4.

[26] Y. Wang et al., *A Systematic Review on Affective Computing: Emotion Models, Databases, and Recent Advances*, 83–84 Information Fusion 19, 19 (2022).

[27] Multimodal biometric signals refer to the combined use of two or more types of biometric data such as facial expressions, voice, eye movements, or physiological signals like EEG and heart rate to infer an individual's emotional, cognitive, or identity-related states. Compared to unimodal systems, multimodal approaches are more robust, accurate, and resistant to spoofing, as they integrate information from multiple sources to reduce uncertainty and improve system performance. *See* P. S. Sanjekar and J. B. Patil, *An Overview of Multimodal Biometrics*, 4 Signal & Image Processing: An International Journal 57, 58 (2013).

[28] Wang et al., *supra* note 26 at 19.

[29] R. A. Calvo & S. D'Mello, *Affect Detection: An Interdisciplinary Review of Models, Methods, and Their Applications*, 1 IEEE Transactions On Affective Computing 18, 23–25 (2010).

[30] Y. Xu *et al.*, *Learning Affective Computing Research: A Systematic Literature Review Based on International Studies*, Featured Article Digital Education 1, 4.

[31] Wang et al., *supra* note 26 at 20.

[32] H. Liu et al., *Review on Emotion Recognition Based on Electroencephalography*, 15 Front. Comput. Neurosci. (2021), https://www.frontiersin.org/journals/computational-neuroscience/articles/10.3389/fncom.2021.758212/full.

[33] Xu et al., *supra* note 30.

contextual variability.[34] Consequently, even technically feasible systems may produce misclassifications or erroneous assessments in real-world classroom environments, which can have ethical and legal implications when used to guide instructional decisions.[35]

China's deployment of an EEG-based attention-monitoring device illustrates these contrasts. In one notable case, several elementary schools adopted the *Focus headband*,[36] a device that measured students' brainwave activity and displayed colour-coded indicators of attentiveness: red for focused, blue for distracted. It also sent real-time attention scores to teachers and parents.[37] The project was soon suspended following public backlash over potential harm to children's well-being: concerns included the potential inaccuracy of the attention measurements, intrusive student surveillance, potential manipulation of emotional states, and risks to children's privacy and data protection regarding the processing of their biometric data.[38]

To ground the subsequent legal and comparative analysis, the following section turns to the Chinese context, where affective computing and attention monitoring systems have been deployed most visibly in educational settings. It traces their policy foundations, practical implications, and public controversies to illustrate how China's broader AI strategy translates into the classroom.

### I.2. *Affective Computing and Attention Monitoring in Chinese Classrooms*

AI is increasingly shaping the education sector worldwide. According to the 2025 *AI Index Report*, two-thirds of countries now offer or plan to offer K–12 computer science education, twice as many as in 2019.[39] China has prioritised AI education on the national agenda. The latest *Blue Book on AI-Powered Applications in Basic Education*[40] reports that by early 2025, AI technologies had entered the initial stages of integration into China's basic education system through a pilot project spanning teaching, learning, assessment, student development, educational research, and governance. These initiatives aim to build a data-driven smart education ecosystem, featuring tools such as intelligent lesson preparation, personalised learning assistance, multimodal performance evaluation, and automated education management.

Behind these applications lies the growing use of affective computing to assess students' emotional and cognitive engagement. The so-called 'Attention Index' has emerged as a key indicator of instructional quality.[41] Yet because these systems rely on processing highly

---

[34] N. Babu et al., *Emotion Recognition in Virtual and Non-Virtual Environments Using EEG Signals: Dataset and Evaluation*, 106 Biomedical Signal Processing and Control 107674, 2 (2025).

[35] A. McStay, *Emotional AI and EdTech: Serving the Public Good?*, 45 Learn Media Technol. 270 (2020).

[36] The Focus headband is a product of BrainCo, a company founded in 2015 and incubated at the Harvard Innovation Lab. A FOCUS Headband consists of three parts: hardware, algorithm, and software. By using its proprietary sensors to detect brain signals and deploying an AI algorithm to translate signals into focus levels in real time, the Headband provides insights into the engagement levels of users and tracks whether a user is focused or distracted. *See* BrainCo company website: https://brainco.tech/technology/

[37] *AI Headbands Tracking Student Attention Levels Suspended amidst Online Controversy* - People's Daily Online, https://en.people.cn/n3/2019/1101/c90000-9628768.html (last visited Jan. 28, 2026).

[38] *Headbands Monitoring Elementary Students' Focus Likened to 'Tightening Curse': What Fuels the Backlash against Smart Education Devices?*, Xinhua Net, http://www.xinhuanet.com/politics/2019-11/10/c_1125214619.htm (last visited July 19, 2025).

[39] N. Maslej *et al.*, *Artificial Intelligence Index Report 2025*, Artificial Intelligence, 367 (2025).

[40] Engineering Research Center for Smart Technology and Education, Ministry of Education; Beijing Digital Education Center (Beijing Educational Technology Center), Blue Book on AI-Enabled Applications in Basic Education (2025) (2025).

[41] A. Al-Nafjan & M. Aldayel, *Predict Students' Attention in Online Learning Using EEG Data*, 14 Sustainability 6553, 1 (2022); *See also* A. Becerra, R. Cobos & C. Lang, *Enhancing Online Learning by Integrating Biosensors and*

sensitive biometric and emotional data, their use has sparked public controversy. The diffusion of these attention monitoring systems has followed a phased diffusion trajectory, moving from initial pilot projects through intense public debate to a relatively stable, though still contested, stage.

A landmark pilot was the 'Intelligent Classroom Behaviour Management System' installed in 2018 at Hangzhou No. 11 High School.[42] Using facial-recognition technology, the system classified and recorded students' classroom behaviours (e.g., hand-raising, reading, distraction) as well as their emotional states (e.g., happiness, anger, fear) in real time.[43] Developed jointly with Hikvision[44], the project drew extensive domestic and international media attention for its intrusive monitoring capabilities and sparked vigorous debate over student privacy, informed consent, and the ethics of emotion surveillance.[45]

Despite continuing concerns, similar technologies have proliferated across 'smart classroom' initiatives. Corporate materials from Zhizhou AI[46] describe systems that generate individualised student profiles integrating behavioural, emotional, and cognitive data, using indicators such as an Attention Index to monitor engagement and support pedagogical adjustment. In these systems, computer vision technologies analyse students' facial expressions, body postures, and gaze direction to infer levels of attention and participation. Real-time dashboards present visualised data such as emotional distribution charts (e.g., neutral, active, serious), heatmaps of classroom engagement, and time-series graphs showing fluctuations in collective attention throughout a lesson.[47] These analytics are further used to generate diagnostic reports for teachers, detailing behavioural frequencies and engagement patterns, thereby providing data-driven insights for instructional design and learning adjustment.[48]

China's national AI strategy strongly emphasises integrating intelligent technologies into basic education as part of a broader shift towards evidence-based teaching. Affective computing, particularly attention monitoring systems, now sits at the core of this shift. However, their continuous collection of sensitive data, particularly biometric data, has triggered significant ethical and legal concerns.

This controversy highlights a broader regulatory dilemma: how to safeguard children's data protection and privacy rights in the digital classroom when affective and attention

*Multimodal Learning Analytics for Detecting and Predicting Student Behaviour: A Review*, Behaviour & Information Technology 1 (2025).

[42] *Chinese School Uses Facial Recognition to Make Kids Pay Attention*, Engadget (May 17, 2018), https://www.engadget.com/2018-05-17-chinese-school-facial-recognition-kids-attention.html. (last visited 11 Oct. 2025).

[43] ARTICLE 19, Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights 29 (2021).

[44] Hikvision is a leading provider of AI-driven video surveillance technologies, headquartered in Hangzhou, China. Hikvision, *Smart Classroom Solution*, http://www.hikvision.com/en/solutions/solutions-by-industry/education/smart-classroom/ (last visited June 23, 2025).

[45] GETChina Insights, *Schools Using Facial Recognition System Sparks Privacy Concerns in China*, Medium (Sept. 9, 2019), https://edtechchina.medium.com/schools-using-facial-recognition-system-sparks-privacy-concerns-in-china-d4f706e5cfd0 (last visited June 23, 2025); M. Standaert, *Chinese Primary School Halts Trial of Device That Monitors Pupils' Brainwaves*, The Guardian, Nov. 1, 2019, https://www.theguardian.com/world/2019/nov/01/chinese-primary-school-halts-trial-of-device-that-monitors-pupils-brainwaves (last visited Oct. 13, 2025).

[46] Zhizhou AI is a product developed by Beijing Zhizhou Technology Co., Ltd., a Chinese educational technology company focused on smart classroom solutions. https://mp.weixin.qq.com/s/03lXymFqUSaXYE3sfEC2AQ (last visited 16 July 2025.)

[47] Zhizhou AI, *AI Smart Teaching System: Six Core Technologies for In-Depth Learning Analytics.* (June 3, 2024), https://mp.weixin.qq.com/s/03lXymFqUSaXYE3sfEC2AQ (last visited July 16, 2025).

[48] *Id.*

monitoring systems are deployed in learning environments, a question to which the following sections will turn.

## II. LEGAL FOUNDATIONS AND REGULATORY FRAMEWORKS

The preceding discussion has shown that affective computing and attention-monitoring technologies introduce unprecedented forms of observation and inference in the classroom. Their capacity to capture or predict children's emotional and cognitive states exposes deep tensions between educational innovation and the protection of privacy and children's data. These tensions underscore the urgent need for a coherent legal framework capable of addressing the direct risks of biometric processing and the subtler harms arising from constant behavioural surveillance.

Children are particularly vulnerable in this context, as they are often less aware of the risks, consequences, and their rights regarding data processing.[49] Any breach of their data, therefore, poses a greater risk to their fundamental right to data protection.[50]

The legal framework governing children's data protection in Europe and China has its antecedents in the international human rights law, specifically in the United Nations Convention on the Rights of the Child[51] (CRC), which lays down nearly universally recognised rights for Children. Whereas data protection is not explicitly mentioned as one of those rights[52], various UN reports[53] and the 2021 General Comment No. 25 (GC 25)[54] have affirmed that children have a fundamental right to data protection.

The UNCRC lays down four essential principles that underpin children's data protection[55]:

1. Non-discrimination: Guaranteeing the same rights to all children without discrimination (Article 2).
2. Best interests of the child: Ensuring that the interests of children are given paramount consideration above those of others (state, parents, and community) (Article 3).
3. The right to survival and development: Recognising children's right to the full extent of their development (Article 6).
4. Participation and inclusion: Ensuring that children's views are taken into account throughout their different stages of development (Article 12).

These principles are reflected, to varying extents, in the legal frameworks of the EU and China. The next section will examine the law governing children's data protection in the

---

[49] GDPR r 38.

[50] K. Faisal, *Certain Legal Aspects of Children's Right to Protect Personal Data in the Context of AI under the European Union Data Protection Laws*, Vapaita Sanoja. Viestintäoikeuden Vuosikirja 106, 109 (2022).

[51] Convention on the Rights of Child (adopted 20 november 1989, entered into force 2 september 1990), UNTS 1577.

[52] V. Verdoodt, Y. Zhang & E. Lievens, *Safeguarding the Child's Right to Privacy and Data Protection in the European Union and China: A Tale of State Duties and Business Responsibilities*, 28 International Journal of Human Rights 125, 5 (2024).

[53] United Nations General Assembly, The Right to Privacy in the Digital Age: Resolution Adopted by the General Assembly on 17 December 2018 [on the Report of the Third Committee (A/73/589/Add. 2)] 73/179. The Right to Privacy in the Digital Age (2019), http://digitallibrary.un.org/record/1661346; Human Rights Council, Artificial Intelligence and Privacy, and Children's Privacy: Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci (2021), https://documents.un.org/doc/undoc/gen/g21/015/65/pdf/g2101565.pdf.

[54] UN Committee on the Rights of the Child, 'General Comment No. 25 on Children's Rights in Relation to the Digital Environment' (2021) UN Doc CRC/C/GC/25.

[55] C. Caglar, *Children's Right To Privacy And Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?*, 12 European Journal of Law and Technology 11 (2021), https://ejlt.org/index.php/ejlt/article/view/828.

context of attention monitoring and affective computing systems in the European Union. The focus will be on the key provisions within the GDPR and the recently enacted AI Act that address the protection of children's personal data in these emerging technological applications. The aim is to explore how these EU regulations seek to uphold the core principles of children's rights within the specific context of AI-driven educational technologies that monitor students' emotional and cognitive states.

### III.1 *The EU's Legal Framework for Children's Data Protection*

The EU's legal framework for protecting children's data rights in the context of affective computing and attention monitoring systems is firmly rooted in its fundamental legal instruments. Article 8 of the Charter of Fundamental Rights of the European Union explicitly safeguards the right to data protection for 'everyone,' which has been interpreted to include children.[56] This provision establishes data protection as a fundamental human right that applies to all individuals, regardless of age.[57]

Furthermore, the legal foundation for children's data protection can be traced back to the founding treaties of the EU. The Treaty on European Union establishes data protection as a fundamental human right that underpins the Union's values and objectives.[58] Article 16 of the Treaty on the Functioning of the European Union[59] further enshrines the right of all individuals to the protection of their personal data, requiring the European Parliament and Council to enact legislation to this end.

It is on this basis that the GDPR was adopted and is now applicable. The AI Act, on the other hand, was enacted in response to the growing prominence of AI systems and aims to regulate them, including those used in the education sector. Together, the GDPR and AI Act lay down the law on the use of biometric data which are characteristic of attention monitoring systems.

#### III.1.1. *Key Definitions and Legal Scope in the AI Act and GDPR*

Affective computing and attention monitoring systems in educational settings often rely on biometric data such as facial expressions, voice, and physiological signals to detect and respond to students' emotional and cognitive states. However, other attention monitoring systems also employ non-biometric data, such as on-screen activity[60], test completion rates[61] or keyboard stroke[62] tracking to determine the attentiveness of students. Under

[56] Council of Europe, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment-- Recommendation CM/Rec(2018)7 of the Committee of Ministers, 12–22 (2018), https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.

[57] Article 29 Data Protection Working Party, Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) 3 (2009), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf.

[58] Consolidated Version of the Treaty on European Union of 2016, 202 OJ C 202/17.

[59] Consolidated Version of the Treaty on European Union of 2016, 202 OJ C 202/55.

[60] M. Dorge et al., *Screen Activity Monitoring Using Federated Learning*, in 2025 International Conference in Advances in Power, Signal, and Information Technology (APSIT) 1 (2025), https://ieeexplore.ieee.org/abstract/document/11086241.

[61] T. C. Papadopoulos et al., *Assessment of Attention in School Children: Teachers' Ratings Related to Tests of Attention*, 17 European Journal of Special Needs Education, 15 (2002).

[62] V. Kuvar et al., *Partner Keystrokes Can Predict Attentional States during Chat-Based Conversations*, *in* Proceedings of the 16th International Conference on Educational Data Mining 217 (M. Feng, T. Käser, & P. Talukdar eds., 2023), https://zenodo.org/record/8115697.

both the AI Act and GDPR, these affective computing technologies intersect with key legal concepts and definitions.

*Biometric data under GDPR*

Biometric data is defined in the GDPR as 'personal data resulting from specific technical processing relating to a natural person's physical, physiological or behavioural characteristics, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.'[63] Personal data, more broadly, refers to 'any information relating to an identified or identifiable natural person ('data subject').'[64] Facial recognition, gaze tracking, and other physiological signals processed by attention monitoring systems fall under these definitions.[65]

The GDPR categorises biometric data as a 'special category' ( or 'sensitive data') of personal data.[66] Special categories of data include data revealing one's racial, ethnic, political, religious or philosophical beliefs as well as data concerning one's health, sex life or sexual orientation.[67] These data are considered sensitive because of their significant risk to 'fundamental rights and freedoms'[68] and therefore trigger heightened protections. Consequently, the processing of such data is generally prohibited, unless specific conditions are met, such as explicit consent, substantial public interest, or necessity for preventive/occupational health.[69] These exceptions to the general prohibition of processing of special categories of data are interpreted strictly.[70]

However, the GDPR's scope is limited in certain respects when it comes to affective computing technologies.[71] The regulation does not apply to anonymous information, and its definition of biometric data is confined to information that allows or confirms unique identification.[72] Thus, biometric data processing that does not identify or render the data subject identifiable falls outside its material scope.[73] For example, a system that analyses aggregated or anonymised emotional responses for non-individualised purposes may not qualify as personal data processing under the GDPR.[74] In practice, however, anonymisation in educational settings is rare, as such systems are usually tied to named students and used for evaluative purposes.[75]

Moreover, emotion data is not automatically classified as 'special category' personal data under Article 9 GDPR. This special category designation only applies if the emotion data is derived from physiological sources that enable unique identification, such as facial images or fingerprints. This distinction means that visual approaches relying solely on

63 GDPR art 4(14).
64 *Id.* at art. 4(1).
65 AI Act r 15.
66 GDPR art 9, r 51.
67 *Id.* at art. 9(1).
68 *Meta Platforms Inc and Others v Bundeskartellamt* 66 (ECJ 2023).
69 GDPR art 9(1) (a-j); *Meta Platforms Inc and Others v Bundeskartellamt*, *supra* note 68, paras 74–85.
70 *Meta Platforms Inc and Others v Bundeskartellamt*, *supra* note 68, para 76.
71 A. Häuselmann et al., *EU Law and Emotion Data*, *in* 2023 11th International Conference on Affective Computing and Intelligent Interaction (ACII) 1, 3 (2023), https://ieeexplore.ieee.org/document/10388181/.
72 GDPR r 26, art 4(14), 9.
73 L. Menges & E. Weber-Guskar, *Digital Emotion Detection, Privacy, and the Law*, 38 Philosophy & Technology 77, 84 (2025).
74 *Id.* at 85.
75 *See* A. P. Carvalho et al., *Big Data, Anonymisation and Governance to Personal Data Protection*, in The 21st Annual International Conference on Digital Government Research 185 (2020), https://dl.acm.org/doi/10.1145/3396956.3398253.

facial expressions may escape enhanced protections, whilst physiological approaches processing data like heartbeat or electrodermal activity generally fall within them. This differential treatment reflects the GDPR's focus on identifiability and biometric identification as the key criteria for heightened protection. Yet even when not classified as special category data, emotion and attention inferences remain personal data, subject to GDPR principles of lawfulness, fairness, necessity, and proportionality. This creates a regulatory gap: certain attention monitoring systems may escape the strictest safeguards despite producing highly sensitive inferences about students' emotional states.

*Biometric data under the AI Act*

The AI Act and its follow-up commission guidelines[76] *attempt* to address some of these gaps by including specific provisions related to 'emotion recognition systems' (ERS)[77], and other affective computing technologies.

The keyword here is *attempt,* since the current definition of emotion recognition systems suffers from two key limitations. First, the Act defines an ERS system as 'an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data'[78]. Biometric data under the Act reproduces the exact wording of the GDPR[79], tying its scope to data that enable or confirm the unique identification of an individual.

This definitional choice has a narrowing effect: only systems that rely on biometric signals such as facial images, voice, or physiological patterns are captured. Emotion or attention inference based on non-biometric indicators, such as on-screen activity[80], time spent on task[81], or log-in patterns[82], thus falls outside the prohibition on ERS in educational settings, even though such systems may generate comparably sensitive inferences. However, such systems may still qualify as personal data processing under the GDPR, insofar as the inferences are linked to identifiable students, and may be categorised as high-risk under the AI Act where they play a role in assessment or progression decisions. Their definitional status is therefore one of partial exclusion: they escape the strictest categorical safeguards of EU law but remain potentially subject to general obligations depending on their deployment.

Second, the inclusion of both 'emotions' and 'intentions', even though they are intertwined, produces an overbroad and conceptually ambiguous category. Emotions, though difficult to standardise, refer to recognisable affective states.[83] Intentions, by contrast, imply predictions about future behaviour, such as whether a student is likely to

[76] European Commission, Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act) (2025).

[77] The term 'emotion recognition system' is used in the Act to refer to the broader concept of affective computing. *See* D. Iren, L. P.J.J. Noldus, & A. M. Brouwer, AI Act & Guidelines on Prohibited Artificial Intelligence (AI) Practices: An Analysis for the Emotion Recognition Field 1 (2025), https://www.aigl.blog/content/files/2025/04/AI-Act---Guidelines-on-Prohibited-Artificial-Intelligence--AI--Practices--An-Analysis-for-the-Emotion-Recognition-Field.pdf.

[78] AI Act art 3(39).

[79] *Id.* at art. 3(34); GDPR art 4(14).

[80] P. Krieter & A. Breiter, *Track Every Move of Your Students: Log Files for Learning Analytics from Mobile Screen Recordings*, *in* Die 16. E-Learning Fachtagung Informatik (DELFI) (2018).

[81] D. Mistry et al., *Privacy-Preserving On-Screen Activity Tracking and Classification in E-Learning Using Federated Learning*, 11 IEEE Access 79315 (2023).

[82] V. Mandalapu et al., *Student-Centric Model of Login Patterns: A Case Study with Learning Management Systems* (International Educational Data Mining Society 2021) https://eric.ed.gov/?id=ED615654 (last visited Oct. 15, 2025).

[83] K. Mulligan & K. R. Scherer, *Toward a Working Definition of Emotion*, 4 Emotion Review 345, 346 (2012).

disengage, cheat, or drop out.[84] By conflating these distinct forms of inference, the Act risks sweeping together fundamentally different technologies while at the same time failing to provide clear boundaries for what counts as ERS. The conflation of these categories makes it difficult to establish clear boundaries for what counts as ERS, reducing legal certainty.

### III.1.2. *EU Legal Implications for Attention Monitoring Systems*

The definitional analysis above shows where (non) biometric attention monitoring systems sit within the GDPR and the AI Act. What matters next is not only the regulatory categories themselves, but how the obligations that follow from them interact with the rights of children. Against this backdrop, the obligations set out in the GDPR, and the AI Act must be read through a child-centred lens: one that rests on the CRC principles and recognises the long-term consequences of profiling in educational settings.

#### *Compliance with the GDPR*

The GDPR's primary aim is to protect all individuals' fundamental right to data protection, with children explicitly recognised as the only group[85] in the GDPR requiring 'specific protection' in data processing.[86] This protection extends in particular to collecting their data for marketing or services offered directly to them.[87] To this end, data controllers processing children's data are required to provide information regarding such processing in clear and plain language 'that [a] child can easily understand'[88].

Additionally, the GDPR imposes strict obligations on all data controllers to comply cumulatively with the principles in Article 5, namely fairness, lawfulness, transparency, purpose limitation, proportionality, data minimisation, accuracy, storage limitation, confidentiality, and accountability. Compliance with one principle does not excuse non-compliance with another.[89] Children are also afforded individual data subject rights, including the right to erasure[90], data portability[91] and the right to be informed[92]. Relatedly, all processing must be grounded in on one of the legal bases listed under article 6, among which consent, contract and legitimate interest of the controller are the most relevant for children's data processing.

It is doubtful that data processing in attention monitoring systems can meet these cumulative obligations. Whilst this paper does not analyse every principle and right in detail, it focuses on consent as a legal basis for data processing and the proportionality and

---

[84] V. G. Morwitz & K. P. Munz, *Intentions*, 4 Consumer Psychology Review 26, 27 (2021).

[85] The GDPR refers to children as 'vulnerable' (recital 75). However, academics have criticised such inference and instead argue for a more agency-oriented outlook in children's rights protection. *See* for example L. Lundy, *Vulnerability Should Not Eclipse Agency: Children's Perspectives on Their Own Lives*, *in* Perspectives on Children, Rights, and Vulnerability 31 (2025), https://www.scup.com/doi/10.18261/9788215069500-25-03.

[86] GDPR r 75.

[87] *Id.* at art. 38.

[88] *Id.* at art. 58.

[89] A. Atabey & R. Scarff, *The Fairness Principle: A Tool to Protect Childrens Rights in Their Interaction with Emotional AI in Educational Settings*, 4 Global Privacy Law Review 5, 5 (2023).

[90] GDPR art 17.

[91] *Id.* at art. 20.

[92] *Id.* at art. 13, 14.

fairness principles to illustrate that such systems are unlikely to comply with GDPR's requirements.

At the heart of the GDPR is the requirement for consent to process data. Consent under the GDPR is valid when certain conditions are met: It has to be freely given, specific, informed and unambiguous,[93] taking into account the maturity of the concerned child. Additionally, under Article 8, only children who are at least 16 years old can consent to information services offered to them; otherwise, parental/guardian consent is required[94]. Because of the inherent imbalance of power that exists between educational institutions and children[95], consent is unlikely to be freely given. Children and their guardians often have little practical choice but to accept such technologies if they are integrated into the learning environment, undermining the voluntariness of consent. Furthermore, the complex nature of attention monitoring, which often involves opaque algorithmic inferences and data flows, makes it nearly impossible for data subjects to provide fully informed consent.

Likewise, the proportionality of the use of attention monitoring systems is questionable. Proportionality is closely tied to the purpose limitation and data minimisation principles[96] and requires that any interference with privacy be necessary and not excessive in relation to the aim pursued. Attention monitoring systems involve the continuous and granular collection of data, often in real-time, ostensibly to improve student engagement. While such an objective could be educationally desirable, the scale and sensitivity of data processing in these systems exceed what is necessary to achieve their stated objectives.[97] Moreover, a proportionality assessment requires an account not only of the volume of data collected but also of the potential harms[98], such as the normalisation of surveillance[99], chilling effects on student behaviour[100] or long-term risks of profiling[101].

Finally, the fairness principle, embedded in Article 5(1)(a) GDPR, is also challenged by the use of attention monitoring systems. Fairness operates as a normative safeguard, ensuring that data processing respects individuals' reasonable expectations and does not reproduce unjust outcomes. The opacity that characterises attention monitoring systems makes it difficult for children and parents to understand how their data is processed. Additionally, such systems may also misinterpret attention cues, which are subjective and vary according to one's cultural background[102], behavioural or neurodivergent differences[103]. This lack of fairness and accuracy in the data processing can have significant consequences for children, potentially leading to unfair outcomes that undermine their educational experiences and opportunities.

---

93 *Id.* at art. 4(11).

94 Member states, however, can choose to lower the age, which should not be lower than 13.

95 Atabey and Scarff, *supra* note 89 at 13.

96 M. Finck & A. J. Biega, *Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems*, 2021 Technology and Regulation 44, 57 (2021).

97 D. Lupton & B. Williamson, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, 19 New Media & Society 780, 789 (2017).

98 Article 19, Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights 28,30 (2021), https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

99 Lupton and Williamson, *supra* note 97 at 789.

100 Atabey and Scarff, *supra* note 89 at 10.

101 Article 19, *supra* note 98 at 30.

102 *See* L. F. Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, 20 Psychol Sci Public Interest, 1 (2019).

103 N. Ouherrou et al., *Comparative Study on Emotions Analysis from Facial Expressions in Children with and without Learning Disabilities in Virtual Learning Environment*, 24 Education and Information Technologies 1777, 1785 (2019).

These data protection principles, which are central to the various data subject rights enshrined in the GDPR, are enforced by independent Data Protection Authorities (DPAs).[104] DPAs are competent to receive complaints, including those submitted by or on behalf of children, and may issue a variety of administrative procedures, including warnings, fines, and reprimands, when infringements occur.[105]

However, the complex and often opaque nature of attention monitoring systems presents significant challenges for DPAs in effectively supervising and regulating their deployment, particularly in the context of protecting children's rights and interests. This is because, in and of itself, the GDPR is limited in scope, in that it does not effectively account for 'different layers of vulnerabilities of children'.[106] For instance, children with learning difficulties or neurodivergent conditions may face heightened risks when attention monitoring systems process their behavioural data, as the GDPR does not explicitly address how such intersecting vulnerabilities should be integrated into data protection assessments. This regulatory gap finds partial expression in the AI Act's risk-based framework. Nevertheless, as the following section illustrates, the Act's narrowly defined conception of 'risk' leaves important gaps in the protection of children's rights and interests.

*Compliance analysis under the AI Act*

Building upon the GDPR's data protection framework, the AI Act introduces complementary, risk-based approach to the regulation of AI systems. This tiered model[107] assigns differentiated obligations to deployers and data controllers depending on system's assessed risk profile.[108] However, while the Act refrains from defining the notion of 'risk', it adopts a relatively narrow interpretation, confining its scope to health, safety, and fundamental rights concerns.[109] Notably, the Act does not outline any criteria for categorising the different levels of risk.[110] This limited framing raises questions about whether the Act sufficiently captures the nuanced or context-specific harms, such as those affecting special-interest groups, including children, that arise from the deployment of attention-monitoring systems.

To operationalise this framework, the Act categorises AI systems into five distinct risk levels, each corresponding to a different degree of regulatory intensity; These comprise: (i) prohibited practices posing unacceptable and unmitigable risks; (ii) high-risk systems subject to a variety of obligations; (iii) general-purpose AI models with transparency requirements; (iv) limited-risk AI systems with lighter transparency obligations; and (v) minimal-risk systems, such as chatbots or simple recommendation engines, largely exempt from the Act's transparency rules. Yet, the classification of certain technologies, such as attention monitoring systems, within this hierarchy remains legally and conceptually contested, particularly where their deployment intersects with the protection of children's fundamental rights.

---

104 GDPR r 116–123.

105 *Id.* at art. 58.

106 Atabey and Scarff, *supra* note 89 at 12.

107 G. Makauskaite-Samuole, *Transparency in the Labyrinths of the EU AI Act: Smart or Disbalanced?*, 8 Access to Justice in Eastern Europe, 38, 42 (2025).

108 AI Act r 26.

109 *Id.* at art. 52,53,72; N. A. Smuha & K. Yeung, *The European Union's AI Act: Beyond Motherhood and Apple Pie?*, in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* 228, 236 (N. A. Smuha ed., 2025).

110 M. Ebers, *Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, 16 European Journal of Risk Regulation 684, 692 (2025).

The AI-Act risk-based framework impacts attention monitoring and affective systems to differing degrees. Despite the definitional ambiguity surrounding ERS systems, the Act explicitly bans AI systems used to identify or infer emotions through biometric data processing in educational settings, except for health and safety reasons.[111] Follow-up commission guidelines clarify that whilst article 5(1)(f) does not explicitly mention ERS systems, the prohibition under this article should be interpreted as having the same scope as rules applicable to other ERS systems as provided under Annexe III (1)(c) and Article 50 AI Act.[112] Most importantly, the guidelines confirm the limitations on biometric data discussed above.

Concerns over the limited reliability, generalisability, and cultural variability of these technologies justify the prohibition in Article 5(1)(f)[113] , as well as the recognised imbalance of power in educational (and work) settings[114].
This limited prohibition under Article 5(1)(f) creates two distinct scenarios for attention monitoring systems:

1. AI systems that infer emotions for medical or safety reasons are permitted but classified as high-risk, triggering strict obligations.[115] These include establishing a risk management system[116], implementing a data quality and governance framework[117], producing technical documentation[118], and maintaining human oversight to ensure effective review of automated decisions[119].
2. Non-biometric attention monitoring systems could be classified as either high-risk or low-risk, depending on their functionalities. High-risk systems in educational contexts include those that influence grades, affect progression or access to opportunities, or shape educational pathways.[120] Lower-risk systems, such as those using aggregate analytics (for instance, '10% of the class is disengaged after 20 minutes), are still subject to general AI Act obligations like accuracy, transparency, copyright, and system evaluation requirements.[121]

The transparency obligations for high-risk systems are quite comprehensive. Providers must disclose detailed information to users and affected individuals, such as the purpose and functionality of the system, accuracy rates, and potential biases. In the context of children, this includes explanations comprehensible to minors and their guardians. However, the Act stops short of requiring the disclosure of the specific emotions detected to individuals, a gap that was unaddressed under the GDPR. This increased transparency is vital given these systems' significant impact on the fundamental rights of children.
Regarding enforcement, the Act sets up mechanisms such as market surveillance by authorities[122], conformity assessments[123], and fines for non-compliance[124]. These tools

111 AI Act art 5(1)(f).
112 European Commission, *supra* note 76 at 244–246.
113 AI Act r 44.
114 *Id.*; European Commission, *supra* note 76 at 253.
115 *See* AI Act section 2.
116 *Id.* at art. 9.
117 *Id.* at art. 10.
118 *Id.* at art. 11.
119 *Id.* at art. 14.
120 *Id.* at art. 127 Annex III 3.
121 *Id.* at art. 53(1), 55(1).
122 AI Act r 156.
123 *Id.* r 173; art. 16(f).
124 *Id.* r 168; art. 99.

provide a more proactive approach to ensuring compliance compared to GDPR's mainly reactive, complaint-based system.

III.1.3. *Analysis EU law: Children's rights and data protection*

An examination of the GDPR and AI Act shows that both pieces of legislation recognise that affective and attention-monitoring systems in education are high-stakes, high-risk, and require unique, children's rights-centred legal attention. Both regulations attempt to translate CRC principles (*non-discrimination*, the *best interests of the child*, a *child's right to survival and development*, and the *participation and inclusion* principles) into technical and procedural safeguards for children exposed to affective and attention-monitoring technologies.

The CRC mandates that all children enjoy their rights without discrimination.[125] The AI Act and GDPR embody this principle by emphasising the need to protect children from discriminatory outcomes arising from the use of AI-driven affective computing systems. Recital 28 of the AI Act highlights concerns over manipulative and exploitative practices enabled by AI, stating such practices are 'particularly harmful and abusive and should be prohibited because they contradict Union values. including the right to non-discrimination, to data protection and to privacy and the rights of the child'. Within the GDPR, recital 75 specifically flags risk of discrimination as a key reason for affording special protection to children. Similarly, *Non-discrimination* is reflected in the GDPR's fairness, purpose, and accuracy obligations[126], and in the AI Act's requirement to test for bias, ensure data quality, and monitor discriminatory outcomes[127], which together force developers and deployers of attention-monitoring technologies to consider the disparate impact on children.

Article 3 requires that the *best interests of the child* be a primary consideration in all actions concerning children. This principle is given effect by GDPR's special protection for minors[128], i.e., high-threshold consent requirements and tailoring information for children, and by the AI Act's specific prohibition of ERSs in education settings, except for narrowly defined safety or medical uses[129]. This precaution privileges children's welfare over unfettered deployment.

Similarly, the child's right to *survival and development*[130] is advanced through GDPR's data minimisation, purpose limitation, and restrictions on profiling[131], which limits harmful inferences that could stigmatise or channel a child's educational trajectory. The AI Act complements this with mandatory risk-management and corrective action duties for high-risk systems.[132]

Finally, *participation and inclusion* are supported by heightened transparency and information obligations: the GDPR requires clear, age-appropriate notices and parental/guardian consent where relevant[133], and the AI Act imposes disclosure obligations for systems that

[125] CRC art 2.
[126] GDPR art 5(1) (a), 5(1) (c), 25.
[127] AI Act arts 10, 15, Annexe III.
[128] GDPR art 5(1) (a), 5(1) (c), 25.
[129] AI Act art 5(1) (f), Annexe III.
[130] CRC art 6.
[131] GDPR art 5,9,22.
[132] AI Act art 9,20,27.
[133] GDPR art 6,8,12.

interact with or infer states of natural persons[134] and human-oversight safeguards[135] to preserve meaningful agency.

However, some gaps persist, notably a definitional and scope ambiguity within EU law. The GDPR and AI Act do not entirely align on how biometric data and ERSs are defined and when they fall within heightened protection or prohibition. As discussed above, this produces uncertain coverage for some attention-monitoring tools (e.g. systems that infer affect based without uniquely identifying pupils or those using non-biometric proxies), and hence uneven legal obligations for providers and schools. Placing this internal EU ambiguity beside China's comparatively permissive approach where attention monitoring systems have been widely deployed under a different mix of state oversight, parental authority and education policy, brings to focus the contrast and similarities in approaches in the two jurisdictions. It also provides a vantage point for examining the potential and limits of the Brussels Effect: the capacity of EU law to influence regulatory practices beyond its borders. Whereas both jurisdictions recognise that children merit particular protection in the digital sphere, they operationalise this recognition in markedly different ways. The following section analyses Chinese law relevant to attention monitoring systems. Thereafter, a comparative assessment of both legal frameworks will be proffered.

### III.2 *China's Legal Framework on Children's Biometric Data Protection*

The establishment of Chinese privacy and data protection law came later than in Europe.[136] In terms of legislative approach, it initially drew on EU-style techniques by centring regulation on the processing of personal information, while distinguishing between privacy protection and the regulation of information processing.[137] The 2020 Civil Code systematised personality rights, explicitly including privacy as one category and framing its protection in the context of interpersonal relationships.[138] The 2021 Personal Information Protection Law (PIPL)[139], China's first dedicated data protection law, establishes the rights of data subjects and sets out principles for lawful processing, framing its protection in the context of information processing activities.[140] Together, these two laws form a complementary *dual-track system*, in which the Civil Code safeguards individual autonomy and dignity, while the PIPL governs personal data processing and compliance obligations, reflecting both EU-inspired principles and China's distinct focus on balancing individual rights, security, and digital sovereignty.

Against the backdrop of the gradual deployment of affective computing and attention monitoring in schools, China has not yet enacted a unified AI law. Current governance relies on sector-specific regulations[141], which provide limited constraints on the use of AI

134 AI Act art 50(3).
135 *Id.* at art. 14.
136 E. Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 Penn State Journal of Law & International Affairs 49, 53 (2020).
137 X. Ding *The Jurisprudential Relationship between the Protection of Privacy Rights and Personal Information Protection*, 40 Studies in Law and Business 61, 63–64 (2023).
138 Civil Code of the People's Republic of China of 2020.
139 Personal Information Protection Law of the People's Republic of China of 2021.
140 M. He & Y. Chen, *Personal Data Protection in China: Progress, Challenges and Prospects in the Age of Big Data and AI,* Telecommunications Policy 49, 1–28 (2025).
141 The current governance structure relies heavily on sectoral regulations and administrative rules issued by specialised agencies such as the Cyberspace Administration of China (CAC), particularly in relation to algorithmic transparency, data governance, and content moderation. Notable examples include the *Provisions on the Administration of Algorithmic Recommendation for Internet Information Services* (2021) and the *Provisions on the Administration of Deep Synthesis for Internet Information Services* (2022).

in educational settings but remain fragmented and lack systematic operational standards.[142] In addition, regarding biometric information, China has no standalone legislation and instead relies on a fragmented protection framework established through the PIPL and the Civil Code.

III.2.1. *Legal Recognition and Conceptual Uncertainty under the Civil Code*

In the Chinese legal system, 'biometric information' has been recognised as an independent 'civil interest' instead of a 'civil right'[143], mainly reflected in Chapter 6 Protection of Privacy and Personal Information of Part IV Personality Rights of the Civil Code, as well as in Chapter 2 Protection of Sensitive Personal Information of the PIPL.[144] This recognition progresses from the Civil Code, as the general law, to the PIPL, a specialised law. However, issues regarding its legal nature, specific rights and powers, and methods of protection still require further clarification and in-depth study.

Specifically, Article 1034 (2) of the Civil Code enumerates biometric information as a type of personal information; [145] it does not confer an independent right to personal information, which means protection relies on privacy rights and tort remedies, rather than allowing individuals to assert claims solely based on their biometric information. Moreover, its placement under the chapter on privacy and personal information protection should not be misconstrued as equating biometric data with privacy rights. Notably, Paragraph 3 of the same article provides that confidential information within personal information may be governed by the rules on the right to privacy.[146] However, this does not mean that biometric data, by default, constitutes such confidential information. Consequently, the legal characterisation of biometric information remains uncertain.

Therefore, under the Civil Code, it is necessary to determine whether biometric information qualifies as confidential information. The Civil Code does not provide explicit criteria for determining what constitutes confidential or private information. According to judicial practice—for instance, in the *WeChat Reading Case*[147]—the plaintiff argued that their WeChat friend list and reading records should be regarded as private information. However, the court rejected this claim. The judge reasoned that privacy refers to information that an individual does not wish others to know, emphasising the element of subjective intent. Nonetheless, such intent cannot be determined solely by the individual's personal will; it must also accord with the general standard of reasonableness recognised by society. This general perception of what is considered private may vary depending on factors such as region, cultural tradition, legal tradition, and social custom. Therefore, the determination of privacy must be made on a case-by-case basis, taking into account the specific context and its broader social implications.

When biometric information is recognised as *confidential*, three protective pathways become available for invocation. First, rely on Article 1033, which strictly prohibits acts

142 X. Fu, *The unified legislation on artificial intelligence should proceed with caution*, Oriental Law 17, 20 (2025).

143 Ding, *supra* note 137 at 65.

144 L. Cui, *Legal Characterization and Regulatory Approaches to Personal Biometric Information: An Analysis Based on Article 1034 of the Chinese Civil Code*, 313 Study & Exploration 73, 73 (2021).

145 Civil Code of the People's Republic of China 2020, art 1034(2).

146 *Id.* at art. 1034(3). 'Private information within personal information is subject to the provisions on the right to privacy; where there are no such provisions, the rules on personal information protection shall apply.'

147 *Xunxun Technology (Shenzhen) Co., Ltd. et al., Online Infringement Liability Case* (China) [2020] Beijing Internet Court (2019) Jin 0491 Min Chu No. 16142.

that infringe upon an individual's peace of private life, private space, private activities, or confidential information, unless otherwise provided by law or explicitly consented to by the right holder.[148] Second, regarding remedies, the specific provisions on the protection of personality rights may be applied. These include the general clause on personality rights (Article 990)[149], the right to claim relief for infringements on personality rights (Article 995)[150], and the injunction provision (Article 997)[151]. Third, one may invoke the general tort provisions as a fallback remedy, specifically Articles 1165 and 1166,[152] in the Part on Torts, which provide general protection against infringements. If biometric information is not recognised as private information, the data subject may find it difficult to obtain effective remedies under the Civil Code's provisions on personality rights or tort liability. In such cases, they must instead rely on the administrative or compliance mechanisms provided by the PIPL, rather than asserting a civil claim in the tort law sense. This *dual-track* structure results in significantly different levels of protection for the biometric data of children.

III.2.2. *Regulatory Framework and Compliance Obligations under the PIPL*

Under Article 28 of the PIPL, biometric data is explicitly classified as 'sensitive personal information', defined as data that, if leaked or illegally used, may infringe upon a natural person's dignity or endanger their personal or property safety.[153] Article 29 requires obtaining separate consent for processing sensitive personal information, and Article 30 further mandates that data controllers clearly justify the necessity of processing and explain its potential impact on individual rights.[154] Article 26 further regulates the use of image-capture and identity-recognition devices in public spaces, limiting such use to the necessity of maintaining public safety and requiring prominent notification. The collected data for such purposes may not be repurposed without separate consent.[155] Moreover, Article 31 introduces additional obligations for handling 'minors' personal information'. When processing the personal data of children under the age of fourteen, controllers must obtain the consent of their parents or other guardians and establish dedicated processing rules specifically designed for minors' data.[156]

148 Civil Code of the People's Republic of China art 1033.
149 *Id.* at art. 990. 'Personality rights are the rights enjoyed by civil subjects, including the right to privacy and other related rights.'
150 *Id.* at art. 995. 'Where personality rights are infringed, the victim has the right to request the infringer to bear civil liability in accordance with this Law and other applicable laws...'
151 *Id.* at art. 997. 'Where a civil subject has evidence proving that another party is committing or is about to commit an unlawful act that infringes upon their personality rights, and failure to stop such an act in time would cause irreparable harm to their legitimate rights and interests, the civil subject has the right to apply to the People's Court for an order requiring the other party to cease the relevant act in accordance with the law.'
152 *Id.* at art. 1165,1166. Article 1165: 'A person who infringes upon the civil rights and interests of others due to his fault shall bear tort liability. If it is presumed by law that the person is at fault, and the person cannot prove that he is not at fault, he shall bear tort liability.' Article 1166: 'If the law stipulates that a person shall bear tort liability for damaging the civil rights and interests of others, regardless of whether the person is at fault, such provisions shall apply.'
153 Personal Information Protection Law of the People's Republic of China (adopted 20 august 2021, effective 1 november 2021) of 2021.
154 *Id.* at art. 29, 30.
155 *Id.* at art. 26.
156 PIPL art. 31.

However, these provisions are largely principled and abstract, lacking specific standards for implementation and enforcement.[157] Violations involving biometric data often involve procedural breaches, such as failure to inform or failure to obtain clear consent, but it remains difficult in practice to determine whether such infringements of the right to be informed and the right to autonomous decision-making constitute legally remediable harm, thereby creating barriers to individual redress.[158] Moreover, under Article 26, the installation of image and identity recognition devices is permitted in public spaces solely for the purpose of maintaining public safety. However, educational environments such as classrooms serve pedagogical or administrative purposes rather than public safety functions. Therefore, their regulation should not be analogised to public-space surveillance but should instead be subject to stricter consent and transparency requirements, particularly when minors' biometric data are involved.

III.2.3. *Practical Limitations of the Civil Code and PIPL: Insights from Judicial Cases*

Civil remedies under the Civil Code are only available when personal information is simultaneously recognised as private. In such cases, individuals may initiate a tort action based on the infringement of privacy rights. Nevertheless, this remedy often proves ineffective in practice because plaintiffs must bear the burden of proving the defendant's fault under tort law. For example, in *Luo v Company X, Privacy and Personal Information Protection Dispute*[159], the plaintiff was required to provide evidence demonstrating that the defendant had unlawfully collected his mobile phone number, which in practice entailed preserving and submitting all relevant communications and transaction records.

Similar evidentiary difficulties are further magnified in AI-enabled educational settings. The collection and processing of children's educational data is often continuous, opaque, and embedded within complex technological systems, making it difficult for children and their guardians to identify specific unlawful acts or attribute responsibility to particular data controllers.[160] Coupled with the structural power imbalance between educational institutions and children,[161] these characteristics significantly undermine the data subjects' practical ability to gather evidence and effectively pursue civil remedies. Consequently, rendering tort-based relief pathways largely ineffective in addressing data protection risks in AI-powered educational environments.

A significant legislative advancement in the PIPL is the introduction of the presumption of fault under Article 69(1), which shifts the burden of proof to the data controller. If the controller cannot prove that they are not at fault for the infringement, they must bear liability for damages.[162] This theoretically alleviates the evidentiary burden on minors and their guardians. However, under Article 69(2), which stipulates that compensation is determined by the losses suffered by the individual or the benefits obtained by the

[157] H. Zhu, *Definition of Sensitive Personal Information and Improvement of the Path of Handling*, Data Governance, 53.

[158] W. Fu, *A Legal Protection Model for Personal Biometric Data and China's Regulatory Approach*, Journal of East China University of Political Science and Law, 84 (2019).

[159] *Luo v Company X, Privacy and Personal Information Protection Dispute* (China) [2021] Beijing Internet Court (2021) Jing 0491 Min Chu No 5094.

[160] R. Taylor, *New Approaches to Data Stewardship in Education*, *in* Education Data Futures: Critical, Regulatory and Practical Reflections (2022).

[161] E. Day et al., *Who Controls Children's Education Data? A Socio-Legal Analysis of the UK Governance Regimes for Schools and EdTech*, 49 Learning, Media and Technology 356 (2024).

[162] PIPL art 69(1)

controller, and where both are difficult to determine, the court shall decide the amount based on actual circumstances.[163] In judicial practice, this valuation mechanism often results in nominal rather than substantial relief. The *Guo Bing v. Hangzhou Safari Park*[164] case vividly illustrates the difficulty of quantifying losses in biometric processing. Despite the unauthorized unilateral shift from fingerprinting to facial recognition, the court only awarded compensation for the plaintiff's direct out-of-pocket expenses (such as travel costs), while dismissing claims regarding the inherent value of facial data or the risk of its misuse.

This precedent suggests that under the PIPL, the actual circumstances clause may be interpreted restrictively. For children in educational settings, the loss of biometric privacy is an intangible and long-term risk rather than an immediate financial injury. If the judiciary continues to rely on a *tangible loss* standard, Article 69(2) effectively renders the presumption of fault a right without a remedy, as the cost of litigation for guardians far outweighs the meager compensation typical of such cases.

## IV. Comparative Insights

### IV.1 *EU regulatory framework vis-à-vis the Chinese regulatory framework*

The Chinese and European children's data protection regimes present both normative similarities and differences in governing attention monitoring systems in education. Both systems recognise the specific needs of children and provide enhanced protection for their data.[165] Standard provisions in both frameworks include consent requirements for processing children's data and the classification of biometric data as sensitive, with additional obligations for data controllers. Notably, under the PIPL, personal data for children under 14 is automatically classified as sensitive personal information.[166] Verdoodt, Zhang, and Lievens argue that the PIPL was inspired by the GDPR, hence the several points of convergence. They illustrate several areas where the EU and Chinese regulatory approaches converge, including these core protective principles.[167] Additionally, two significant differences in the regulatory framework: are noted: the lack of an independent supervisory authority in the Chinese framework, and the application of children-specific protections only to those under 14.[168]

| Aspect | European Union (GDPR & AI Act) | China (PIPL & Civil Code) |
|---|---|---|
| **Definition of Biometric Data** | Personal data enabling unique identification from physical, physiological or behavioural traits | Broad personal information, including biometric characteristics; special focus on children's data |

[163] *Id.* at art. 69(2).
[164] *Guo Bing v Hangzhou Wild Animal World Co., Ltd, Service Contract Dispute* (China) [2020] Zhejiang Higher People's Court (2020) Zhe 01 Min Zhong No 10940. In this case, the defendant unilaterally upgraded its entry system from fingerprint recognition to facial recognition without obtaining the plaintiff's explicit consent.
[165] Verdoodt, Zhang, and Lievens, *supra* note 52 at 18; GDPR recital 38; PIPL art 28
[166] PIPL art 28.
[167] Verdoodt, Zhang, and Lievens, *supra* note 52 at 18.
[168] *Id.*

| | | |
|---|---|---|
| **Scope of Regulation** | Processing of personal data and AI systems use in market/services; risk-based approach | Personal information processing within the territory and extraterritorially; emphasis on data security |
| **Protection of Emotion Data** | Not automatically 'special' data unless biometric or physiological data | Classified as sensitive for children; stringent consent for minors under 14 |
| **Transparency Requirements** | Clear and plain language for children; differential transparency obligations according to risk level of AI system; no requirement to disclose detected emotions | Children not explicitly mentioned, Information to children's guardians should be 'conspicuous and clear' (Art. 9 PIPL) |
| **Consent stipulations** | Generally, 16, can be lowered to 13-15 by Member States but only applies to information services (Article 8 GDPR) | 14 years, with parental consent requirement for younger children |
| **Supervisory authorities** | Independent data protection authorities with enforcement powers, the European Data Protection Board (EDPB) ensures consistent implementation; AI Act establishes and recognises different supervisory and implementation authorities including the AI Office (recital 148), Market surveillance authorities and competent national authorities | Multiple government bodies, no single independent authority |

Summary Table: Comparison of EU and Chinese Regulations on Affective Computing-based AI Monitoring Systems and Biometric Data

However, the regulatory logics underpinning the existing frameworks differ. Whereas EU law adopts a right, risk-focused approach that is at least partially responsive to children, Chinese law, characterised by the permissibility of attention monitoring systems in education, approaches it from a perspective of state oversight, parental authority, and educational management. The heightened safeguards in the GDPR and a categorical prohibition of biometric ERSs in schools under the AI Act confirm this European approach. China, by contrast, grounding its approach in data sovereignty and educational management, continues to deploy attention monitoring and affective systems in schools as part of a broader educational management and behavioural evaluation programmes, subject to generalised data protection obligations rather than categorical prohibitions.

Attention monitoring thus provides an important lens through which to test the robustness of the legal frameworks in protecting children's data. In both the EU and China, cracks and gaps remain. Regarding the EU model, the definitional uncertainty around what constitutes biometric data or an ERS, and the risk-based classification of AI systems in the AI Act, pose challenges for classifying attention-monitoring systems, some of which may fall outside the scope of regulation. On the other hand, the Chinese framework largely prioritises administrative oversight and parental consent, potentially leaving children exposed to surveillance and automated evaluation without proper safeguards.

This comparative perspective also raises questions of whether the 'Brussels Effect' may influence Chinese regulation in the future. Unlike the EU, where attention monitoring

systems in educational settings are not yet standard practice, China has rapidly deployed and continues to roll out such technologies nationwide. This rapid expansion of affective computing and attention monitoring in Chinese classrooms starkly contrasts with the more cautious approach in Europe. Whether this already affects the current and future alignment of Chinese law with the European framework is yet to be seen, as discussed in the following section.

### IV.2 *Brussels Effect or Independent regulatory approach?*

Both the GDPR and the AI Act exemplify the EU's growing ability to project its regulatory norms globally. This phenomenon, dubbed the 'Brussels Effect', is a term coined by Anu Bradford to describe the EU's unilateral capacity to shape global standards via market mechanisms rather than coercive diplomacy.[169] Companies seeking access to European markets adapt their practices to comply with EU rules, producing a form of *de facto* harmonisation beyond Europe's borders.[170] Elements of this influence can be observed in the evolution of China's data protection framework. The PIPL incorporates GDPR-inspired provisions, such as lawful bases for processing, special protection for minors, and recognisable data subject rights, indicating formal alignment between the two regimes.[171]
Yet, scholarship has increasingly questioned whether the *Brussels Effect* adequately captures the dynamics at play. Bradford describes the phenomenon where global businesses adapt to comply with EU law, but states maintain their domestic frameworks[172]. This leads to bifurcated compliance models where Chinese technological companies operating internationally design products to meet EU requirements while adhering to different state exigencies for their national operations.
In this context, Chinese purported alignment with EU law, such as the GDPR with the PIPL, has been described as a '*gravity assist'*, where the development of a country's privacy law results from internal and external factors (*sources of gravity*).[173] Driven by strategic motivations, a partial alignment of data privacy rules between regimes is viewed as a temporary phenomenon[174], so that the EU's unilateral regulatory influence will diminish once complying with EU standards outweighs the benefits. Thus, EU law functions less as a normative template and more as a reference point used strategically to bolster China's global legitimacy, facilitate data transfers and consolidate state-led governance.
These tensions are illustrated vividly when considering children's data protection in the context of affective computing and attention monitoring. While the AI Act explicitly bans ERS in schools, China still permits experimental use of EEG headbands and gaze-tracking systems, justifying them as educational efficiency and social control tools. The Brussels Effect thus results in only partial convergence: it influences the language and formal structures of Chinese data protection law but not its core commitments. Analysing the evolution of Chinese data protection law through the concept of gravity assists highlights the importance of differentiating between formal similarities and substantive alignment

169 A. BRADFORD, The Brussels Effect: How the European Union Rules the World (2020), https://scholarship.law.columbia.edu/books/232.
170 A. Bradford, *Exporting Standards: The Externalization of the EU's Regulatory Power via Markets*, 42 International Review of Law and Economics 158, 159 (2015).
171 Verdoodt, Zhang, and Lievens, *supra* note 52 at 18; R. Creemers, *China's Emerging Data Protection Framework*, 8 Journal of Cybersecurity 1, 6 (2022); W. Li & J. Chen, *From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China*, 54 Computer Law & Security Review 1 (2024).
172 Bradford, *supra* note 170 at 160.
173 Li and Chen, *supra* note 171 at 6.
174 *Id.*

when evaluating the global spread of EU standards in children's rights and educational technologies.

Still, the interaction between the EU and Chinese frameworks reveals the potential for reciprocal influence, even in the absence of full convergence. For instance, the PIPL's automatic classification of personal information of children under 14 as sensitive data establishes a higher threshold of protection than that provided under EU law, where no equivalent age-based presumption exists. However, this protection remains limited in scope. Children aged 14 to 18 occupy a legal grey zone: their personal information does not enjoy the same heightened protection, leaving their data in regulatory limbo. While EU law does not provide an explicit statutory definition of a child, the Article 29 Working Party[175] interprets this category consistently with Article 1 CRC, covering all individuals under 18.

Additionally, unlike in the EU, China's Constitution does not explicitly recognise personal information as a fundamental right, while the Civil Code classifies it merely as a type of personal information, with protection largely dependent on privacy rights as a remedy. The EU's rights- and risk-based approach under the GDPR and AI Act could, thus, inform future Chinese reforms by offering a model of rights-based contextualised protection and proactive oversight, particularly relevant to technologies such as attention monitoring systems.

## V. CONCLUSION

Attention monitoring and affective computing technologies in educational settings highlight the growing tension between technological innovation and the protection of children's fundamental rights. Because these systems process sensitive data such as emotion and biometric data, their governance warrants the highest level of legal protection.

The comparative analysis of the EU and China frameworks reveals both shared regulatory challenges and normative divergences. In the EU, the definitional ambiguities in the GDPR and AI Act risk leaving some emotion recognition and attention monitoring systems outside the formal scope of biometric data protection. However, the categorical prohibition on biometric-based ERSs in educational settings reflects a precautionary approach consistent with the Union's rights-based legal order. In contrast, China's framework, while demonstrating formal convergence with global data protection norms through the PIPL, continues to emphasise state imperatives alongside data protection and privacy considerations.

These findings also illustrate the global relevance and limits of European regulatory influence. Although European data protection models exert gravitational influence (*gravity assists*), substantive divergence persists where domestic priorities and conceptions of public interest prevail. The diffusion of EU-style data protection norms thus remains partial and value contingent, reflecting distinct regulatory cultures.

In conclusion, protecting children in AI-driven educational environments requires moving beyond narrow definitional boundaries towards a children's rights-centred governance framework. Such a framework, anchored in the CRC principles of non-discrimination, a child's best interests, participation, survival, and development, treats affective and attention monitoring systems with caution. It also ensures that technological innovation in education advances rather than compromises children's rights and dignity.

[175] Guidelines On Transparency Under Regulation 2016/679 (Adopted On 29 November 2017 As Last Revised And Adopted On 11 April 2018) 10 (2017).

# CENTRAL BANK DIGITAL CURRENCIES AND PRIVACY: A COMPARATIVE ANALYSIS OF REGULATORY APPROACHES IN THE EU AND CHINA

*Sonia Sforza*

TABLE OF CONTENTS:



*Central bank digital currencies (CBDCs) raise complex challenges concerning privacy, as they operate at the intersection of individual data protection, public interest, and state oversight.*
*This paper aims to propose a comparative assessment of the governance frameworks underpinning the digital euro and the e-CNY, the CBDCs respectively developed by the European Union and the People's Republic of China. This study focuses on how privacy is conceptualized and regulated in each model, taking into account their distinct legal traditions, specific sociocultural context and societal priorities.*
*The comparative analysis carried out in this paper also serves to reflect on the potential global implications of the two models, in a field where the development of common standards is essential to enable cross-border payments and, more broadly, to ensure the successful implementation of CBDCs.*

**Keywords**: Central Bank Digital Currency; privacy; personal data protection; surveillance; European Law; Chinese Law; Brussels Effect; Beijing Effect

## I. INTRODUCTION

The progressive digitalisation of monetary systems has brought Central Bank Digital Currencies (CBDCs)[1] to the forefront of both institutional and academic debate[2].

[1] Although there is no internationally agreed definition, certain recurring characteristics emerge in regulatory practices of CBDCs. These include: the classification of a CBDC as legal tender; its nature as a direct liability of the issuing central bank (see T. Mancini-Griffoli *et al.*, *Casting Light on Central Bank Digital Currency*, IMF Staff Discussion Note (2018), at 6); the possibility of issuance and distribution through centralised technological infrastructures or, subordinately, hybrid or partially decentralised infrastructures (see BIS, *Central bank digital currencies: foundational principles and core features*, Report n. 1 (2020), at 15). Additionally, if the CBDC is accessible to end users (households and businesses), it is referred to as a retail CBDC; if the CBDC is only available to certain institutions, mainly banks, it is referred to as a wholesale CBDC. See J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, Seton Hall L. Rev., 54 (2023), at 71.

[2] Globally, interest in these instruments is reflected in a wide array of projects, involving over 134 countries and monetary unions. See Atlantic Council, *Central Bank Digital Currency Tracker*, available at https://www.atlanticcouncil.org/cbdctracker/ (last visited Jul. 23, 2025). To date, three jurisdictions have launched a CBDC: the Bahamas, Jamaica and Nigeria. The Chinese digital yuan is currently the largest CBDC pilot project in the world, with a transaction volume of $986 billion in June 2024. Among the motivations for developing CBDCs, it is possible to identify a tendency among developed countries to regard their issuance as a means of safeguarding monetary sovereignty in the face of increasing competition from the private sector within the payments market, a competition most notably embodied by crypto-assets and, in particular, by stablecoins (see L. Beltrametti, G. B. Pittaluga, *Monetary Policy Implications of Stablecoins and CBDCs*, Economia internazionale, 76 (III, 2023), at 468-469, who highlighted widespread concern about stablecoins as a tool that could potentially undermine the monetary sovereignty of central banks, with negative consequences for the overall stability of the financial system). Conversely, in developing countries, the adoption of CBDCs appears primarily (though not exclusively) to aim at fostering financial inclusion by

Conceived as digital forms of legal tender issued by central banks, CBDCs differ from cash not only in their technological infrastructure, but also in the quantity and granularity of data they may generate through each transaction. Among the various legal and policy issues raised by these instruments, one of the most paradigmatic is the potential for central banks to collect massive amounts of data on end users. Such data aggregation raises serious concerns regarding mass surveillance, increases cybersecurity vulnerabilities, and opens the door to potential abuse or misuse by state authorities, particularly in the absence of clear and stringent safeguards[3]. These risks are further compounded by the involvement of private intermediaries, whose participation in the CBDC ecosystem can generate additional layers of data processing, thereby amplifying the potential for both security breaches and improper use of sensitive information[4].

This article aims to investigate – from a comparative perspective[5] and taking into consideration ideological, institutional, and socio-cultural foundations – how two major global actors, the European Union and the People's Republic of China[6], have approached the issue of privacy protection in the design and regulation of their respective CBDCs: the digital euro and the digital yuan (or e-CNY). The objective of this study is to understand how the regulators of both systems address, concretely, the delicate balance between control, efficiency, and individual freedom, thereby revealing whether, and to what extent, the legal system prioritizes the protection of the individual, collective security, or the safeguarding of institutions.

The analysis of the regulatory choices concretely adopted by these jurisdictions fits within the broader and growing body of legal scholarship on privacy and CBDCs. However, while the doctrinal debate has largely focused on theoretical aspects of the issue – such as CBDC design models that enhance privacy and the necessary balancing between privacy rights

expanding access to safe and efficient payment services for unbanked population (see: IMF, *Central Bank Digital Currency's Role in Promoting Financial Inclusion* (2023), at 2; A. Kosse, I. Mattei, *Making headway-results of the 2022 BIS survey on central bank digital currencies and crypto*, BIS Papers (2023), at 7).

[3] J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, cit., at 112.

[4] *Id.*, at 113.

[5] A. Gambaro, R. Sacco, M. Graziadei, Sistemi giuridici comparati (5th ed. 2024); R. Sacco, *Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II)*, The American Journal of Comparative Law 39 (I, 1991); M. Cappelletti, The Judicial Process in Comparative Perspective (1989).

[6] The decision not to include the United States in the core comparative analysis of this article is a conscious and methodologically motivated choice, grounded in the specific and distinctive approach adopted by U.S. authorities towards CBDCs. In contrast to jurisdictions actively developing retail CBDCs, the United States has recently taken a markedly different stance. In 2025, a presidential executive order formally prohibited the establishment, issuance, and circulation of a CBDC at the federal level (Executive Order of the President of the United States, *Strengthening American Leadership in Digital Financial Technology*, 23 January 2025, available at https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/). This decision reflects long-standing concerns within the U.S. debate regarding the potential implications of CBDCs for individual privacy, the distribution of monetary power, and the role of the state in financial intermediation. Opponents of a U.S. CBDC have argued that the introduction of a digital dollar could facilitate excessive governmental control over financial transactions and pose risks to civil liberties, while also disrupting the existing two-tier banking system. In this context, policy discourse has increasingly favoured market-based alternatives, particularly privately issued, dollar-denominated stablecoins, as instruments capable of supporting payment innovation without expanding the role of the central bank in retail finance (see D. Krause, *The Implications of a U.S. Ban on Central Bank Digital Currencies: Global Financial Dynamics and the Future of Payments* (2025), at 5-6).

and anti-money laundering/counter-terrorism financing objectives[7] – relatively little attention has been paid to the specific regulatory solutions adopted by individual jurisdictions[8].

In this still-evolving field, the comparative analysis assumes a fundamental role, as it enables the examination of heterogeneous regulatory models, the identification of convergent or divergent regulatory approaches, and critical reflection on the prospects for legal harmonisation or normative circulation.

This need is not merely theoretical, but also finds practical resonance in the increasing international focus on the potential for cross-border payments through CBDCs[9]. In this context, the concept of interoperability between different CBDCs acquires central importance. This term refers to the technical and operational capacity of digital currency systems issued by distinct monetary authorities to interact with one another, that is, to ensure mutual recognition and immediate convertibility[10]. In a globalised economy, achieving this objective appears to be of strategic importance in order to ensure the efficiency of cross-border transactions, reduce transaction costs, and promote financial inclusion[11]. However, technical interoperability necessarily presupposes a certain degree of legal interoperability[12]. The ability of different CBDCs to interact cannot disregard the existence of a lowest common denominator in relation to certain fundamental regulatory choices, particularly those concerning user identification, data ownership, as well as the allocation of access and control powers between public and private entities[13]. The absence

[7] K. P Murphy *et al.*, *Central Bank Digital Currency Data Use and Privacy Protection*, IMF – Fintech Notes (2024); Z. Wang, *Money laundering and the privacy design of central bank digital currency*, Review of Economic Dynamics, 51 (2023); N. Pocher, A. Veneris, *Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme*, IEEE transactions on network and service management, 19 (II, 2022); J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, cit..

[8] G. Kaur, *Privacy implications of central bank digital currencies (CBDCs): a systematic review of literature*. EDPACS, 69 (IX, 2024). The author conducted a literature review on the topic of CBDCs and privacy, identifying the areas that have attracted the most scholarly attention as well as the existing gaps. He highlighted that the approaches to privacy in CBDC design vary significantly across jurisdictions; however, few comparative assessments have been conducted, and in many cases, national privacy strategies remain opaque. Therefore, further comparative research could help clarify these divergences, contributing to the development of comprehensive legislative frameworks.

[9] Traditional cross-border payments are money transfers between parties located in different jurisdictions. These payments have been criticised for their high costs, slow execution, limited access and lack of transparency. Due to these critical issues, the G20 has identified the improvement of cross-border payments as a global priority. In this context, CBDCs represent an opportunity to rethink existing payment infrastructures, overcoming many of the current inefficiencies thanks to the possibility of designing shared solutions from the outset. However, this potential can only be realised if central banks consider the international dimension in the design of their digital currencies from the outset and coordinate to ensure interoperability. CPMI, BIS Innovation Hub, IMF and World Bank, *Options for access to and interoperability of CBDCs for cross-border payments*, Report to the G20 (2022), at 1-3.

[10] *Id.*, at 5.

[11] For example, CBDCs could be used by immigrant workers to send money to their families without the traditional transaction costs. See J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, cit., at 87.

[12] BIS and other Central Banks, *Central Bank Digital Currencies: Legal aspects of retail CBDCs* (2024), at 25; C. Mu, *Theories and practice of exploring China's e-CNY, Data, Digitalization, Decentralized Finance and Central Bank Digital Currencies: The Future of Banking and Money* (2023), at 187.

[13] BIS and other Central Banks, *Central Bank Digital Currencies: Legal aspects of retail CBDCs*, cit., at 25.

of a shared regulatory framework in these areas ultimately risks undermining not only user trust but also the overall success of CBDCs themselves[14].

Ultimately, building on these insights, this paper will analyse the potential influence that both the EU and PRC may exert on international regulatory trends, especially in a field that is devoid of common standards but where common standards are needed. On one side, the European Union has already demonstrated the capacity to shape foreign legal systems through the so-called Brussels Effect[15]. On the other, PRC may exert influence by leveraging its geopolitical network through the Belt and Road Initiative (BRI). In this light, the governance models of CBDCs adopted by these two actors may contribute to shaping future global standards in the field of CBDCs, particularly as regards privacy and data governance.

## II. CBDCs and Privacy Protection: A Theoretical Framework

Before proceeding, it is necessary to provide a theoretical premise regarding the specific relationship between CBDCs and the protection of personal data. The implementation of CBDCs is expected to lead to an exponential increase in the volume of financial data in circulation, data that is particularly sensitive, as it can reveal numerous personal characteristics, and which may therefore significantly affect individual freedom[16].

The issue outlined above arises from the fact that a CBDC, as mentioned, does not merely represent the dematerialised transposition of physical cash[17]. Rather, it entails regulatory choices that embody a structural tension between the protection of privacy and the safeguarding of public interests.

---

[14] CPMI, BIS Innovation Hub, IMF and World Bank, *Options for access to and interoperability of CBDCs for cross-border payments*, cit., at 3; C. Lopez, *Digital Currency: A Global Regulatory Framework is Needed*, in N. Bilotta, F. Botti, The (Near) Future of Central Bank Digital Currencies. Risks and Opportunities for the Global Economy and Society (2021), at 186.

Indeed, in a hypothetical scenario in which interoperability between CBDCs does not materialise, the risk emerges that digital currencies may reproduce, rather than overcome, the structural fragmentation of the current international payment system. In such a context, different regions could progressively align with distinct monetary and technological blocks, depending on economic ties, geopolitical influence, or infrastructural dependence. The absence of interoperability would thus limit the effectiveness of CBDCs in facilitating cross-border transactions and could result in the duplication of existing correspondent banking arrangements, along with their associated costs, delays, and barriers to access. Rather than constituting a transformative innovation, CBDCs would risk becoming digital replicas of the traditional system, thereby undermining their capacity to enhance efficiency, inclusion, and transparency in international payments. At the same time, even in the absence of full interoperability, forms of partial or functional interoperability could emerge, for instance through bilateral or multilateral arrangements, shared technical standards, or interoperability layers designed to enable limited cross-border use without full regulatory convergence. Such solutions, however, would likely remain fragile, as they would operate against the backdrop of divergent legal frameworks, particularly with respect to data governance, user identification, and the allocation of control between public and private actors. Against this background, the absence of interoperability would not merely represent a missed opportunity, but could actively undermine the transformative potential of CBDCs in the cross-border context.

[15] A. Bradford, The Brussels Effect: How the European Union Rules the World (2020).

[16] A. C. Penedo *et al.*, *Untangling Digital Euro's Personal Data Protection Challenges, An Exploration of Data Processing Activities and Latent Privacy Risk* (2024), at 8.

[17] Unlike any other digital payment method, cash is still the most privacy-friendly form of payment, as it is the only tool that guarantees complete anonymity. See: C. M. Khan *et al.*, *Money is Privacy*, Int'l Econ. Rev., 46 (II, 2005), at 377.

In this regard, it is no coincidence that the international debate has raised concerns about the potential use of CBDCs by authoritarian regimes for purposes of surveillance and political repression, with the attendant risk that the comprehensive monitoring of individual transactions may be exploited not for strictly economic objectives, but for political and social control[18]. Indeed, the architecture of many CBDC systems allows central banks – and, through them, state authorities – direct and real-time access to users' transactional data, thereby opening up ambivalent scenarios. On the one hand, this capability provides an important tool for monitoring financial flows, preventing criminal activities, and improving the overall efficiency of the monetary system[19]. On the other hand, such access could be used to restrict political action, for instance through the selective blocking of payments or the economic exclusion of individuals deemed "undesirable"[20].

In light of these risks, it is evident that design choices concerning CBDCs are never neutral: the way in which a digital currency is structured directly influences the degree of privacy protection and the safeguarding of fundamental rights[21]. In this context, the principle of privacy-by-design, whereby the protection of privacy must be embedded from the earliest stages of system development, assumes a pivotal role[22]. It is the responsibility of regulators to define the fundamental rights that must be effectively guaranteed and integrated into technological infrastructures, as well as to set clear limits on data control by the various actors involved[23]. A regulatory approach lacking in specific guidance – or, worse, entirely absent – risks legitimising the creation of opaque systems in which the rights and obligations of the parties involved are difficult to identify.

From this perspective, regulatory choices (or the absence thereof) and the consequent design of CBDCs ultimately constitute a political matter, as they presuppose a decision

---

18 K. Takami, *China's Bid for Digital-Yuan Sphere Raises Red flags at G-7* (2021), available at https://asia.nikkei.com/Spotlight/Cryptocurrencies/China-s-bid-for-digital-yuan-sphere-raises-red-flags-at-G-7 (last visited Jul. 23, 2025); R. Khalaf, H. Warrell, *UK spy chief raises fears over China's digital renminbi* (2021), available at https://www.ft.com/content/128d7139-15d6-4f4d-a247-fc9228a53ebd (last visited Jul. 23, 2025).

19 C.-Y. Tsang *et al.*, *Disciplining CBDCs: Achieving the Balance Between Privacy Protection and Central Bank Independence*, Nw. J. Int'l L. & Bus., 43 (2023), at 258.

20 N. Rancie *et al.*, *Central Bank Digital Currency (CBDC) and Digital Euro*, Economic and Social Development: Book of Proceedings (2024), at 4. Consider, for example, contexts in which political opposition is considered an illegal activity, making financial tracking a tool for political control. See M. Warren, *Let the Digital Euro Circulate: Introducing a Retail C.B.D.C. in the Eurozone with Unlimited Holdings by Users*, University of Bologna Law Review, 8 (I, 2023), at 20).

21 For an analysis of the various design choices, see J. Mascelli (2023). *Data Privacy for Digital Asset Systems*, Finance and Economics Discussion Series, Washington: Board of Governors of the Federal Reserve System, 59 (2023).

22 See N. Pocher, A. Veneris, *Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme*, cit.. The principle of privacy-by-design falls within the broader scope of regulation-by-design, constituting a specific application of the latter to the protection of personal data. Regulation-by-design is an approach that aims to incorporate regulatory requirements directly into the technical design of systems, creating tools that are inherently compliant with the rules. This approach evolved from Lessing's concept of "code is law", according to which behaviour in cyberspace must be controlled by software code. See L. Lessig, Code v. 2.0. (2006). The principle of privacy-by-design is a cornerstone of data protection: it was already highlighted in a UN recommendation (Report of the Secretary-General, UN doc. A/74/821) and has also been adopted in the GDPR (Art. 25 and Recital 78).

23 K. Rommetveit *et al.*, *Data Protection by Design: Promises and Perils in Crossing the Rubicon Between Law and Engineering*, Privacy and Identity Management: The Smart Revolution, 526 (2018), at 32.

regarding the level of privacy to be afforded to users and the degree of access to their data permitted to public and private actors[24].

The tension between public control and the protection of fundamental rights becomes even more pronounced in the international context, particularly insofar as CBDCs may be used to facilitate cross-border payments[25]. In such scenarios, the issuing central bank could potentially obtain access to the personal data of individuals residing in other jurisdictions. The establishment of common standards regarding privacy and data governance in relation to CBDCs therefore becomes, as already noted, essential to prevent regulatory asymmetries.

These theoretical considerations form the necessary starting point for the analysis of the regulatory and technical solutions adopted in the principal reference models, particularly when examined in light of their specific institutional, social, and cultural contexts.

## III. Privacy Protection in the European Union: An overview

The European Union's longstanding commitment to balancing technological innovation with the protection of fundamental rights and European values constitutes a cornerstone of its digital strategy[26]. In fact, in its process of digital transformation, the EU pursues a model that may be defined as human-centric, aimed at reconciling technological innovation with the safeguarding of fundamental rights. This is reflected in the EU's intention to build an inclusive digital ecosystem, where citizens and businesses can operate and thrive under fair conditions. According to this vision, digital infrastructure must remain an open and democratic space, where technologies serve society as tools at its disposal[27].

Moreover, as digitalisation progressively permeates all societal spheres, the protection of personal data has, over the years, assumed an increasingly central role.

The European journey in the field of privacy began with Directive 95/46/EC[28], which for the first time provided a harmonised framework for the protection of personal data within the EU. Although significant, this regulatory framework was based on a minimum harmonisation model, leaving Member States a wide margin of discretion in its implementation.

---

[24] BIS and other Central Banks, *Central Bank Digital Currencies: Legal aspects of retail CBDCs*, cit., at 19; R. Mahari, T. Hardjono, A. Pentland, *AML by Design: Designing a Central Bank Digital Currency to Stifle Money Laundering*, MIT Science Policy Review, 3 (2023), at 58.; C. Westermeier, *The digital euro: a materialization of (in)security*, Review of International Political Economy 31 (V, 2024), p. 1575.

[25] C.-Y. Tsang *et al.*, *Disciplining CBDCs: Achieving the Balance Between Privacy Protection and Central Bank Independence*, cit., at 245.

[26] A. Adinolfi *et al.*, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, Quaderni AISDUE-Sezione Atti convegni AISDUE, 15 (2023), at 322-323; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Shaping Europe's Digital Future' COM(2020) 67 final.

[27] M. Niestadt, *The global reach of the EU's approach to digital transformation*, European Parliament - Briefing (2024).

[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

Subsequently, the Charter of Fundamental Rights of the European Union (CFREU)[29] expressly recognised, in Articles 7 and 8, the right to respect for private and family life and the right to the protection of personal data as autonomous fundamental rights, affirming principles that are binding both on European institutions and on Member States when implementing European law.

This normative evolution culminated in the adoption of Regulation (EU) 2016/679 (the General Data Protection Regulation, GDPR)[30], which marked a paradigm shift by introducing a uniform discipline directly applicable in all Member States. The GDPR strengthened the protection of personal data, placing emphasis on the principles of data minimisation, transparency, accountability, and privacy-by-design, imposing stringent obligations on both private entities and public authorities.

Although the European Union places strong emphasis on the protection of privacy, this right must, in any case, be balanced against the legitimate need to safeguard national security[31]. This delicate equilibrium between two potentially conflicting interests has been the subject of significant development in the case law of the Court of Justice of the European Union (CJEU). The Court has repeatedly affirmed that, while the rights enshrined in Articles 7 and 8 of the Charter are not absolute, any limitation must be provided for by law, respect the principle of proportionality, and pursue objectives of general interest or the protection of the rights and freedoms of others, in accordance with Article 52(1) CFREU[32].

In light of this regulatory and jurisprudential evolution, the protection of personal data now emerges not only as an individual right but also as a distinctive feature of the European model in the global context. These principles also underpin the approach adopted by the EU in the design of the digital euro[33], which is currently at the centre of a legislative process initiated with the proposal for a regulation presented by the European Commission on 28 June 2023[34] (hereinafter, the "Proposal").

---

[29] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.

[31] L. Borlini, *Tutela della privacy e protezione dei dati personali a fronte della sicurezza pubblica e dell'integrità del Sistema finanziario europeo*, Diritti Umani e Diritto Internazionale, 11 (I, 2017), at 24.

[32] See *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (Case C-623/17, CJEU, 6 October 2020); *Tele2 Sverige AB v Post-och telestyrelsen* (Joined Cases C-203/15 and C-698/15, CJEU, 21 December 2016) concerning the balancing of the right to data protection with national security interests; see also *Digital Rights Ireland and Others* (Joined Cases C-293/12 and C-594/12, CJEU, 8 April 2014) where the Court rendered Directive 2006/24/EC on data retention invalid.

[33] In line with the objective of creating a digital euro consistent with the democratic principles of the Union, the EDPB has highlighted the need to carry out a holistic assessment of the fundamental interests and rights involved – such as financial and digital inclusion, privacy protection, freedom of movement and security – to ensure that the design of the new digital currency is fully compliant with the founding values of the European legal system. See: EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro (2021).

[34] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, COM(2023) 369 final.

## IV. The Proposed Regulation on the Digital Euro

The digital euro – still in the design phase – arises from the need to address the progressive digitalization of payment methods[35], strengthen the financial stability of the Eurozone, reduce dependence on private operators[36], and reaffirm the EU monetary sovereignty[37]. It will adopt a two-tier model, likely based on an intermediated architecture[38], whereby the European Central Bank (ECB) will directly issue the digital currency, while payment service providers (PSPs) will manage relationships with end users, providing wallets and payment services. The digital euro will not be programmable[39].

The digital euro aims to become an alternative (not substitutive) payment instrument to those already in existence, offering citizens a safe, accessible solution with a particular focus on the protection of privacy in digital payment transactions[40].

The importance given to this latter aspect is also reflected in the results of the public consultation conducted by the ECB[41], which revealed that 43% of participants – including citizens, businesses, and professionals – identified privacy as the main desired feature in the design of the digital euro. These concerns have been acknowledged by the ECB itself, which, from the beginning of the exploratory phase, emphasized that one of its core objectives is to identify design solutions capable of ensuring a high level of personal data protection and preventing potential risks for citizens, intermediaries, and the economy as a whole[42].

Consistently, the Proposal places data protection among the guiding principles of the initiative, explicitly referencing Article 8 CFREU of the European Union, the GDPR, and Regulation (EU) 2018/1725. In light of this, from the design phase onwards[43], the ECB and PSPs will be required to prioritize configurations that minimize the collection of personal data. These obligations have been formalized in Articles 34 and 35 of the Proposal.

In particular, the Proposal introduces specific obligations for PSPs to ensure that the processing of users' personal data fully complies with the principles of data minimization

---

35 F. Panetta, *Il costo di non emettere un euro digitale*, CEPR-BCE Conference (2023).

36 V. Lubello, *Central Bank Digital Currencies and the Digital euro: A Comparative Prism Between Sovereignty and Technology*. Itinerari della Comparazione, Scritti in onore di Giuseppe Franco Ferrari, 1 (2023), at 2.

37 P. Cipollone, Monetary sovereignty in the digital age: the case for a digital euro (2024), speech available at https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240927~11ed8493a4.en.html (last visited Jul 24, 2025).

38 In which the ECB will not have access to the register of all transactions. I. E. Linaritis, *Governance Issues Concerning the Issuer of CBDC, Who Supervises and Controls the CBDC Scheme?,* in Central Bank Digital Currency: The Birth of the Digital Euro (2025), at 196.

39 Programmability refers to the ability to embed conditions or restrictions directly into the digital currency itself, such as limiting its use to certain goods or services, defining a time period for its use, or specifying eligible recipients. This implies that the digital euro will not contain embedded features allowing public authorities to restrict its use for predefined purposes. There will be no technical mechanisms enabling the European Central Bank or governmental bodies to control how, when, where, or with whom digital euros can be spent. See FAQ on the digital euro, available at https://finance.ec.europa.eu/digital-finance/digital-euro/frequently-asked-questions-digital-euro-and-legal-tender-cash_en (last visited Jul 24, 2025).

40 F. Panetta, *Il costo di non emettere un euro digitale*, cit., at 9.

41 ECB, *Public consultation on a digital euro*, which was launched on 12 October 2020 and ran until 12 January 2021.

42 ECB, *Report on a Digital Euro* (2020).

43 In line with the principle of privacy-by-design codified at EU level by Art. 25 GDPR.

and purpose limitation[44], ensuring that the information processed is limited to the public interest purposes expressly set out in Article 34[45]. PSPs will need to adopt appropriate technical and organizational measures to ensure that the data processed are relevant and limited to what is necessary for the provision of payment services and for fulfilling regulatory obligations. PSPs are also responsible for adopting adequate technical and organizational measures to ensure that the data transmitted to the ECB and National Central Banks (NCBs) do not allow the direct identification of individual users[46].

Particularly stringent restrictions on access to personal data are imposed on the ECB and NCBs. Article 35 of the Proposal clarifies that the ECB and NCBs may only process data necessary to ensure the integrity, resilience, security, and operational continuity of the digital euro infrastructure, as well as to prevent fraud and cybersecurity incidents. In this context, processing must be carried out using pseudonymization techniques, encryption mechanisms, and separation of identifying information, in order to prevent the ECB and NCBs from being able to identify individual users[47].

Despite this regulatory framework, concerns have been raised in the literature about the risk that the proposed structure could still leave residual spaces for potential privacy violations, particularly by public authorities[48]. However, the CJUE, as mentioned, has already established the need to impose strict limits on government access to personal data, ruling that such access may occur exclusively for crime prevention purposes, subject to judicial authorization or independent review, and provided that the data are stored within the EU and permanently deleted at the end of the retention period[49]. It is reasonable to think that these limits may, in the future, also be applied to the digital euro.

Concerns similar to those raised in the literature have also been expressed by independent authorities, particularly the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), which, in their joint opinion of 2023, highlighted the risk that the creation of the single access point[50] provided for in Article 35(8) could lead to an excessive concentration of sensitive data, potentially enabling the identification of users by parties other than PSPs, in violation of the principles of data minimization and proportionality[51].

---

44 Recital 72.

45 Art. 34 (1) Proposal. On this point, the question arises as to whether the list is considered exhaustive or illustrative. See A. C. Penedo *et al.*, *Untangling Digital Euro's Personal Data Protection Challenges, An Exploration of Data Processing Activities and Latent Privacy Risk*, cit., at 13.

46 Art. 34(4) Proposal.

47 Art. 35(4) Proposal.

48 G. Soana, T. de Arruda, *Central Bank Digital Currencies and financial integrity: finding a new trade-off between privacy and traceability within a changing financial architecture*, J. Bank Regul., 25 (2024), at 482-483; A. C. Penedo *et al.*, *Untangling Digital Euro's Personal Data Protection Challenges, An Exploration of Data Processing Activities and Latent Privacy Risk*, cit., at 16.

49 Joined Cases C-203/2015 and C-698/2015 (parr. 100 ff.; 120 ff.).

50 The single access point is a centralised technical infrastructure that allows PSPs to verify compliance with individual limits on the holding of digital euros by users. This system provides only aggregate responses (e.g. whether a given payment can be accepted without exceeding the limits) without allowing direct identification of users by parties other than the relevant payment service provider. The management of this infrastructure is entrusted to the ECB, possibly in conjunction with NCB, which are the controllers or joint controllers of the related personal data. See Recital 25 and Article 35(8) Proposal.

51 EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro (2023).

Consistently with the aim of maximizing privacy protection in the digital euro, the EDPB has also proposed[52] that the digital euro should replicate the features of cash, particularly in terms of privacy protection, adopting a threshold-based approach with proportional levels of anonymity depending on usage.

Coherently, the Proposal introduces the possibility of making offline payments in digital euros through hardware devices that do not require an internet connection: such transactions – largely assimilated to the use of cash or, more precisely, to ATM withdrawals[53] – are designed to offer a high level of privacy, ensured through data pseudonymization and the impossibility for the ECB, NCBs, and PSPs to access transaction details[54]. In this scenario, PSPs may only process data relating to the funding and defunding of accounts, but not data concerning peer-to-peer transfers[55].

For online payments, the Proposal provides for the application of the general principles on data protection and security, particularly the rules on anti-money laundering and counter-terrorist financing (AML/CFT). Online transactions will therefore be traceable in a manner similar to existing digital payment methods, and PSPs will remain subject to the reporting obligations under anti-money laundering regulations.

On this point, however, the joint opinion of the EDPB and EDPS expressed a significant reservation[56]. The two authorities regretted the European legislator's decision to exclude the adoption of a "selective privacy" regime even for low-value online payments. According to the supervisory bodies, the AML/CFT risk level for the online digital euro will largely depend on the technological and design choices made during the development phase. In this context, the introduction of risk mitigation measures could make it possible to extend the enhanced privacy regime provided for offline transactions also to low-value online payments. For this reason, the EDPB and EDPS strongly recommend that co-legislators consider introducing a threshold below which online transactions would not be subject to AML/CFT traceability, thereby ensuring a higher level of privacy aligned with user expectations.

The multi-layered architecture outlined by the Proposal thus appears to build an advanced balance between privacy protection and the security and transparency requirements of the payment system, even if some critical issues remain: beyond those already mentioned, the complexity of the proposed system – with the coexistence of different levels of data access and the need to ensure interoperability between public and private entities – could result in practical uncertainties and accountability risks[57].

In any case, the provisions appear consistent with the European approach to personal data protection and respond to the need to preserve user trust, which, as noted, is considered an essential condition for the widespread adoption of the digital euro.

---

52 EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro, cit..

53 Recital 71 Proposal.

54 Recital 71, Recital 82, articles 34 and 37.

55 Art. 37 Proposal

56 EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, cit..

57 A. C. Penedo *et al.*, *Untangling Digital Euro's Personal Data Protection Challenges, An Exploration of Data Processing Activities and Latent Privacy Risk*, cit., at 10.

Moreover, the extended timeline for the approval of the digital euro Regulation, combined with the careful analysis of privacy-related risks, is consistent with the prudential approach of the European legislator, traditionally committed to seeking regulatory solutions capable of effectively balancing personal data protection with the needs of financial system stability and security.

## V. THE PEOPLE'S REPUBLIC OF CHINA APPROACH TO PRIVACY

The Chinese legal culture has always placed particular attention on notions such as public interest, national security, and social stability, values that are often considered to take precedence over individual rights[58]. This longstanding emphasis on these values has traditionally left limited room for the recognition of personal privacy as a legally protected right[59].

Starting from the 1980s, with the reforms promoted by Deng Xiaoping, the People's Republic of China (PRC) has witnessed a re-evaluation of the concept of privacy[60].

The evolution towards a market-oriented society and the growing legal transplantation of Western values[61] have indeed led to significant changes in the social perception of individual rights. The advent of new technologies has further encouraged the emergence of the individual as an autonomous subject with personal interests, while cultural opening has made discussions on issues such as personal freedom and individual rights, including the right to privacy, increasingly legitimate[62].

However, despite this evident cultural evolution and the enhancement of the legal protection of personal privacy compared to the past[63], scholars have highlighted that the Chinese approach to privacy continues to maintain a radical distinction from Western

---

[58] A. Gambaro, R. Sacco, M. Graziadei, Sistemi giuridici comparati, cit., at 362; G. Ajani, A. Serafino, M. Timoteo, Diritto dell'Asia orientale (2007), at 53.

[59] See S. Peng, *Privacy and the Construction of Legal Meaning in Taiwan*, International Lawyer, 37 (IV, 2003), at 1039. H. Wang, *The conceptual basis of privacy standards in China and its implications for the China's privacy law*, Frontiers of law in China, 7 (2012), at. 137.

[60] H. Wang, *The conceptual basis of privacy standards in China and its implications for the China's privacy law*, cit., at 140-141; L. Yao-Huai, *Privacy and data privacy issues in contemporary China*, Ethics and Information Technology, 7 (2005), at 9. It should be noted that the traditional Chinese word for privacy, 阴私, historically carried a negative connotation, often referring to shameful or immoral secrets, and therefore was not adopted into legal discourse (see M. Xu [ 徐明], *Privacy Crises in the Big Data Era and Responses under Tort Law*, [大数据时代的隐私危机及其侵权法应对], China Law [中国法学] 1 (2017)). The word that translates the western concept of privacy is 隐私 (see G. Zhu, *The Right to Privacy: An Emerging Right in Chinese Law*, Statute Law Review, 18 (III, 1997), at. 208).

[61] A. Gambaro, R. Sacco, M. Graziadei, Sistemi giuridici comparati, cit., at 373-374; G. Ajani, A. Serafino, M. Timoteo, Diritto dell'Asia orientale, cit., at 306 ff.

[62] Lu Yao-Huai, *Privacy and data privacy issues in contemporary China*, cit., at 11.

[63] Already in 1982, the Chinese Constitution recognized certain privacy-related rights, such as personal dignity (art. 38), personal freedom and residence (arts. 37 and 39), and the confidentiality of correspondence (art. 40). Article 101 of the 1986 General Principles of Civil Law established the right to reputation for individuals and legal entities, prohibiting insults, defamation, and other acts that harm personal dignity. In 1988 the Supreme People's Court issued a legal interpretation clarifying that publicly disclosing someone's private information constitutes a violation of their right to reputation and may give rise to civil liability (法 [办] 发 [1988]6 号《最高人民法院关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见（试行）》).

models: in the Chinese perspective, the protection of privacy remains strongly anchored to the centrality of collective interests and public order[64].

Not even the adoption of dedicated legislation on personal data protection, namely the *Personal Information Protection Law* (PIPL)[65], nor the inclusion of privacy within the personality rights of the Chinese Civil Code[66], seem to have altered this trend. On the contrary, it has been observed that the introduction of privacy regulations in the PRC takes on a strongly public dimension[67]. In fact, the widespread public discontent arising from personal data breaches has pushed the regulator to officially recognize privacy invasions as potential sources of social instability[68].

Additionally, the strategy adopted by the regulator has not resulted in a limitation of public surveillance but rather in a reinforcement of its role as the citizens' protector against abuses perpetrated by third parties. The legislative action has allowed the leadership to present itself as the primary defender of privacy, without however questioning the prerogatives of state control[69]. In this narrative, privacy violators are never identified as the authorities themselves but rather as external actors such as greedy companies or fraudsters[70]. This framework seems to reflect a recurring pattern in Chinese governance, characterized by a notable asymmetry between the stringent restrictions placed on private actors and the wide discretionary powers afforded to public authorities[71].

In this context the development of the e-CNY takes place. The digital yuan not only represents a technological advancement in the payment system but also constitutes an instrument through which multiple objectives are pursued: from promoting innovation and economic efficiency to ensuring more effective supervision of financial transactions, as well as advancing the internationalization of the RMB. The e-CNY thus stands at the crossroads of digitalization, security needs, and privacy protection objectives, according to an approach that reflects the distinctive features of the Chinese system.

---

64 Lu Yao-Huai, *Privacy and data privacy issues in contemporary China*, cit., at 11.

65 Personal Information Protection Law [中华人民共和国个人信息保护法], promulgated by the Standing Committee of the 13th National People's Congress on August 20, 2021, effective November 1, 2021.

66 Book 4, Personality Rights, Chinese Civil Code [中华人民共和国民法典], promulgated by the 13th National People's Congress on May 28, 2020, effective January 1, 2021.

67 M. Jia, *Authoritarian Privacy*, University of Chicago Law Review, 91 (2024).

68 This is mentioned, for example, in the "*Notice Relating to Performing Good Work During New Year's Day and the 2021 Spring Festival*" issued by the General Office of the Chinese Communist Party Central Committee and the State Council General Office (中共中央办公 厅 国务院办公厅印发《关于做好 2021 年元旦春节期间有关工作的通知》).

69 E. Toti, *Dalla Decisione per il rafforzamento della protezione delle informazioni su internet alla Legge sulla tutela delle informazioni personali della RPC "con caratteristiche cinesi"*, Rivista di Diritto dei Media (I, 2023), at 212.

70 Mark Jia, *Authoritarian Privacy*, cit., at 737; this perspective appears to align with the Chinese approach to the rule of law "with Chinese characteristics", a model in which law is subordinated to the leadership of the Communist Party and serves primarily as an instrument for achieving policy goals. For a more in-depth discussion on this topic, see: G. Ajani, *La Rule of Law in Cina*, Mondo Cinese, 126 (2006); I. Castellucci, Rule of Law and Legal Complexity in the People's Republic of China (2012).

71 R. Cavalieri, *La legalità socialista di Xi Jinping*, Tra storia e politica. L'Asia orientale contemporanea e il contributo di Enrica Collotti Pischel (2024), at 107.

## VI. THE DIGITAL YUAN

Although Chinese authorities have been focusing on the topic of CBDCs for over a decade[72], there is currently no specific regulation concerning the digital yuan in the PRC, nor concerning privacy protection in this field[73]. Furthermore, no case law on the matter has been recorded. Therefore, the legal analysis must rely on non-binding rules and on the existing legal framework for personal data protection as provided in the Civil Code and the PIPL.

From an operational standpoint, as outlined in the White Paper issued by the People's Bank of China (PBOC) in 2021[74], the e-CNY is based on a two-tier system in which the PBOC retains control over the issuance and central management of the currency, while distribution and interaction with end users are entrusted to private entities, such as commercial banks and authorized payment platforms. Unlike the digital euro, the PBOC also maintains the ledger of all transactions carried out in e-CNY, making it a hybrid model where the operational management is delegated to intermediaries, but the control over the transaction flows remains centralized with the monetary authority[75].

The digital yuan is programmable, and the system's architecture is inspired by the principle of "managed anonymity", according to which low-value transactions have a higher degree of anonymity, while high-value transactions are fully traceable[76]. The e-CNY is stored in different types of wallets, each offering varying levels of anonymity and spending limits. Wallets are classified based on the degree of identification required: those with less stringent requirements allow low-value payments (up to a maximum of 2,000 CNY per transaction) and can be accessed with just a phone number registration[77].

At first glance, this structure – similar to that of the EU, as it consists of a hybrid model between account-based and quasi-account-based systems [78] – presents, however, significant differences in terms of privacy: low-value transactions, which are comparable to offline payments in the digital euro project, do not offer the same levels of anonymity, since the Chinese wallet is always mandatorily linked, as mentioned, to a phone number

---

[72] The first studies on the creation of a national CBDC date back to 2014. Attention turned more to the issue in 2019, as a way of countering crypto-assets and stablecoins, which had already been banned since 2017 and then expanded. See PBOC, *Progress of Research & Development of E-CNY in China*, Working Group on E-CNY Research and Development of the People's Bank of China (2021), at 1.

[73] Despite this, scholars have repeatedly highlighted the need for clear and comprehensive regulations in this area, and the same point was made by the authorities in the white paper. See: Y. Chen, M. Adams, *The Regulation of Digital Currency in China: Past, Present, and Future*, European Journal of Law Reform, 25 (I-II, 2023), at 159; PBOC, *Progress of Research & Development of E-CNY in China*, cit., at 11.

[74] PBOC, *Progress of Research & Development of E-CNY in China*, cit..

[75] This means that the central bank can keep a copy of retail balances and transactions, giving the PBOC full, centralised access to detailed data on each user's accounts and transactions, regardless of the intermediary used. See: J. Jiang, *supra*, at 117.

[76] PBOC, *Progress of Research & Development of E-CNY in China*, cit., at 7.

[77] See Guangzhou Huadu District Financial Work Bureau [广州市花都区金融工作局], Mu Changchun of the Central Bank explains the four types of digital RMB wallets in detail, [央行穆长春详解四类数字人民币钱包] (2021).

[78] Z. Li, J. Li, 2025. *Evaluating the Wallet-Based DCEP: Regulatory Innovations and Implementation Strategies in China's Retail CBDC*, Laws 14 (III, 2025), at 4. It should be noted that high levels of anonymity are provided by the so-called value-based category, which are hardware devices that contain digital yuan without being linked to a bank account (examples include prepaid cards or transport cards).

which, in turn, is tied to an identity card[79]. Even though the European model also requires some form of identification, strict limits are imposed on the use of data related to these transactions[80]. The absence of similar provisions in the Chinese context increases the risk that even low-value operations may be subject to systematic tracking and profiling.

Reflections on this CBDC model, when read in light of the privacy-by-design principle, make the e-CNY a paradigmatic example of how the technical infrastructure of a digital currency can itself serve as a policy tool, translating political goals into operational solutions through the CBDC's design[81]. Unlike the European project, where the Proposal explicitly imposes limitations on data access by the ECB, NCBs, and PSPs – constraints that must necessarily be embedded in the technical infrastructure through specific engineering solutions – the absence of equivalent legal safeguards in the PRC[82] raises the risk that the e-CNY infrastructure may allow for unlimited processing of users' financial information, with clear concerns in terms of privacy protection and transparency[83].

Even the existing personal data protection framework does not seem adequate to protect users from potential abuses for two main reasons: *(i)* firstly, because *ex post* regulation does not provide the same level of protection as that which is embedded directly within the technical infrastructure; *(ii)* secondly, because the Chinese privacy framework contains room for interpretation that could, in practice, significantly broaden the authorities' powers to access personal data.

Regarding the first point, it has been observed that existing privacy laws offer protective measures that operate downstream and are thus secondary, whereas embedding personal data protection directly into the infrastructure is more effective than sanction-based, *ex post* interventions[84].

---

[79] Y. Chen, M. Adams, *The Regulation of Digital Currency in China: Past, Present, and Future*, cit., at 156; article 24 Cybersecurity Law (中华人民共和国网络安全法).

[80] As discussed in section IV, PSPs will only be able to process essential information related to the funding and defunding of funds, without being able to access data relating to transactions between users. Furthermore, pursuant to recital 71 and Article 37(2), neither the ECB nor the national central banks may attribute the data to an identified or identifiable user of the digital euro. A partial exception in this regard is provided for in Article 37(3), which requires PSPs to make user data available in cases of suspected money laundering or terrorist financing.

[81] C. Xu, B. Jin, *Digital currency in China: pilot implementations, legal challenges and prospects*, Juridical Tribune 12, (II, 2022), p. 185.

[82] Article 51 PIPL, which can be regarded as the provision closest to a codification of the privacy-by-design principle within the Chinese legal framework, nonetheless differs from Article 25 GDPR insofar as it does not establish such an approach as a general design principle, but rather as a set of operational obligations aimed at ensuring the security of processing. Partially complementing Article 51 is the Information Security Technology – Personal Information Security Specification (信息安全技术个人信息安全规范), which appear, in Article 11.2, to set out an *ex ante* requirement for the development of systems that ensure privacy protection. However, this document is non-binding in nature.

[83] C. Lopez, *Digital Currency: A Global Regulatory Framework is Needed*, cit., at 185-186.

[84] J. Jiang, *Privacy Implications of Central Bank Digital Currencies*, cit., at 130.

As for the second point, it seems that the general personal data protection framework formally applies to the e-CNY as well[85]. This framework is characterized by a "dual" structure, as it is divided between the Civil Code and the PIPL[86].

Both sources seem to recognize that financial information falls within the category of protected personal data[87]: therefore, transactions conducted through e-CNY would also appear to fall within this category. Since this information qualifies as personal data, it should, at least in principle, be protected against potential misuse, both by private entities and by public authorities. The Chinese legal framework, indeed, seems to place public and private actors on the same level, following what has been defined as a unitary legislative model[88]; however, the legislation includes broad exceptions aimed at safeguarding public interests.

In this context, all data controllers – whether authorities[89] or commercial banks – are, at least in theory, required to comply with the provisions of the PIPL, which imposes strict limits on the collection, use, and storage of users' data, and requires the implementation of appropriate technical and organizational measures to ensure the security and confidentiality of the processed information[90]. In particular, the law requires that personal data be processed lawfully, fairly[91], and when necessary, following the principles of minimization and specific purpose limitation[92].

However, as mentioned, Chinese regulation – consistently with the traditional approach to privacy outlined above – recognizes significant exceptions to these general principles

---

85 X. Chen, *Privacy Protection in the Context of CBDC: Development Trends and China's Practice*, J. East Asia & int'l l., 16 (II, 2023); J. Jiang, L. Lucero, *Background and implications of China's e-CNY*. University of Florida Journal of Law and Public Policy, 33 (II, 2023), at 265.; C. Mu, *Theories and practice of exploring China's e-CNY, Data, Digitalization, Decentralized Finance and Central Bank Digital Currencies: The Future of Banking and Money*, cit., at 185.

86 D. Clementi, *La legge cinese sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?*, Rivista di Diritti Comparati (2022). As highlighted by the author, the Civil Code and the PIPL protect, respectively, the autonomous rights to privacy and personal information: the former is seen as a "negative" right to prohibit intrusion into private life; the latter is seen as a positive right, which values the right to control who uses one's personal information. For a general overview of the PIPL, see B. Verri, *The Chinese Frontiers of Data Protection: The Personal Information Protection Law (PIPL)*, in M. Timoteo, B. Verri, R. Nanni (eds.), Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China (2023).

87 The financial data would in fact fall within the scope of Article 1034 of the Civil Code and the combined provisions of Articles 4 and 28 PIPL.

88 Y. Wang [王怡坤], *A Research on the Legitimacy Standard of Personal Information Processing Behaviors by State Organs* [国家机关个人信息处理行为正当性标准研究], China L. Rev. [中国法律评论] 42 (VI, 2021).

89 Art. 33 PIPL.

90 However, Chinese scholars have raised some concerns about the effective protection of personal data by the banking institutions involved in managing e-CNY wallets. In particular, it has been noted that when downloading the digital yuan app, users are required to accept the specific privacy policies set by individual commercial banks, without which the wallet cannot be opened. However, these policies vary significantly between different banks and, in some cases, require users to provide personal data that appears to exceed the minimum requirements of current legislation. See: W. Wang [王炜炫], *Personal Information Protection in the Issuance and Circulation of Digital RMB* [数字人民币发行和流通中的个人信息保护], Southern Finance [南方金融], 562 (2023). This critical issue does not contradict the fact that banks are subject to stringent obligations regarding the protection of personal data. On the contrary, it highlights a possible disconnect between the formal regulatory framework and its application in practice, which requires legislative intervention to standardise the conditions for opening wallets.

91 Art. 5 PIPL.

92 Art. 6 PIPL.

when necessary to protect public interests. Article 1036 of the Chinese Civil Code provides for an exemption from civil liability when personal data is processed for the protection of the public interest.

Consistently, Article 13 of the PIPL allows the processing of personal data without the data subject's consent when such processing is necessary for the exercise of public functions, for purposes of public interest, for the protection of health, for journalistic activities, or for public opinion supervision.

Although such exceptions seem to be justified, particularly from the perspective of Chinese scholars[93], by the need to combat crimes that may jeopardize social stability, the vagueness and ambiguity of the terminology used in the legislation – especially references to generic concepts such as the public interest or public opinion supervision – risk creating significant areas of legal uncertainty, resulting in a substantial erosion of privacy guarantees[94].

This legal uncertainty appears, in fact, to be a recurring feature of the Chinese legal system[95], which inevitably leads to a certain degree of flexibility in interpretation and application of law on a case-by-case basis. Such vagueness becomes particularly problematic in the context of the digital yuan, where financial data can notoriously reveal with great accuracy spending habits, individual preferences, and deeply personal aspects of a person's identity.

In light of these considerations, the legal and technical architecture of the e-CNY seems to confirm the existence of a governance model that is strongly focused on the protection of public interest and the safeguarding of social stability, where privacy protection, although formally acknowledged, appears structurally subordinated to widespread control needs. The absence of specific regulation for the digital yuan and of strict legal safeguards limiting public authorities' access to data, combined with the broad exceptions provided in the general data protection framework, ultimately may contribute to an imbalanced system in which end users have limited avenues to challenge potential misuse of their data.

In this sense, the digital yuan seems to be a clear example of a governance model of CBDC "with Chinese characteristics" (中国特色), reflecting a balance between privacy and public interest that is profoundly different from the one emerging in the European context.

Against this backdrop, future research should closely monitor how the Chinese legal system will concretely operationalize its data protection principles in the context of the digital yuan, particularly in relation to the role of courts in addressing potential rights violations.

## VII. The Brussels Effect and the Beijing Effect in the field of CBDCs

This paper has examined the divergent governance and design models of CBDCs through a comparative lens, highlighting the emergence of distinct regulatory paradigms: these

93 X Chen, *Privacy Protection in the Context of CBDC: Development Trends and China's Practice*, cit., at 229.
94 J. Jiang, L. Lucero, *Background and implications of China's e-CNY*, cit., at 267.
95 D. Cao, Chinese Law: A Language Perspective (2004), at 94 ff.; P. B. Potter, The Chinese Legal System: Globalization and Local Legal Culture (2001), at 11; E. Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, Penn. St. J.L. & Int'l Aff., 8 (2020), at 74; B. Verri, *The Chinese Frontiers of Data Protection: The Personal Information Protection Law (PIPL)*, cit., at 195.

models could also be replicated in other jurisdictions, given the need, as mentioned, to create common standards for cross-border payments.

The absence of a consolidated global regulatory model for CBDCs offers the European Union a valuable opportunity to establish itself as a leader in the definition of such standards[96], potentially influencing the regulatory choices of other jurisdictions. The European Union, already a key player in the global standard-setting process through the phenomenon known as the Brussels Effect[97], is well positioned to extend its influence on the field of CBDCs as well[98]. In this sense, the adherence of third countries to European standards may become a necessary condition for achieving the interoperability objectives mentioned above, especially where these countries wish to ensure compatibility between their CBDC systems and the European one.

The EU regulatory influence in this context could be exercised for two principal reasons: *(i)* firstly, because it satisfies the conditions identified by Anu Bradford for the emergence of the Brussels Effect, combining a large consumer market with a high regulatory capacity and a strong political will to impose stringent rules. Moreover, the CBDC domain targets relatively inelastic users (such as citizens and businesses) and relies on technological infrastructures that cannot be easily segmented across jurisdictions, given the need for a common framework to ensure interoperability between different CBDCs; *(ii)* secondly, due to the central role that privacy protection plays in the perception and acceptance of CBDCs by both citizens and businesses. Indeed, the demand for digital payment instruments is increasingly shaped by users' sensitivity to the processing of personal data, and it is reasonable to expect that citizens and businesses will prefer to use CBDCs – rather than alternative digital payments – only where such instruments effectively safeguard their privacy[99].

Finally, it should be noted that, in the context of CBDCs, the need to apply uniform standards does not concern PSPs alone but also central banks and public authorities more broadly. In this regard, a mere *de facto* adaptation by PSPs located outside the EU to European standards would not be sufficient to ensure genuine regulatory convergence. Only through a formal harmonization of domestic legal frameworks in line with European principles (*de jure* alignment) can full legal interoperability between CBDC systems be guaranteed.

Unlike the European Union, whose potential influence in the CBDC domain could materialize through regulatory projection based on the Brussels Effect, the international influence of the PRC may develop according to profoundly different logics.

---

[96] C. Lopez, *Digital Currency: A Global Regulatory Framework is Needed*, cit., at 187 emphasises the importance of creating a global regulatory framework.

[97] A. Bradford, The Brussels Effect: How the European Union Rules the World, cit..

[98] F. Panetta, *The present and future of money in the digital age*, ECB (2021), available at: https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211210~09b6887f8b.en.html (last visited Jul 24, 2025).

[99] F. Tronnier, W. Qiu, *How do privacy concerns impact actual adoption of central bank digital currency? An investigation using the e-CNY in China*, Quantitative Finance and Economics, 8 (I, 2024); S. Choi *et al.*, *Central Bank Digital Currency and Privacy: A Randomized Survey Experiment*, BIS Working Papers (2023); F. Tronnier *et al.*, *Investigating privacy concerns and trust in the digital Euro in Germany*, Electronic Commerce Research and Applications, 53 (2022).

It is worth noting that although China was long considered a rule-taker, generally inclined to adopt external norms[100], this approach has shifted in recent decades. China has gradually moved away from the role of mere recipient of standards developed by other jurisdictions to become an active rule-maker, particularly in emerging technological sectors[101].

This shift has been particularly evident since 2013, with the launch of the Belt and Road Initiative (BRI)[102], which therefore constitutes a unique standpoint for analysing China's international projection strategies. The BRI, introduced under Xi Jinping's presidency, is a global strategy aimed at building infrastructure and promoting a new China-centered model of globalization. Through massive investments in Eurasia and other strategic regions, China seeks to consolidate its sphere of influence, not only through economic and industrial advantages but also by exporting its own standards, norms, and values[103].

A particularly significant component of this strategy is the Digital Silk Road, the BRI's branch dedicated to investments in information and communication technologies[104]. Through these projects, China is not merely expanding its economic and political presence but is actively promoting the adoption of its technological architectures and imposing the use of Chinese technical standards. This dynamic has produced considerable effects: the diffusion of Chinese technological infrastructures prompts private operators and third countries to adopt compatible standards to ensure system interoperability[105], thereby consolidating PRC influence in the digital sphere and reinforcing the global penetration of Chinese standards.

In addition to this mechanism of exporting technological standards, PRC also exerts an attractive influence through its model of data sovereignty, which is characterized by strong centralization and the clear subordination of private operators to public objectives[106].

This model of influence has been described in scholarly literature as the Beijing Effect, in contrast to the aforementioned Brussels Effect[107]. Unlike the latter, which is based on the normative influence of European rules, PRC influence is not expressed through the direct projection of legal norms[108] but rather – as noted – through the export of a data

[100] China's transplantation of legal models has not occurred through a mere transposition of foreign legal frameworks in its legal system, but rather through a selective adaptation of external legal standards to its own socio-cultural and political context. See P. B. Potter, The Chinese Legal System: Globalization and Local Legal Culture, cit., at 4; D. Zoppolato, P. D. Farah, *China's Path to Modernization and Legal Pluralism: Transplants and the Belt and Road Initiative*, Asian Journal of Law and Society (2025), at 3 ff.

[101] R. Cavalieri, *La legalità socialista di Xi Jinping*, cit., at 107; H. Wang, *Selective Reshaping: China's Paradigm Shift in International Economic Governance*, Journal of International Economic Law, 23 (2020), at 584.

[102] *Id*., at 584; D. Zoppolato, P. D. Farah, *China's Path to Modernization and Legal Pluralism: Transplants and the Belt and Road Initiative*, cit., at 2.

[103] M. Simonov, *The belt and road initiative and partnership for global infrastructures and investment: comparison and current status*, Asia and the Global Economy (2025), at 2

[104] F. Klein, N. Baker, *China and its Central Bank Digital Currency – Is the E-Yuan a Role Model for Europe and the Euro System?*, Friedrich Erbert Stifung (2023), at 6

[105] M. S. Erie, T. Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance,* N.Y.U. J. Int'l L. & Pol., 54 (I, 2021), at 23.

[106] *Id*, at 21.

[107] *Id*, at 17-20.

[108] Indeed, this could hardly be the case: China's regulatory capacity and expertise still face certain limitations, particularly with regard to the extraterritorial application of its laws. See A. Bradford, Digital empires: the global battle to regulate technology (2023), at 328-329. Unlike the European Union, China has never sought to adopt extraterritorial regulations as a means of projecting its influence abroad, in line with its traditional anti-hegemonic stance. Only in recent years has China shown a tendency towards extraterritoriality, with the

governance model and the dissemination of technological standards that gradually become established in international markets[109].

In light of this reconstruction, it cannot be excluded that this model could also extend to the realm of CBDCs. In fact, the inherently technological nature of CBDCs and the need to ensure interoperability between different digital payment systems may represent a particularly favourable channel through which the Beijing Effect could operate.

Given that many BRI countries often lack adequate financial infrastructures, it is likely that they will collaborate with Chinese financial institutions to develop their own CBDCs. In this context, it is plausible that the governments of these countries will rely not only on Chinese technologies but also on Chinese policies concerning CBDCs[110]. Furthermore, it seems reasonable to expect that these countries may gradually emulate the Chinese model of financial data governance, converging towards practices of managed anonymity and traceability of financial flows. In these terms, the Beijing Effect could materialize.

In addition to this perspective, an emerging strand of scholarship has emphasized PRC influence over other jurisdictions by framing it within a broader paradigm of digital authoritarianism, characterized by pervasive surveillance practices, infrastructural control, and restrictions on the autonomy of private actors[111]. According to some authors, the design and governance of CBDCs could serve as a vehicle for the extension of this model to other jurisdictions. Specifically, this doctrine highlights that the regime of managed anonymity reflects an authoritarian conception of privacy, which may have the potential to influence other authoritarian regimes transnationally[112].

The analyses presented here ultimately suggest that, despite the absence of a comprehensive and systematic regulatory framework for the digital yuan that could be replicated as a normative model by other jurisdictions, PRC has nonetheless succeeded in positioning itself as a central actor in the international CBDC discourse. This outcome has been facilitated both by PRC first-mover advantage, gained through the early introduction and advanced experimentation of the e-CNY, and by its active participation in key standard-setting bodies, where it contributes to the development of guiding principles for CBDCs[113].

---

PIPL representing a significant step in this direction. See W. Cong., *The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics*, in M. Jiang, L. Belli (eds.), Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance (2025), at 79.

[109] *Id*, at 23.

[110] C.-Y. Tsang, P.-K. Chen, *Policy Responses to Cross-Border Central Bank Digital Currencies – Assessing the Transborder Effects of Digital Yuan*, Capital Markets Law Journal, 17 (2022), at 250.

[111] A. Polyakova, C. Meserole, *Exporting digital authoritarianism*, Brookings Institute Foreing Policy Reports (2019). On the topic see also: X. Qiang, *Chinese Digital Authoritarianism and Its Global Impact*, in Digital Activism and Authoritarian Adaptation in the Middle East (2021), available at https://pomeps.org/chinese-digital-authoritarianism-and-its-global-impact (last visited Jul 25, 2025); A. Liaropoulos, *Digital Authoritarianism "Made in China": Installing a Digital Dystopia*, National security and the future, 23 (I, 2022); D. Lilkov, *Made in China: Tackling digital authoritarianism*, European View, 19 (I, 2020).

[112] N. Kshetri, *China's Digital Yuan: Motivations of the Chinese Government and Potential Global Effects*, Journal of contemporary China, 32 (2023), at 103.

[113] H. Wang, *Selective Reshaping: China's Paradigm Shift in International Economic Governance*, cit., at 593.

In conclusion, the PRC may exert significant influence in the future, predominantly of a technical and infrastructural nature, in shaping the global CBDC ecosystem, promoting a model that is no longer primarily regulatory, but rather technical and governance-oriented.

## VIII. CONCLUSIONS

The comparative analysis conducted in this work developed from the identification of a problem shared by multiple legal systems: the need to design CBDCs that combine the efficiency and security of payments with an adequate level of privacy protection for citizens. This common issue has constituted the starting point for an investigation aimed at examining the concrete solutions adopted (albeit in an evolving context) by two of the main economic actors on the global stage.

This balancing exercise is inevitably situated within the social, cultural, and political framework of each legal system. The analysis of the EU and the PRC models have shown that the design of CBDCs reflects implicit cultural structures – the so-called cryptotypes[114] – that profoundly influence regulatory choices. The differing conceptions of the relationship between public authority and the individual, and of the function of personal data protection, are manifested in the distinct technical and legal architectures of the respective CBDCs.

What emerges is that the European model is characterized by a strong *ex ante* and *ad hoc* regulatory framework, which seeks to embed the fundamental principles of the European legal order within the technical and design choices of the CBDC. By contrast, the Chinese model appears to allow a relatively broad degree of discretion in shaping the technical infrastructure and, as a result, in managing data, in the absence of a detailed and binding regulatory framework.

The analysis of the divergences and convergences between these models made it possible not only to highlight their underlying rationales, but also to suggest potential future trends in the global regulation of CBDCs. Indeed, a jurisdiction's approach to privacy in the context of CBDCs can influence other States[115], potentially guiding the emergence of shared practices and new international standards in their design and regulation.

As noted at the outset of this contribution, the efficiency of CBDCs will largely depend on their ability to be employed in cross-border transactions, which presuppose not only technical but also legal interoperability. From this perspective, it is evident that regulatory harmonization – particularly in the field of personal data protection, but not exclusively – is not only desirable but in fact essential[116].

The European Union, which already plays a central role in shaping global regulatory standards through the Brussels Effect, appears well placed to extend this influence on the emerging field of CBDCs. At the same time, the PRC, as noted, can positions it as a potential influencer of other legal systems, leveraging its geopolitical network through the BRI, and on its first-mover advantage in a field devoid of common standards.

---

114 A. Gambaro, R. Sacco, M. Graziadei, Sistemi giuridici comparati, cit., at 6.

115 H. Wang, *Understanding Disputes Over Digitalization: A Perspective of Cross-Border Central Bank Digital Currencies* (2025), at 16.

116 BIS and other Central Banks, *Central Bank Digital Currencies: Legal aspects of retail CBDCs*, cit., at 25.

How these models will interact, compete, or converge on the international stage remains to be seen. What is certain, however, is that the choices made today by key global actors will have long-lasting implications for the governance of digital money and the protection of individual rights in the digital age.

# GOVERNANCE PROFILES OF SECONDARY USE OF HEALTH DATA IN THE EHDS

*Raffaele Ambrosino*

TABLE OF CONTENTS



*This contribution offers a critical analysis of the governance framework for the secondary use of electronic health data established by Regulation (EU) 2025/327 on the European Health Data Space (EHDS), situating it within the broader context of the European data strategy. The author starts from the observation that the growing economic valorisation of health data risks fostering the emergence of a lex mercatoria of data, potentially at odds with the sensitive nature of health information and with the protection of individual rights. From this perspective, the EHDS is interpreted as a regulatory response aimed at removing the health data market from purely private-law logics and reorienting it towards a model of public governance grounded in the pursuit of collective interests. The paper focuses in particular on the opt-out mechanism provided for the secondary use of data, highlighting its ethical and legal shortcomings. According to the author, the presumption of consent to data reuse—subject to the exercise of a right to exclusion—is problematic in light of the conditions of vulnerability under which consent to the collection of health data is typically given. The opt-out mechanism thus results in a downsizing of the role of informed consent, which is recovered only ex post, and marks a further step towards overcoming consent as the central legal basis for the processing of health data. Considerable attention is devoted to the analysis of data access bodies, identified as the core actors in the governance system for secondary use. These public bodies are characterised as true second-level data controllers and as providers of a public service of data access, formalised through administrative decisions and authoritatively determined tariffs. This institutional design reflects, in the author's view, a process of progressive "administrativisation" of data protection, which strengthens the public-law dimension of data reuse and legitimises processing on the basis of an important public interest. Finally, the contribution examines the delicate balance between collective objectives and the protection of individual rights, focusing on the principles of transparency and data minimisation, on anonymisation and pseudonymisation techniques, and on the use of secure processing environments. While acknowledging the regulation's overall guarantee-oriented approach, the author points out that the broad margins of discretion left to Member States and to data access bodies may result in uneven implementation, thereby placing strain on the objective of achieving a genuinely uniform European health data space*

**Keywords:** European Health Data Space (EHDS); Secondary use of health data; Data governance; Health data regulation

## I. THE EUROPEAN HEALTH DATA SPACE AS A NEMESIS TO THE *LEX MERCATORIA* OF HEALTH DATA.

One of the main effects of the implementation of the use of technology is the exponential enhancement of data, an element that, in its digital declination, represents both the product and the main source of supply of digital innovation systems whose operation and

development depend on algorithmic information[1] processors. And so even data, which has become an indispensable resource for the progress of the community, are at the center of a real market.

With the natural development of a bargaining area having as its object the exchange of data, however, it becomes necessary to interface, both with the legal implications related to the ontological characteristics of the commodity in question, and with the purposes that animate the user of the data to its procurement. In fact, it must be considered that the transfer of data, which takes the form of the well-known activities of communication and/or sharing of information, if it is attributable to a natural person, involves subjective interests partly extraneous to the purely patrimonial dimension of the activity underlying them, interests which, due to the particular sensitivity of which they are characterized, postulate another (r)o[2] degree of legal protection. It therefore seems unfortunate to run the risk of consigning these exchanges to the evolution of a peculiar *lex mercatoria.*

The European legislator, aware of these circumstances, but in particular of the strategic role inherent in the circulation of data, has therefore decided to focus its political agenda precisely on the regulation of data. As some scholars observe, "with the 'European strategy for data' the European Union aims to obtain a leading role in the data economy"[3] and, focusing on the phenomenon of data sharing[4], aims at the substantial construction of "data spaces"[5] that are cross-border, interoperable and, in a holistic vision, suitable to become technically secure environments and compatible with the protection of the aforementioned subjective interests on a legal level.

The construction of data spaces at the European level is based on the EU's duty to ensure the well-being of the community and to encourage, through its regulatory intervention, the development of certain strategic activities, among which the protection of public health and the advancement of scientific research stand out[6].

With respect to the latter sectors, Regulation (EU) 2025/327 of the European Parliament and of the Council was issued last February with the declared "aim of establishing the European Health Data Space (EHDS)". There seem to be two cornerstones on which the

[1] Recently, the framing of "data" as a form of digital representation of information has been addressed by A. Iannuzzi, *I regolamenti intersettoriali per l'istituzione dei «data spaces»: Data Governance Act e Data Act,* in *La regolazione europea della società digitale,* (ed.) P. Pizzetti, Turin, 2024.

[2] In the face of the process of commodification of the data, the personalistic aspects linked to the ontological dimension of the sensitive information found in it, requires forms of protection more suited to the protection of subjective rights than the mere recourse to the classic means of asset protection relating to contractual relationships.

[3] Thus D. Sborlini, *Il broad consent come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, in Contratto e Impresa, 2024, I, 223.

[4] The activity of "data sharing" is expressly defined in Article 2, no. 10, EU Reg. 868/2022 (*Data Governance Act*) as "the provision of data by a data subject or a data subject to a data user for the purpose of the joint or individual use of such data, on the basis of voluntary agreements or Union or national law, directly or through an intermediary, for example in the context of open or commercial licences, for remuneration or free of charge".

[5] The definition of "data spaces" is not provided for at the legislative level, it is the result of doctrinal elaboration, in particular see E. Curry, S. Scerri and T. Tuikka, *Data Spaces: Design, Deployment, and Future Directions*, Berlin/Heidelberg, 2022; M. Franklin, A. Halevy and D. Maier, *From databases to dataspaces: a new abstraction for information management*, in SIGMOD Record, Vol. 34, IV, 2005, 27 et seq.

[6] About it see T. Petrocnik, *Health data between improving health (care) and fueling the dataeconomy,* in Technology and Regulation*,* 2022, 124.

EHDS is based: the secure management of electronic health data, which can be subsumed in the category of the so-called. sensitive data; and the expansion of the hypotheses of reuse of the same; In other words, not only that individual use consisting in the use of health data for the purposes for which it is *naturaliter* formed and originally collected (so-called primary use) must be favored and regulated, but in particular the so-called "primary use". "secondary use", i.e. reuse - in aggregate form and in a collective information dimension - for the pursuit of purposes unanchored from the activity that led to its direct formation [7]. Article 53 of the Regulation expressly identifies the purposes in question corresponding to the achievement of collective interests, including: the protection of public health, statistical production, scientific research and the development of artificial intelligence algorithms.

More generally, it should be noted that the regulation, in line with the aforementioned political purposes, aims to establish a framework for structuring an organic discipline of data management activity, thereby transforming itself into an application model that can be adopted in the future in sectors other than healthcare. This is demonstrated by the detailed regulations governing each phase of the shared management procedure for electronic health data.

Due to the expansive scope of the so-called "S.p.A. secondary use, through which it is envisaged that actors belonging to sectors of social life unrelated to public health are expected to participate in the procurement of digital health data, it seems necessary to review the governance profiles

processed for the management of access to data by subjective categories other than the "data subject" and the data subject. The work aims to examine the presence of any structural obstacles to the uniform application of the discipline dictated by the regulation, in order to verify in a comparative key whether the spaces of discretion left to national legislators in the field of governance can be harbingers of unequal treatment between subjects belonging to another subjective category placed at the center of the electronic health data market: the so-called. "data users".

## II. THE OPT-OUT: THE (POSTHUMOUS RETRIEVAL OF) CONSENT TO THE SECONDARY USE OF ELECTRONIC HEALTH DATA.

The analysis of the health data governance system provided for by Section 2 of Chapter IV of the Regulation requires some preliminary clarifications on issues impacting the substantive profiles of secondary use. First of all, it should be noted that the regulation *in question* refers to a specific category of health data, the "electronic" one[8], a concept

[7] See in particular A. Cabrio, *La seconda vita dei dati. Luci e ombre della normativa privacy in materia di secondary data use*, in *Il futuro della sanità. Strumenti per una reale innovazione*, (edited by) F. Frattino - F. Massimino, 2024, 21; M. Ciancimino, *Circolazione "secondaria" di dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche*, in Il diritto di famiglia e delle persone, 2022, I, 37.

[8] As observed by S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in Le Nuove Leggi Civili Commentate, III, 2025, 563, with the introduction of the regulation a new category of data is defined, since "Not only is there no coincidence between the notion of electronic health data and that of health-related data, but not even between health-related data and personal electronic health data:

verbatim declined in the double definition of "personal electronic health data" identified (pursuant to letter a), art. 2 co. 2 of the regulation) in the "data relating to health or genetic data processed in electronic format"; and of "non-personal electronic data" which is instead the electronic health data other than the personal one that can include both the (totally) anonymized data and that by its nature "never" referable to a data subject[9]. Remaining in the space dedicated to definitions, it should then be emphasized that secondary use is identified as an activity of "processing" of the data[10].

Hence, the important classification approach: the secondary use of data in the EHDS is, in general, an activity of processing health data in electronic format, a framework confirmed by the express provision of coordination based on which the regulation in question is in a relationship of subsidiarity with EU Regulation 2016/679[11]. In fact, from the point of view of the European legislator, the EHDR regulation "specifies and integrates" the rights of natural persons guaranteed by the GDPR[12].

It is now useful to point out that - on a functional level - secondary use, although it is ontologically distinct and is conceived in terms of autonomy with respect to primary use, cannot be separated from the latter. In the genesis of the raw material, i.e. the electronic health data, the primary use represents the source of the original materialization of the same which, in most cases[13], comes into existence when the patient's electronic medical

Thus, in order for a data relating to health to be considered personal electronic health data, it is necessary that it be processed in electronic format and, conversely, for a personal electronic health data to be considered data relating to health, it must not be a genetic data. In fact, the definition of "personal electronic health data" includes both health data and genetic data". For a legal framework of data in the specific sector of scientific research, even before the approval of the regulation, see P. Guarda, *Il regime giuridico dei dati della ricerca scientifica*, Editoriale Scientifica, 2021 and G. Bincoletto, *Scientific research processing health data in the European Union: data protection regime vs. open data*, in Journal of Open Access to Law, II, 2023, 1.

[9] L. Ruggeri, *La dicotomia dati personali e dati non personali: il problema della tutela della persona nei c.dd. dati misti,* in Dir. fam. pers., 2023, 808.

[10] Pursuant to Article 2(d) of Regulation (EU) 2025/379, the definition of 'secondary use' corresponds to the 'processing of electronic health data for the purposes set out in Chapter IV of this Regulation, which are different from the initial purposes for which such data were collected or produced';

[11] EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data, in the Official Gazette, Law 119, 4 May 2016; on this point R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (eds.), ), *Codice della privacy e data protection*, Milan, 2021; P. Guarda*, Il diritto alla protezione dei dati personali in Europa ed il Regolamento Generale sulla Protezione dei Dati*, in P. Guarda – G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Milan, 2023, 55.

[12] The European legislator in the context of secondary use (both in Article 1 par. 8 where it states that "access to electronic health data for secondary use agreed within the framework of contractual or administrative agreements between public or private entities remains unaffected", as well as in Article 52 par. 3 where it is provided that data access bodies when issuing data authorizations "may include contractual agreements between health data holders and health data users for sharing data containing information or content protected by intellectual property rights or trade secrets.") it clears the use of the contract as a tool for the circulation of electronic health data, paving the way for the idea of a real market for electronic health data. In this regard, C. Perlingieri, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, in Tecnologie e diritto*,* II, 2024, 485.

[13] Access to data for secondary use in accordance with the provisions of Article 51 of Regulation (EU) 2025/379 concerns not only information in digital format from electronic health records but also other categories of electronic health data: personal electronic health data automatically generated by medical devices; data from wellness applications; data from clinical trials, clinical trials, clinical investigations and performance studies subject to Regulation (EU) No 536/2014, Regulation (EU) 2024/1938 of the European Parliament and of the Council, Regulation (EU) 2017/745 and Regulation (EU) 2017/746; data from medical records and mortality registers; other health data from medical devices. With the exception of those

record is constructed. A moment that generally coincides[14] with the formation or sharing of the personal health information of the data subject in the constancy of a medical care or assistance activity conducted by a health professional. So, if these data, incorporated in the electronic medical record[15], represent in their individual dimension the substrate of primary use in the EHDS, they, as a result of the transfer mechanisms conceived in terms of legal obligations by EU Regulation 2025/327, represent, in a "collective" dimension, the main source of supply for secondary use. But be careful; if we consider that primary use presupposes the formation of the data on an individual level, it must still be recognized that the data thus formed represents a necessary but insufficient element for the purposes of secondary use, as the achievement of the purposes referred to in Chapter IV of the Regulation requires a *quid pluris*, i.e. a large-scale aggregation of individual data relating to individual medical[16] records; aggregation that presupposes an activity of further processing of the set of data collected. For these reasons, secondary use should be identified as a "second-level" treatment of electronic health data already acquired for primary use. This close genetic interconnection is evidenced, on a textual level, by the Community legislator itself which, aware of the uniqueness of the data, already at the time of its formation (in the context of primary use) is concerned with introducing the necessary legal basis for the processing of health information for secondary use.

The issue of the legal basis is important because, in addition to reflecting on the standards of adequacy and proportionality guiding data governance, it represents one of those matters in which the European legislator has left some margin of discretion to state legislators[17]. Firstly, since the purposes characterizing secondary use imply, on an ontological level, a "collective" destination of the patient's personal information - not

included in public registers and biobanks, the source of most health data intended for reuse is in any case an activity that can be subsumed in the so-called "Renewable Environment". primary use. It is quite rare, and moreover hindered by anonymization obligations, that electronic health data can be created *from scratch* for a mere secondary use.

[14] Electronic health data for primary use is not always the product of a technically clinical activity, just think of the data generated by applications for the well-being of smart electronic devices, the subject of attention of the Regulation together with electronic medical records.

[15] For an examination of the various positions and obligations relating to the subjects involved in the processing of medical record data, please refer to C. Perlingieri, A. Cocco, *'Primary' and 'Secondary' Use of Electronic Health Data*, in Italian Law Journal, X, 2024, 275, where the authors highlight the need for coordination between the discipline introduced with the approval of the EHDS Regulation and the provisions of the minister's decree EHR 2.0 of 20 May 2022.

[16] According to Recital (53) of EU Reg. 2025/327 as "Electronic health data used for secondary use can bring great benefits to society. The use of real-world data and evidence, including information on patient-reported outcomes, should be encouraged for evidence-based regulatory and policy purposes, as well as for research, health technology assessment and clinical objectives." In order to achieve this objective, recital (53) states that "it is important that the datasets made available for secondary use under this Regulation are as complete as possible."

[17] Pursuant to Article 51, paragraph 4 of EU Reg. 2025/327, member states are given the possibility to "introduce stricter measures and additional guarantees at national level aimed at protecting the sensitivity and value of the data falling under paragraph 1, letters f), g), i) and q)."; Furthermore, with reference to the power to exclude access to data for secondary use, art. Article 71, paragraph 4 of the Regulation provides that, under certain conditions, "a Member State may provide in its national law for a mechanism to make available the data for which the right of exclusion has been exercised". A systematic reading of the two rules leads us to believe that in some circumstances the legal basis for secondary use provided for at a general level by European legislation can be integrated or even deactivated by individual national states, generating inhomogeneity in the governance of electronic health data.

contemplated by the purposes of medical assistance and treatment - it is necessary to protect the autonomy of the subjects to whom the health data belong in the light of their sensitive nature. For these reasons, the reuse of data would presuppose a specific decision by the natural person on the processing of the same for the specific purposes incorporated in the so-called secondary use.

Such a decision implies, of course, the manifestation of a consent that must be collected by the data controller at the time the data comes into existence, which also corresponds to that of the production of the information for "individual" clinical purposes. However, the path taken by the European legislator on this point is that of the so-called mechanism. opt-out, a (relative) presumption according to which in the absence of an express exclusion by the data subject, the health data formed for primary use can also be used for secondary uses provided for by the regulation[18]. Following this approach, the consent to the processing of the data by the data subject assumes its relevance, as it can affect, even if *ex post*, the secondary use. It is also important to note the strong dogmatic force of the opt-out, whose implementation could theoretically resurface the question of the data subject's consent as a basis for the lawfulness of processing sensitive data[19]. However, in the case of health data, this issue seems to have long been superseded, given the super-individual needs underlying and protected by the combined provisions of Articles 9(2)(h) and (i) and 89 of the GDPR. From an interpretative perspective, the provision seems to highlight an atavistic need to retrieve an expression of will from the data subject "upstream" in order to authorize a "downstream" use whose legal basis is entirely different from that for which the data is being processed[20].However, caution should be exercised because, as will be

[18] Before the entry into force of the regulation, with reference to the hypotheses of reuse of health data contained in an electronic health record for so-called "electronic health record" activities. In the case of proactive medicine developed in the autonomous province of Trento, the Italian Data Protection Authority has taken a radical position, denying the possibility of considering the reuse in question lawful in the absence of an autonomous expression of consent by the data subject. According to the supervisory authority, a healthcare professional subject to professional secrecy may only use the data for treatment purposes when this is necessary and essential for the patient's health. Whenever one is outside the ontological perimeter of primary use, any further data processing activity must be expressly and autonomously authorized.

[19] According to the majority doctrinal approach, in the matter of personal data we are faced with subjective legal situations that can be declined as personality rights. At the dawn of the introduction of Law no. 675 of 31 December 1996, E. Giannantonio, *Dati personali (tutela dei),* in *Enciclopedia del diritto,* Aggiornamento III, Milan, 485, reconstructed the law on personal data, as a sort of *habeas corpus* of the cybernetic era; consequently, only the consent of the data subject, which can always be revoked, could have made lawful any operation relating to the use of such information by by a person other than its owner. As recently stated by P. Gallo, *Dati personali (diritto allo sfruttamento economico),* in *Digesto delle discipline privatistiche,* Turin, Update 2022: "taking into account the unavailability of the rights in question, the consent of the entitled party fulfills the important function of making the processing of personal data lawful, just as in general the consent of the entitled party is valid for discriminating certain intrusions into the sphere of others personal, such as the publication of the image, intrusions into privacy and so on". On this point, see also A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto,* Naples, 2017; S. Thobani, *Diritti della personalità e contratto,* Milan, 2018; F. Bravo, *Il diritto a trattare dati personali nello svolgimento dell'attività economica,* Padova, 2018; G. Resta, V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2018, 411; G. Resta, *I dati personali oggetto del contratto*, in *Annuario del contratto,* 2018; V. Ricciuto, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in Rivista di diritto civile, 2020, 642.

[20] It is useful to point out that, in Italy, in application of art. 110-bis of the GDPR, if there are particular cases in which obtaining the consent of the data subject for the reuse of personal data for the purposes of scientific research appears complicated, the data subject is given the opportunity to request an authorization for reuse directly from the Data Protection Authority, subject to the adoption of precautions aimed at

further specified below, this approach is actually geared towards definitively overcoming consent as a necessary means of legalizing processing[21].

The point deserves a reflection which, in the opinion of the writer, makes the choice of the opt-out tool ethically questionable. If the sharing and consequently the processing of personal data must be considered lawful activities only if assisted by the consent of the data subject, which is therefore a necessary condition of the entire operation, it is equally essential that such consent, in order to be binding, be expressed in a conscious and free manner. It should also be remembered that in health matters the so-called consent. privacy often goes hand in hand with consent to health treatment itself, which is strengthened in its ontological traits by being "informed".[22] Precisely in the case of processing health data, the psychological condition in which this consent matures must be taken into account. The concrete context of reference, as mentioned, is almost always that of the patient who discloses his or her sensitive information to the professional as part of an individual health

eliminating any danger of re-identification of the data subject. ("The Garante may authorise the further processing of personal data, including those of the special processing referred to in Article 9 of the Regulation, for scientific research or statistical purposes by third parties who mainly carry out such activities when, due to particular reasons, informing the data subjects is impossible or involves a disproportionate effort, or risks making impossible or seriously jeopardizing the achievement of the purposes of the research, provided that appropriate measures are taken to protect the rights, freedoms and legitimate interests of the data subject, in accordance with Article 89 of the Regulation, including preventive forms of data minimization and anonymization"), on point F. Polito, *Il consenso al trattamento dei dati personali in tema di ricerca medica e gli artt. 110 e 110*-bis *del codice privacy*, in *Ricerca in sanità e protezione dei dati personali. Scenari applicativi e proposte future* (edited by) E. Chizzola – P. Guarda – V. Maroni – L. Rufo, Editoriale Scientifica, 2024, 5.

[21] According to S. Corso, in *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327,* cit. 579, with the introduction of an autonomous legal basis for processing for secondary use, as an exception to art. 6 of the GDPR "consent, albeit limited to secondary use, is not only no longer the main legal basis and case of derogation from the prohibition, but can no longer even be an additional condition for the processing of data relating to health, *pursuant to* Article 9(4) (35). In this sense, the EHDS, in the context of secondary use, goes beyond the mere overcoming of any national settings, even more or less consensus-centric, and bans the instrument of consent – understood at least as consent of the data subject or *ex ante consent* – from European legislation". On this point, cf. see also M. Afra, *An Assessment on Innovator's Ability for Consent-Free Health Data Reuse*, *In the Context of the GDPR and EHDS: The Netherlands Case Study*, in European Journal of Health Law, vol. 31, V, 2024, 475; F. Kertesz, *Collaboration in Healthcare: Implications of Data Sharing for Secondary Use in the European Union,* ibid., 497 ff.; C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in Contr. impr., II, 2020, 860.

On the downsizing of the role of consent in the context of the reuse of data relating to health for medical research and statistical purposes, see also F. Polito, *Il consenso al trattamento dei dati personali in tema di ricerca medica e gli artt. 110 e 110*-bis *del codice privacy,* cit. 16 who expresses perplexity about the easy identification of the specific cases in which it is possible to resort to the derogation from consent referred to in art. 110-bis Privacy Code.

[22] Although informed consent to health treatment must be distinguished from the so-called privacy policy, pursuant to Article 4, no. 11 of the GDPR, also in this context the duty to inform is an essential element of the case since the consent of the data subject is "any freely given, specific, informed and unambiguous expression of the will of the data subject, with which the same expresses his consent, by a statement or unambiguous affirmative action, that personal data concerning him or her are being processed". It should be reiterated that "informed consent" in the matter of health treatments, according to the prevailing approach, can in no case be considered presumed. On this point, N. Todeschini, *Liability in Medicine*, Milan, 2023 who, on p. 209, defines the presumption of (informed) consent as a "contradiction in terms". Compliant, Cass. civ., sec. III, 27 November 2011, no. 20984 according to which if it is true that on the evidentiary level informed consent does not require the existence of written evidence *ad substantiam,* on the substantive level it still requires a "real manifestation".

For further information on the relationship between informed consent and privacy, P. Cosomai, *The right to health, informed consent and privacy,* in *EXPLICO – Digital health* (ed.) by P. Cosomai- A. Perrone, Milan, 2020, 98.

care relationship which, in most cases, can be characterized by the existence of a condition of vulnerability (de facto or de jure) of the data subject[23]. Taking into account these conditions, it would be rather risky to suppose the absolute absence of mental reservations on the part of the patient on the awareness of (a possible) reuse of factual data provided for the overcoming of a clinical problem; perhaps it could not even be assumed that there was a mere voluntary disclosure of the data itself, even for primary use. The sharing of information regarding one's state of health is often animated by a psychological (and physical) condition of vulnerability and is based more on the "duty" than on the "wanting(s)" to share in a "contractual" nature. Assuming an equivalence between consent to primary use and consent to secondary use of (personal) data materialized under such conditions appears to be a gamble, even if the consent is preceded by adequate information by the data subject. From this point of view, the retroactivity of which the right of exclusion referred to in art. 71 of EU Reg. 2025/379, which can be exercised at any time, ends up representing a "palliative" solution to the proposed solutions. With the opt-out mechanism, the data subject is allowed to express the desire to limit the use of his or her sensitive data for secondary uses even if consent was originally presumed, recovering only *ex post* an awareness perhaps weakened by a condition of clinical vulnerability.
It is also useful to underline that, also because of the conclusions that will be reached *below*, the hypothesis in question cannot constitute a case of "broad consent"[24] since the so-called broad consent presupposes a priori indefiniteness of the processing purposes which, in the case of reuse, seems to be neutralized by the regulatory taxonomy with which the regulation outlines the purposes in question; and underlies the uniqueness of the data controller receiving the consent of the data subject, a condition, the latter also irreconcilable with the operational structure emerging from the regulation which, on the other hand, concerning the governance of secondary use, provides for mechanisms of joint data controller between several subjects, distinct from each other by nature and functions.

## III. DATA ACCESS BODIES: FUNCTIONS AND LEGAL NATURE OF THE ACTORS IN THE PROCESS OF REUSE OF ELECTRONIC HEALTH DATA.

Having established the link between the individual acquisition of health data for primary use and aggregate use for the purposes referred to in art. 53 of the Regulation, it is now

[23] For a complete analysis, see V.V. Cuocci, *The protection of personal data of vulnerable subjects in the digital dimension. A study of comparative law*, Bari, 2022.
[24] This term indicates a newly minted institution whose objective is to integrate a protection measure for the recovery of the lawfulness of the processing of data, if the latter are collected by the owner in the context of a scientific research activity. It is introduced by Recital no. 33 of EU Regulation 679/2016, according to which "Recital no. 33 of the aforementioned Reg., in particular, provides as follows: "[i]n many cases it is not possible to fully identify the purpose of the processing of personal data for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research where there is compliance with the ethical standards recognised for scientific research. Data subjects should be able to give their consent only to certain areas of research or parts of research projects to the extent permitted by the intended purpose.'

possible to focus the investigation on the governance systems designed by the European legislator for the management of health data for secondary use.
Since secondary use technically corresponds to an activity of "processing" electronic health data, governance must be analyzed starting from this classification. As in any processing activity, on the one hand, we have the data controllers of health data who are not the "data subjects", but the data controllers of the data acquired for primary use; on the other hand, are contemplated the so-called data users, i.e. those subjects who intend to access aggregated digital health data for the achievement of the purposes referred to in art. 53. As mentioned, the processing in question is in itself of the "second level": the access requested by users concerns the so-called " dataset, i.e. an information aggregation in which individually purchased data are collated; this operation therefore underlies the execution of those activities of selection, extraction and interconnection indicated by art. 4 of the GDPR. This implies the need to identify an additional figure responsible for carrying out such processing activities not attributable to the individual data subjects. In fact, the latter, in the case of data authorization, become mere taxable subjects of the legal obligation to communicate the data in their possession which, together with those provided by similar data controllers, end up generating a bundle of individual health data that give rise to the so-called "series of the data". data series. In other words, in the EHDS system, each individual controller is required to communicate the data held to a single reference body that acts as a collector and aggregator of the same and carries out an autonomous and specific processing activity.
The data controller in question is identified as the body responsible for access to the data, an entity that represents the nerve center of the governance of health data for secondary use which is delegated a fundamental role in the context of second-level processing. Any dynamic regarding the governance of the matter in question thus passes through the framing of the entire procedure of access to data in which these new state bodies are protagonists.
This decision is an extension of the approach - initially undertaken with the European Data Strategy, and subsequently implemented specifically with the implementation of various sector regulations (Data Act, DGA, etc.) - which has enhanced the role of data access bodies. These bodies, whether already existing or newly created, as in the case of data access bodies, are conceived and configured by the European legislator as "intermediary" institutional entities. Their primary function is to ensure the appropriate performance of the diverse range of activities encompassed in the concept of data processing, particularly in the case of data dissemination and sharing within the market and within the supranational sphere. This approach, while ensuring the greatest possible uniformity in this area and the hope of thus achieving a single data market, is crucial.
First of all, it should be noted that secondary use comes into play when electronic health data are the subject of an access request, an act that triggers an activity of circulation of health data that involves three subjective profiles: the data owner, the applicant and the data access body.
With reference to the first of the three actors in the procedure, it should be noted that the use of the word "controller" must be declined in an atechnical sense in order to avoid the

danger of confusing the data controller with the data subject. Those who own the requested data (so-called data controller) become data controllers in only two moments and circumstances: the one in which they came into possession of the electronic health data (so-called primary use) and the one in which they communicate, (*recte* is required to communicate) the "personal" [25]electronic health data to the access body required. In the context of secondary use, the actual controller is primarily the data access body. It should also be noted that the identification of the data controller is not predefined[26], as it is linked to the operation of two regulatory variables, which are: the obligation to make the data processed for primary use available to data access bodies[27] on the one hand, and, on the other hand, the exclusion positively from Article 50 of the Regulation. This functional approach leads to the exclusion of a one-to-one correspondence between the data controller in the context of primary use and the data subject for secondary use, since, if the former is a natural person (a researcher) or a micro-enterprise, due to the exemption granted by the legislation, it cannot be considered a "data controller" according to the provisions of Chapter IV of the Regulation. However, care should be taken not to overlook the dispositive nature of the rule governing the exemption in question; the European legislator recognises that individual Member States have the power to deactivate the exclusion *in question* and to also oblige natural persons and micro-enterprises within their jurisdiction to provide data. This exception is of important importance in terms of governance since, being left to a purely discretionary assessment of the individual State, it could give rise to cases of unequal treatment in access to datasets between users of individual States, so that the subjective expansion of data holders, while generating an advantage, would nevertheless be an obstacle to the harmonious functioning of the EHDS envisaged by the legislator.

Therefore, excluding the subsumption of the data subject in the figure of the data controller, in the circulatory phenomenon for secondary use the data controller is explicitly assigned to the data access bodies. Well, the legal nature of the figures in question as a "public body" appears symptomatic of the underlying value of the same concept of secondary use. The regulation, by obliging individual States to set up these bodies *from scratch*, in the event that they do not intend to entrust existing public bodies, ends up

[25] Even if the data subject is subject to an obligation, the performance of the same still takes the form of an activity of communication of sensitive data, therefore this fulfilment must also be considered a processing activity if it concerns personal digital health data. At this stage, we are not in secondary use because the data in question has not yet become available to the requesting user. Particular is the case of the so-called. "reliable" data controllers (in depth *below*) framed by art. 74 EU Reg. 2025/327 as data controllers for secondary use when they make the health data in their possession available to users.

[26] There is no classification that takes into account the mere subjective qualities of the data holder, as stated in recital (59) of EU Reg. 2025/327 "Holders of health data in the context of secondary use should therefore be entities that are providers of health care or care or carry out research activities in relation to the health care or care sectors, or develop products or services for the healthcare or care industries. These entities can be public, non-profit or private".

[27] Ex recital (52) EU Reg. 2025/327, "this Regulation introduces the legal obligation, pursuant to Article 6(1)(c) of Regulation (EU) 2016/679, in accordance with Article 9(2)(i) and (j) of that Regulation, that the holder of health data is required to report personal electronic health data to the bodies responsible for access to health data". A legal basis is introduced for the lawfulness of the communication of data from the data subject to the data access body, an activity that constitutes data processing whose data controller pursuant to art. 74 of the Regulation is precisely the subject who collected the data in the context of primary use.

investing the new operational figures with tasks of public interest and in doing so does nothing but raise the very nature of the purposes underlying the reuse of electronic health data to the public level. The public framework of data access bodies then ensures that the issue of the legal basis of the processing (and the mandatory consent of the data subject) is overcome: in fact, from a legal point of view, the subjective nature of the data controller legitimizes the processing activity that ends up falling within the abstract case referred to in letter f) pursuant to Article 6 of the GDPR and elides, the prohibition referred to in art. 9 par. 1 GDPR[28] taking the form of a hypothesis of processing "necessary for reasons of important public interest based on Union or Member State law".

A combined reading of these classificatory approaches and other hermeneutical elements, based on a systematic approach to the provisions of the regulation, can lead us to the exact framing of the entire legal relationship culminating in the granting of the authorization to the data. The interpretative pieces are represented specifically:

a) the qualification of the third party involved in the re-use of electronic health data (the applicant) and;

b) the provision for the payment of pecuniary fees for access to the same.

With reference to the data requester, the use of the word "user" is significant, with which the person requesting authorization to the data is designated. In this regard, it is legal semantics that offer further clarification regarding the exact legal classification of the relationship that is established between the applicant and the body to which the request is addressed. It is in fact known that, in the legal field, the word "user" means the subject of an economic relationship, an active user of a service whose provision is intended either to an indeterminate category of subjects or, more generally, to the community of associates. It follows that even the activity of disseminating electronic health data for secondary use, according to linguistic interpretation, must be classified as a service, which, due to the legal nature characterizing both the object of the service and the subjects responsible for its provision, can be understood, specifically, as a public service.

In support of this framework, the other hermeneutical element comes to the rescue, namely the provision for the payment of a monetary fee for the use of access to the data series. Even with respect to this element, semantics plays a fundamental role as the European legislator qualifies the fees in question as "tariffs", a term that according to the prevailing doctrine[29] refers to the price paid for the use of a good or service whose determination does not depend on the will of the parties but is imposed authoritatively by reason of the collective interest underlying the service.

It should also be noted that - pursuant to Article 2 paragraph 2 letter v) of the Regulation - the "authorization of data" is defined as "an administrative decision"; This implies a further strengthening of the divided hermeneutical reconstruction which, on a legal level,

[28] On the subject of "special" data referred to in Article 9 of the GDPR, see more M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679,* in Le Nuove Leggi Civili Commentate, I, 2017, 165.

[29] On this point, see F. Merusi, *Su alcuni aspetti problematici della determinazione autoritativa dei prezzi*, in Foro Amministrativo, II, 1965, 157; A. Cassone, *Lo stato attuale della teoria delle tariffe*, in *Econ. Pubbl.*, 1978, 288; P. Bilancia, *Determinazione dei prezzi e libertà d'impresa*, Padova, 1986

corroborates the approach[30] according to which, in the matter in question, the European legislator intends to proceed with the progressive "administrativeization" of data protection. A process that, as other authoritative doctrine observes[31], brings with it the succumbing of the rule of private law compared to that of administrative law.

## IV. Data governance in the prism of the balance between the achievement of collective purposes and the protection of individual rights.

At this point, the analysis of governance in the context of secondary use must be carried out taking into account the classification of the authorization of data as the provision of a public service, and the circumstance that this service has as its object an activity of processing ontologically "sensitive" data. It should also be noted that the management of electronic health data for reuse can only fulfill its political mission if it is able to transform the data into information that is useful for the purpose for which access is requested[32]. However, the potential conflict of this objective with the prerogatives of protection of confidentiality deriving from the sensitivity of health data makes the governance activity articulated, implying the attribution to data access bodies of a delicate function of balancing the various interests at stake[33].

The governance rules coined with the regulation are, on closer inspection, the result of an arduous compromise between the political objectives of the European legislator and the technical-legal instances put in place to protect confidentiality. From the first point of view, the emphasis on data reuse is a corollary of the main strategic objective of the Data Governance Act which encourages data sharing because of the potential altruistic benefits[34] for fundamental sectors of social life. The technical-legal precautions inherent in the folds of certain structural and procedural aspects of governance are instead to be traced back to the observance of the considerations[35] of the European Data Protection Board and the European Data Protection Supervisor regarding the danger to the

30 S. Corso, *The electronic health record 2.0. Ideas for a critical reading*, in The New Commented Civil Laws, 2024, 334.

31 P. Perlingieri, *La pubblica amministrazione e la tutela della privacy. Gestione e segreto dell'informazione nell'attività amministrativa*, in Annali della Facoltà di Economia dell'Università degli Studi del Sannio, VIII, 2003, 211.

32 The doctrine tends to distinguish the datum from the information, specifying that while the former has an intrinsic and objective cognitive value, in the latter the cognitive value turns out to be the result of a subjective operation of the individual user consisting in an elaboration of the former. In this sense, D.U. Galletta, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in federalismi.it, V, 2016.
For an examination of the ontological difference between data and information in relation to health data, G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi,* Bologna, 2012.

34 "Reuse" and "Altruism" of data represent two of the fundamental principles ordering the implementation of the strategic objectives set by the Data Governance Act. On this point, see F. Caloprisco, *Data Governance Act. Condivisione e "altruismo" dei dati,* in *Annali AISDUE*, 2021; E. Salerno, Il Data Governance Act, *il nuovo Regolamento europeo per il mercato unico dei dati rischia di non essere abbastanza e favorire i grandi della tecnologia*, in Privacy e Cybersecurity, 26 febbraio 2021, 7; A. Sola, *Primi cenni di regolazione europea nell'economia dei dati*, in MediaLaws, 2021, III, 194; E. Cremona, *Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso*, in Rivista italiana di informatica e diritto, 2023.

35 This is a joint opinion on the proposal for a Regulation (EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, Adopted on 12 July 2022).

protection of privacy related to the secondary use of digital (personal) [36]health data. The general principles underlying this balance are those of transparency - which guides the entire organizational-institutional structure of the bodies responsible for governance - and data minimization, which instead penetrates the procedural aspects by determining the content of the individual datasets for which authorization is issued.

The implementation of transparent data governance in the EHDS is linked to the public framework of the data access service, and is reflected in the institutional structure of the data access bodies tailor-made by the regulation with the precise aim of avoiding the occurrence of hypotheses of conflict of interest[37]. In this regard, a mere investiture of existing or newly established public bodies seemed insufficient, considering it rather necessary to provide for and regulate (perhaps hypertrophically) certain structural and indefectible characteristics of these entities, and to introduce obligations of a financial nature on the part of the Member States to ensure their managerial autonomy. On the structural side, there is a division of tasks among the various operational sections within the body, each of which is not only autonomous in terms of function and decision-making, but is also independent in terms of organization and economics. Each state body should therefore (be equipped with, or) have a corporate structure in which each body, structurally self-sufficient, is vested with the individual functions assigned by the regulation to the data access body. Only the organic segmentation of corporate bodies would be able to ensure that a request for data is the final product of autonomous institutional steps which, although connected and hinged on the same procedure, remain individually characterized by a decision-making capacity free from reciprocal influences, thus neutralizing potential conflicts of interest. Only through a horizontal diversification within the entity between the body responsible for the selection of data sets, the body responsible for anonymization/pseudonymization, the body responsible for determining the tariff, the body responsible for managing the secure environment for sharing data, etc., will it be possible to defuse mechanisms that manage the processing of data for secondary use that are abstractly conflicting and contradictory with respect for the principle of transparency. It is precisely in this perspective that the obligation for individual States to provide data access bodies with economic and financial resources adequate to the configuration of a compartmentalized organizational structure should be interpreted. The possibility of entrusting the exercise of the functions *in question* to public bodies which, by their nature, are not able to assume a corporative dimension that can guarantee the functional diversification imposed by the European legislator, must therefore be excluded.

As a counterpart to transparency, in compliance with the technical-legal guarantees related to the protection of the privacy of the data subjects, the operation of the principle of data

[36] Scholars have also expressed critical remarks regarding the possibility that the excessive tendency to favor the reuse of data may have as a side effect a loss of control by the data subject over his or her data. In particular L. Marelli et al, *The European health data space: Too big to succeed?*, in Health policy, CXXV, 2023, 104861.

[37] An essential aspect is given by the obligation of individual Member States to notify the European Commission within 24 months of the entry into force of the regulation, the identity of the data access bodies and any changes to them.

minimization is placed[38]. However, the minimization does not affect those "non-personal" electronic health data *ex se* transfused into public databases, available and consultable in the so-called open access mode. The application of this principle governs the initial segment of the data access procedure triggered by a data request submitted to the access body. In fact, the latter, having completed the preliminary step of concrete verification of the specific purpose of use of the requested data and ascertained the absence of the obstructive conditions pursuant to Article 54 of the regulation[39], proceeds with the identification of the data sets useful to meet the user's needs. At this procedural juncture, the collection of the data then made available to the applicant - compulsorily transmitted by the data controllers - undergoes an initial processing activity, consisting of their anonymization or pseudonymization. It should be noted that these activities, although both are the subject of a legal obligation, live in a relationship of functional subsidiarity; According to the intention of the European legislator, anonymization should represent the main path that the body is required to follow in the preparation of the requested data sets, while pseudonymization remains a residual option whose application occurs only if an anonymization of the data nullifies the usefulness of the request in light of the inability of the anonymous data to be transformed, in the concrete case, into information[40]. The

[38] The necessity, adequacy and proportionality of the data requested with respect to the declared purposes are the essential characteristics for a request for access to the data to be accepted by the bodies. Pursuant to art. 5 par. 1 letter c) of the GDPR the data must be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed".

[39] Article 54 of the Regulation prohibits access to health data for: "a) taking decisions detrimental to a natural person or a group of natural persons on the basis of their electronic health data; in order to be considered as 'decisions' for the purposes of this point, they must produce legal, social or economic effects or similarly significantly affect those natural persons; (b) to take decisions, in relation to a natural person or group of natural persons, in respect of job offers, to offer less favourable conditions in the supply of goods or services, including the exclusion of such persons or groups from the benefit of an insurance or credit contract, the modification of their contributions and insurance premiums or the terms of loans, o take other decisions, in relation to a natural person or group of natural persons, which result in discrimination against them on the basis of the health data obtained; c) carry out advertising or marketing activities; (d) develop products or services that are capable of harming humans, public health or society at large, such as illicit drugs, alcoholic beverages, tobacco and nicotine products, weapons, or products or services designed or modified in a way that is addictive, violates public policy or morality, or causes a risk to human health; (e) engage in activities contrary to ethical provisions under national law." According to M. Iaselli, *Le nuove regole per l'uso primario e secondario dei dati sanitari*, Maggioli Editore, 2025, cit. p. 75 if with specific reference to the use for marketing activities, "the inhibition highlights a prudent and guaranteeist approach, in line with the GDPR, to prevent the commercial exploitation of health data without informed and specific consent. However, one question that could arise is the compatibility of such restrictions with innovation in healthcare, particularly for the development of new drugs and personalised treatments based on large volumes of data."

[40] Although according to L. Rocher, J. M. Hendrickx, Y. A. De Montjoye, *Estimating the success of re-identifications in incomplete datasets using generative models*, in Nature communications, X, 2019, 1, it is impossible to speak in an absolute sense of anonymization, since it would always be possible in the abstract to be able to take the opposite path to the process of depersonalization of data; in any case, The distinction between the two procedures, that of anonymization and pseudonymization, is based on the technical and economic effort required for the re-identification of the data subject, which translates into a gradation of the risk inherent to each type of processing used for the elimination of the identification process. In this regard, cf. E. M. Weitzenboeck, P. Lison, M. Cyndecka and M. Langford, *The GDPR and unstructured data: is anonymization possible?*, in International Data Privacy Law, XII, 2022, 184. European case law is of the same opinion: the Court of Justice of the European Union, in the Scania case of 9 November 2023 (Case C-319/22, Gesamtverband Autoteile-Handel v Scania CVAB, ECLI:EU:C:2023:837) has in fact specified that "In order to determine whether a natural person is identifiable, directly or indirectly, all means that could reasonably be implemented by the controller must be taken into account, pursuant to Article 4 (7) GDPR, or by others,

choice between anonymization and pseudonymization is, on a methodological level, oriented by the objective of favoring the dissemination of data to the extent that their knowledge is suitable for transforming itself into useful information[41]. Utility thus becomes a key concept in the governance activity carried out by data access bodies as it represents a fundamental decision-making parameter regarding the guarantees adopted from time to time; moreover, the evaluation of the degree of usefulness that the different data processing method can confer on the information provided to the user represents a further element of decision-making discretion that is the prerogative of data access bodies, whose operations may hinder a harmonious development of the EHDS. On an ontological level, it should be emphasized that utility, becoming an essential attribute of information, ends up impacting the entire market of personal health data[42]. The value of the latter[43] can no longer be traced back to its essential structure, but will be linked to two variables, to be verified on a case-by-case basis, namely: the degree of processing to which the data is subjected and the specific purpose for which it is requested. It will then be appropriate to assess whether the calculation of the fees provided for in the Regulation will have to take into account the level of "purity" of the dataset made accessible. In the opinion of the writer, it seems difficult to admit that the fee to be paid may depend on the market value of the shared data, since we are talking about a tariff and not a consideration, the determination of the price should by its nature remain insensitive to mercantilist logic and respond exclusively to public reasons.

On a dogmatic level, then, the systematic interpretation of the entire regulation leads us to conclude that anonymization (or pseudonymization) does not seem *ex se* sufficient for the full taxonomic transfusion of anonymized data in the category of "non-personal digital health data" positivized by the European legislator. Therefore, the new regulations on the

to identify such a person, without requiring that all information from which such person can be identified be in the hands of a single entity". Even according to the judges, the anonymization of the data is not suitable to eliminate the personal nature of the same.

41 On a practical level, if access to pseudonymised data is granted, the decryption key of the same useful for the re-identification of the data subjects will be held either by the data access bodies themselves or by a reliable third party designated under national law.

42 About critics' points on theme see J. Thomason, *Big tech, big data and the new world of digital health,* in Global Health Journal, 5, 2021, 165; nonchè C. Dantas, K. Mackiewicz, *Are we ensuring a citizen empowerment approach for health data sharing?*, in A. Cartolovni and others, *Proceedings of the 2022 Good Brother International Conference on Privacy-friendly and Trustworthy Technology for Society*, Zagreb 2022, 55.

43 On the marketability of personal data, two doctrinal approaches must be highlighted. One (B. Custers, G. Malgieri, *Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data*, in Computer Law & Security Review*,* 2022, 45; S. Yakovleva, K. Irion, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation,* in American Journal of International Law, X, 2020, 114,) which, by bringing the protection of personal data back to the cases of fundamental human rights referred to in art. 8 of the Charter of Fundamental Rights, denies the availability of the legal positions in question to the interested parties; the other (B. Rossler, *Should personal data be a tradable good? On the moral limits of markets in privacy,* in *Social dimensions of privacy: Interdisciplinary perspectives* (eds.) B. Rossler – D. Mokrosinska, Cambridge, 2015, 141; M. Mursia, C. A. Trovato, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in Media Laws*,* 2, 2021, 165; F. Ferretti, *Directive (EU) 2019/770: personal data as consideration in contracts for the supply of digital content and digital services and the inherent impact on privacy law,* in Actualidad Juridica Iberoamericana*,* XVI, 2022, 1740; D. Poletti, *Le condizioni di liceita del trattamento dei dati personali*, in Giur. It*.,* 2019, 2783; R. Senigaglia, *La dimensione patrimoniale del diritto alla protezione dei dati Personali*, in Contr. impr., II, 2020, 760), denying the absoluteness of the right in question, admits the marketability of the personal data provided that compliance with adequate processing to protect the right to privacy of the data subjects is guaranteed.

re-use of health data seem to conform to that more guaranteeist position that for some time has tended to exclude the possibility of eliminating in an absolute and incontrovertible way the danger of re-identification of the data subject by the data controller or third parties[44].

## V. Robust governance tools for electronic health data: the secure processing environment, limits on the misuse of access to data.

Once the phase of "depersonalization" of the data has been overcome, the further steps of the procedure are also surrounded by precautions aimed at protecting the confidentiality of the data subjects. Pursuant to art. 73 of the Regulation, the sharing of data takes place with their entry into a "secure" processing environment, a place where the material access to the data by the applicant is witnessed.
In order to reconcile the implementation of the strategic purposes related to the re-use of data with compliance with the principle of transparency, a public register shall be set up at each body showing both the access requests submitted by users, accompanied by the specific purposes for which access has been granted, and the (descriptions of) the data sets made available to the authorized user. The advertising obligation is of considerable importance as it guarantees control over the consultation of the data provided and the verification of compliance with the rules relating to their processing. For the writer, the publicity of such news could perform an important function on a transnational level, as through the construction of interoperable mechanisms designed *ad hoc* for the exchange of information between the various bodies of access to the data of the EHDS, or through a functional implementation of those already provided for by the regulation, it would be possible for each entity to ascertain whether a user has already obtained the access to the requested data or even whether this access has been denied to him and for what reasons. This would prevent the refusal of a data authorization from being circumvented by making the same request to a body operating in another Member State, or from the user being able to have access to the same data set for a longer period. This is clearly a *de jure condendo* perspective since, to date, Article 59 of the Regulation provides for each body responsible for governance only the obligation to carry out a biennial report on the activity carried out; moreover, the effectiveness of such an instrument presupposes that the individual data access bodies record and communicate not only the authorizations but in particular the measures of refusal to the data and the respective justifications. There is also the question of what the margins of binding nature may be for each body concerning any denials decreed by similar bodies[45]. In this regard, it would be useful to provide for a specific means of appeal against the refusal measure - or even a decision-making body - at "EU" level with binding effects throughout the European health data space, capable of avoiding differences in judgment or unequal treatment between individual member states.

[44] C. Gallese, *The Risks of Health Data Commodification in the EU Digital Market,* in Yearbook of Antitrust and Regulatory Studies, XXIX, 2024, 89.
[45] A more precise indication will certainly be obtained from compliance by 26 March 2027 with the obligation for the European Commission, provided for by art. 70 of the Regulation, to create standardized models for access to electronic health data.

The construction of the secure sharing space of data datasets is the prerogative of the body and is clearly part of the tasks congenial to its nature as a data controller. Art. Article 73 of the Regulation provides for the indefectible characteristics of the environment in question by providing for specific security measures suitable for making it a closed and controlled system. It is therefore required to adopt technical precautions to neutralize abuses such as the use of data for purposes other than those for which one is authorized, or access to data by unauthorized parties.

The security of the processing environment fulfils the "political" purpose of re-use, as it aims to ensure that the use of sensitive data such as health data is effectively intended to achieve altruistic purposes that justify a derogation from the ordinary legal basis for the processing of the data subject's data. In this sense, according to letter d) of the aforementioned Article 73, the environment is secure only if the user is able to access only the requested data, any possibility of abusive use of the shared data is then excluded since it is impossible to take "personal" health data from the environment; In fact, the user is allowed to export to an environment other than that of sharing only non-personal data or those provided in anonymised statistical form, unable to re-identify the data subjects. Of extreme interest is the need for the environment to be structured in such a way as to prevent the user from copying, modifying and deleting the data to which he has access; These prerogatives seem to correspond to the implementation of the principle of privacy protection by design, as they guarantee the adoption of a protective technological structure already in the design phase of the data sharing system. The safety of the environment was provided not only by resorting to privacy by design but also by limiting access to the processing environment in a time. In fact, by setting a maximum duration for users to consult the datasets, the European legislator, in addition to ontologically "filling" the principle of proportionality, has at the same time put a stop to the risk of reprocessing the shared data that a dilated time availability on the part of the same user could have generated.

The security of the environment, as well as teleologically, is also declined on a subjective level as the provision of art. 73 aims to prevent the data shared in the secure environment from being circulated in favor of subjects other than those authorized. In the absence of technical precautions, it would be possible for the user to "cede" access to the secure processing environment - and therefore to the data - to subjects to whom authorization has been denied, has expired, or in any case has been granted for other types of data or to process data in an anonymized rather than pseudonymized form. Already at the time of submission of the request, the user is required to indicate in a precise and detailed manner the identity of the natural persons in charge of processing the data and, once the measure has been obtained, only these subjects will be allowed access to the processing environment. This will take place according to a double track operating *ex ante* through procedures of entry into the environment by means of personal identification keys; and *ex post* through the recording of every single operation carried out by the authenticated and identified subject in the secure processing environment. The history of the activities carried out ends up becoming a deterrent to the improper use of access data to the secure environment, and at the same time constitutes an effective tool for ascertaining any abuses

and responsibilities in the secondary management of the data made accessible, favoring a reasonable application of any sanctions imposed.

## VI. THE FIGURE OF THE "RELIABLE OWNER".

In the context of the reuse of health data, a final mention should be made of the figure of the "reliable" data holder, i.e. a data holder who, in the light of certain subjective peculiarities and, as a result of an investiture by the individual Member State, is considered suitable for the autonomous management of access requests concerning the data held by him. Thanks to the absence of intermediation by central bodies, if the user intends to use the data in the possession of these figures, the procedural *process* must be initiated directly against the data subject, with the consequence that the subject in question will also become the data controller for secondary use and the data processor for the data granted for use to the applicant. On an operational level, the simplified procedure for access to data in which the reliable controller is present does not derogate from the precautions provided for by the regulation, which are intended to be fully applicable to that entity as well. However, while the provision of a secure processing environment for data sharing seems to be an essential obligation even for the reliable controller, a different argument should be made with regard to the internal structuring of the same. In the opinion of the writer, in fact, the need to equip oneself with a corporative organization capable of guaranteeing horizontal functional autonomy should not be considered indefectible in the hypothesis *in question*. A careful reading of the data authorization procedure highlights how the request for access to the datasets addressed to the reliable data controller does not end with a properly authorizational measure, but rather takes the form of an opinion accompanied by a proposal for a decision; a proposal that must in any case be passed to the scrutiny of the data access body, which can ratify it or deviate both from it and from the opinion issued by the reliable owner. The decision-making process, while not affecting the legal nature that the reliable data controller assumes in the context of the processing, nevertheless guarantees that the authorization measure is in any case the result of an assessment by the data access body (with mere control functions), thus allowing us to dispel any doubts about the presence of potential conflicting interests. On the contrary, the possibility of issuing a decision that differs from that proposed by the reliable owner could be justified precisely in the possible presence of a conflict of interest that the reliable owner by his nature is unable to overcome. Ultimately, for reliability, in the absence of an express provision of the regulation, it does not seem possible to include among the characteristics of the controller, the adoption of a corporate structure as specified by the regulation for data access bodies.

## VII. BRIEF CONCLUDING REMARKS

The framework outlined by the European legislator for the governance of health data for secondary use, as repeatedly emphasized, is the result of a delicate and declared compromise between political objectives driven by the ambition to channel the data market along the lines of altruism and the collective interest, and the need to legally protect

individual subjective interests. Balancing these concerns must take into account a fundamental circumstance: the space of health data created by the new regulation is not conceived as a physical reality, but has a purely digital dimension. It follows that to ensure the efficient development of the EHDS and its governance, it is essential to respect those prerogatives that for twenty years have become axioms of the correct creation and dissemination of digital data. The latter, as is well known, presupposes the essential existence of a medium—the electronic document—capable of maintaining reliability, authenticity, integrity, legibility, and retrievability over time. Well, it is therefore appropriate to highlight how only through an accurate and meticulous respect of these characteristics, the greater the informative potential of the electronic health data will be and the higher the possibilities of implementing the altruistic purposes favored by its secondary use will be.

# CONTRADICTIONS OF TWIN TRANSITIONS: THE ENVIRONMENTAL IMPACT OF AI SYSTEMS FROM THE EUROPEAN UNION PERSPECTIVE

*Gioia Codognotto*

TABLE OF CONTENTS:


*The paper examines the environmental impact of AI systems from the perspective of the European Union, placing the issue within the broader context of the twin transitions, namely the green transition and digital transition, promoted by European institutions through various initiatives, policies and legislative acts. As an introduction, some data on the environmental impact of AI systems will be presented, followed by an analysis of the relevant European legal framework, and concluding with a discussion of the opportunities offered by the digital transition, specifically through AI, in order to identify potential solutions to the challenges outlined.*

**Keywords:** Twin Transitions; AI Systems; Environmental Impact; EU Regulatory Framework; Challenges & Opportunities.

## I. INTRODUCTORY PREMISES

In the present moment, the European Union is facing a complex challenge, identified in the increasing use of Artificial Intelligence systems by all social actors, to which it is attempting to respond through various policies and initiatives. However, these measures only partially harness the potential of technological advancement for environmental sustainability and, in most cases, fail to contain the negative effects of Artificial Intelligence use on the environment. Accordingly, the present research aims to demonstrate this regulatory gap and to analyze its implications from a legal and factual perspective, with a view to examining possible strategies to address the highlighted challenges.

As a preliminary step, some definitions must be provided. First and foremost, the term Artificial Intelligence (hereinafter AI) refers to a type of Information and Communication Technology (hereinafter ICT), capable of performing tasks typical of human cognitive functions, with the aim «to generate outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension»[1]. This definition has also been endorsed by the European

[1] See C. A. Ciaralli, *Intelligenza artificiale, decisione politica e transizione ambientale: sfide e prospettive per il costituzionalismo*, available at https://federalismi.it/nv14/articolo-documento.cfm?artid=49045 (last visited Jul. 24, 2025), p. 44 ff.; C. Di Francesco Maesa, *Economia circolare e IA: a che condizioni è una sfida possibile per l'UE?*, available at

Commission, which describes AI as a set of «systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals»[2].

Against the backdrop briefly described – characterized by both the growing use of AI and the European Union's partial regulatory response – the concept of the twin transitions has emerged, namely the green and digital transition, two key objectives that have shaped European policy in recent years. When examined in relation to each other, these transitions necessarily prompt a more in-depth reflection on technological progress, particularly regarding the environmental impact of AI. Indeed, the practical application of AI tools across various economic and industrial sectors has led to clear simplifications and efficiencies, for example in terms of resource management optimization, automation of repetitive processes, investment predictability and personalization of products and services offered to the public. Nevertheless, at the same time, the implementation of such technologies carries multiple risks with significant consequences for human life and health, foremost among them the environmental concerns, that this research seeks to explore. In this regard, the physical dimension of AI involves data centers, namely fiber optic cables and other infrastructure spread across various parts of the globe, that enable both the training and subsequent functioning of AI. However, these infrastructures require enormous amounts of energy and water to operate and to be cooled effectively.

The tangible nature of these environmental issues becomes clear when considering aspects such as the underwater space through which cables are laid, the airspace used for data transmission via satellites and antennas, the territories where raw materials and valuable natural resources are extracted, or the areas where electronic waste is deposited, added to the massive consumption of water and energy at the expenses of developing countries[3].

It is therefore clear that the scenario outlined above contributes to worsening climate change, which has now become an increasingly serious and urgent issue. This is evidenced by extreme weather events, such as droughts, wildfires, flooding and sea-level rise: all phenomena that are expected to increase further in the coming years as the global temperatures continue to rise above pre-industrial levels (currently at 1.1°C). This trend persists despite a 2018 report

https://www.aisdue.eu/costanza-di-francesco-maesa-economia-circolare-e-ai-a-che-condizionie-una-sfida-possibile-per-lue/ (last visited Jul. 24, 2025), p. 5 ff.; European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, 21.4.2021, COM(2021) 206 final, p. 18, par. 6; A. Nordgren, *Artificial intelligence and climate change: ethical issues*, available at https://www.emerald.com/jices/article/21/1/1/432616/Artificial-intelligence-and-climate-change-ethical (last visited Jul. 24, 2025), p. 2 f.; A. L. Stein, *Artificial Intelligence and Climate Change*, available at https://scholarship.law.ufl.edu/facultypub/996/ (last visited Jul. 24, 2025), p. 891 ff.; L. G. Sciannella, *Intelligenza artificiale, politica e democrazia*, available at https://www.dpceonline.it/index.php/dpceonline/article/view/1577 (last visited Jul. 24, 2025), p. 338 ff.

[2] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence For Europe*, 25.4.2018, COM(2018) 237 final, p. 1.

[3] For an overview of the environmental issues caused by AI, see P. Li, J. Yang, M. A. Islam, S. Ren, *Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models"*, available at https://arxiv.org/pdf/2304.03271 (last visited Jul. 24, 2025).

by the United Nations Intergovernmental Panel on Climate Change (IPCC), which emphasized that limiting global warming to 1.5°C is absolutely essential in order to reduce the impact of climate change on ecosystems, human health, and overall well-being[4].

As previously mentioned, the search for a balance between the twin transitions has become a crucial issue for the European Union, which has responded through a series of measures aimed at reducing the environmental impact of technological progress. The strategy implemented by the EU to address these challenges is grounded in a change of perspective on environmental matters, including in daily life habits, that emphasizes the importance of adopting long-term solutions capable of generating positive effects over time, to the benefit of future generations[5].

[4] Intergovernmental Panel on Climate Change (IPCC), *Special Report: Global Warming of 1.5°C*, available at https://www.ipcc.ch/sr15/ (last visited Jul. 24, 2025), Chapter 3. Further insights on climate change and environmental protection can be found in U. Beyerlin, J. Grote Stoutenburg, *Environment, International Protection*, in R. Wolfrum (under the direction of), *The Max Planck Encyclopedia*, p. 461-483 (Vol. II, Oxford University Press, Oxford, 2012); G. Cataldi, *Ambiente (tutela dell') (DCE)*, in *Enc. giur. Treccani*, p. 1 ff. (Vol. IV, Istituto della Enciclopedia italiana, Roma, 2004); M. Gestri, *Ambiente (dir. int.)*, in S. Cassese (diretto da), *Diz. dir. pubbl.*, p. 214-229 (Vol. I, Giuffrè, Milano, 2006); O. C. Ruppel, *Intersections of Law and Cooperative Global Climate Governance – Challenges in the Anthropocene*, in O. C. Ruppel, K. Ruppel-Schlichting, C. Roschmann (eds.), *Climate Change: International Law and Global Governance: Volume II: Policy, Diplomacy and Governance in a Changing Environment*, p. 35-100 (1st ed., Nomos Verlagsgesellschaft mbH, 2013), available at http://dx.doi.org/10.5771/9783845242774 (last visited Jul. 30, 2025); P. J. Sands, I. Millar, *Climate, International Protection*, in R. Wolfrum (under the direction of), *The Max Planck Encyclopedia*, p. 236-247 (Vol. II, Oxford University Press, Oxford, 2012); P. Sands, J. Peel, A. Fabra, R. MacKenzie, *Principles of International Environmental Law*, p. 195 ff. (4th ed., Cambridge University Press, Cambridge, 2018); G. Tamburelli, *Ambiente (tutela dell') (dir. int.)*, in *Enc. giur. Treccani*, p. 1 ff. (Vol. IV, Istituto della Enciclopedia italiana, Roma, 2004).

[5] On these topics, see European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank. A Clean Planet for All. A European Strategic Long-Term Vision for a Prosperous, Modern, Competitive and Climate Neutral Economy*, 28.11.2018, COM(2018) 773 final e V. Zampaglione, *Climate change: towards global law?*, available at https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/2100 (last visited Jul. 24, 2025), p. 2 ff., which highlights the need to address climate change through shared principles and rules. As for environmental sustainability, policies aimed at sustainable development, with the dual objective of preserving ecosystems to meet the needs of both the present and the future, date back to earlier times, originating with the 1987 Brundtland Report *Our Common Future*, published by the World Commission on Environment and Development (WCED).
Over the years, key milestones have included the Conference of the Parties (COP), which have gained increasing influence on climate matters and led to the adoption of a universal climate agreement at COP21 in 2015 (*Paris Agreement*), later renewed in 2021 through the *Climate Pact* at COP26 in Glasgow.
For an overview of these topics, see G. Cataldi, *Ambiente (tutela dell') (DCE)*, cit., p. 1 ff.; M. Gestri, *Ambiente (dir. int.)*, cit., p. 215 ff. See also M. C. Gaeta, *Intelligenza artificiale sostenibile e tutela dei green rights*, available at https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/2055 (last visited Jul. 24, 2025), p. 150 ff., which also references the UN 2030 Agenda for Sustainable Development (*Transforming Our World: the 2030 Agenda for Sustainable Development*), signed by the governments of the 193 UN Member States in September 2015 and comprising 17 Sustainable Development Goals (SDGs).
The full text is available on the official website of the United Nations at the following link: https://sdgs.un.org/2030agenda. A more recent interpretation of environmental sustainability is the one that emphasizes the shift from a linear economy model to a circular economy model. On this topic, see, among others, E. Chiti, *Verso una sostenibilità plurale? La forza trasformatrice del Green Deal e la direzione del cambiamento giuridico*, in Riv. quadr. dir. amb. (III, 2021); A. D'Aloia, *Prefazione*, in M. Cocconi (a cura di), *La regolazione dell'economia circolare: sostenibilità e nuovi paradigmi di sviluppo*, 9-12 (Franco Angeli, Milano, 2020).

## II. THE ENVIRONMENTAL COSTS OF AI

Before delving into the policies and initiatives adopted by the European Union in the context of the green and digital transition, the following section presents some data concerning environmental pollution caused by the implementation of AI technologies, data that help underscore the urgency of addressing these issues, which can no longer be overlooked.

From the design phase onward, it must be acknowledged that the development of AI systems entails significant environmental costs, primarily linked to the extensive use of natural resources. Over the past fifty years, global resource extraction has tripled, a trend expected to continue in the coming decades. In particular, the production of AI hardware and related infrastructure relies on the extraction of rare and valuable raw materials – such as cobalt, palladium, silver, gold, indium, lithium and aluminum – with the associated environmental and social repercussions, especially in developing countries. In fact, these impacts are often felt in regions hosting resource extraction and data center infrastructures, frequently located outside high-income countries, resulting in damage to local ecosystems and the depletion of natural resources[6].

Moreover, the production of the devices necessary for AI operation involves not only the extraction of raw materials, which, as mentioned, is already environmentally harmful, but also the environmental cost of transporting these materials: from the mining sites to component manufacturing facilities, then to other factories where the end-products are assembled, and finally to the AI developers and users. As is evident, each step in the production chain results in greenhouse gas emissions, which must therefore be counted among the total emissions attributable to AI[7].

For what concerns the functioning of AI systems, then, the servers on which they rely generate massive energy consumption. This is due to the need to power extremely powerful machines capable of performing highly complex computations, consumption which, in turn, results in significant greenhouse gas emissions, thereby contributing to global warming.

Some of the already recorded data on energy consumption are as follows: in 2018, the global energy consumption of data centers across the entire ICT sector rose to 205 TWh, accounting for approximately 1% of global electricity use; this consumption increased to 460 TWh in 2022. According to some estimates, by 2026, the total electricity consumption caused by data centers could exceed 1,000 TWh, roughly equivalent to the total electricity consumption of Japan[8].

---

[6] C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 15 ff. For relevant data on the subject, see H. Roberts, J. Zhang, B. Bariach et al., *Artificial intelligence in support of the circular economy: ethical considerations and a path forward*, available at https://link.springer.com/article/10.1007/s00146-022-01596-8 (last visited Jul. 24, 2025), p. 1451.

[7] In this sense, K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, 23-51 (Yale University Press, New Haven and London 2021); A. Nordgren, *Artificial intelligence and climate change*, cit., p. 3 f.

[8] The figures mentioned are the estimates of the International Energy Agency, *Electricity 2024. Analysis and forecast to 2026*, available at https://www.iea.org/reports/electricity-2024 (last visited Jul. 24, 2025), p. 8. See also F. Camisa, *Ambiente e tecnologia: l'interconnessione tra le 'transizioni gemelle'*, available at https://www.federalismi.it/nv14/articolo-documento.cfm?artid=50685 (last visited Jul. 24, 2025), p. 61 ff.; E. Masanet, A. Shehabi, N. Lei, S. Smith, J. Koomey, *Recalibrating global data center energy-use estimates. Growth in energy use has slowed owing to efficiency gains that smart policies can help maintain in the near term,* available at

Another critical issue closely connected to energy consumption is the enormous water usage required by AI models. Water is first used to generate the electricity needed to power these systems and is thereafter required to cool the servers; by way of example, as early as 2023, one study estimated that ChatGPT consumed approximately 500 ml of water for every 20 to 50 simple question-and-answer interactions. This level of consumption must be understood in the context of increasing global water scarcity and unequal distribution, which threaten water security worldwide[9].

Regarding greenhouse gas emissions, studies based on 2015 data have already shown that the ICT sector was responsible for 1.4% of global greenhouse gas emissions a decade ago. According to some estimates, this percentage could rise to as much as 23% by 2030. One study specifically focusing on AI as a contributor to climate change revealed that training a single AI model for Natural Language Processing (NLP) generates approximately 300,000 kg of carbon dioxide, approximately equivalent to the emissions of 125 round-trip flights from New York to Beijing[10].

Beyond the operational phase, the final stage in the life cycle of AI systems – the disposal of electronic devices – raises additional environmental concerns related to the improper handling of electronic waste (e-waste). Several studies have confirmed that, in most cases, electronic waste, including that generated by AI technologies, is neither properly disposed of nor adequately recycled, releasing toxic substances into ecosystems with serious consequences for both human health and the environment. According to recent research, only 22% of electronic waste is recycled in an environmentally sustainable manner: this raises the critical question of what happens to the remaining portion, which unfortunately represents the vast majority of discarded material[11].

## III. AI WITHIN THE EUROPEAN LEGAL FRAMEWORK: THE DELICATE RELATIONSHIP BETWEEN THE TWIN TRANSITIONS

The European Union's action in the field of environmental sustainability is based on specific provisions of the Treaty on the Functioning of the European Union (TFEU), in particular

https://www.science.org/doi/10.1126/science.aba3758 (last visited Jul. 24, 2025), p. 984-986; A. L. Stein, *Artificial Intelligence and Climate Change*, cit., p. 917 f.

[9] C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 10 ff.; P. Li, J. Yang, M. A. Islam, S. Ren, *Making AI Less "Thirsty"*, cit., p. 5 ff.

[10] For the study mentioned see M. Coeckelbergh, *AI for climate: freedom, justice, and other ethical and political challenges*, available at https://link.springer.com/article/10.1007/s43681-020-00007-2 (last visited Jul. 24, 2025), p. 68 f. On these topics see also A. S. G. Andrae, T. Edler, *On Global Electricity Usage of Communication Technology: Trends to 2030*, available at https://www.mdpi.com/2078-1547/6/1/117 (last visited Jul. 24, 2025), p. 143 f.; J. Cowls, A. Tsamados, M. Taddeo, L. Floridi, *The AI gambit*, cit., p. 290 ff.; J. Malmodin, D. Lundén, *The Energy and Carbon Footprint of the Global ICT and E&M Sectors 2010–2015*, available at https://www.mdpi.com/2071-1050/10/9/3027 (last visited Jul. 24, 2025), p. 1 ff.; A. Nordgren, *Artificial intelligence and climate change*, cit., p. 3 f.; A. van Wynsberghe, *Sustainable AI: AI for sustainability and the sustainability of AI*, available at https://link.springer.com/article/10.1007/s43681-021-00043-6 (last visited Jul. 24, 2025), p. 213 f.

[11] C. P. Baldé, R. Kuehr, T. Yamamoto et al., *The Global E-Waste Monitor 2024*, available at https://ewastemonitor.info/wpcontent/uploads/2024/03/GEM_2024_1803_web_page_per_page_web.pdf (last visited Jul. 24, 2025); F. Camisa, *Ambiente e tecnologia*, cit., p. 59; C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 13 ff.; M. C. Gaeta, *Intelligenza artificiale sostenibile*, cit., p. 148 ff.

Article 11 and the articles contained in Title XX (artt. 191-193), which are explicitly dedicated to the Union's environmental policies. Article 11 TFEU, confirming the principles already expressed in Article 37 of the Charter of Fundamental Rights of the European Union (Nice Charter), states that environmental protection requirements must be integrated into the definition and implementation of the Union's other policies and activities (integration principle), particularly with a view to promoting sustainable development. Article 191(1) TFEU further sets out the objectives of environmental policy, including the protection of human health, the prudent and rational use of natural resources, the promotion of international measures to tackle environmental problems at regional or global level and, notably, the fight against climate change[12].

However, the legal foundations mentioned are proving to be insufficient and outdated in addressing the new environmental challenges posed by the climate emergency, which the European Union could confront more effectively only if the Treaties were revised and supplemented with more detailed and binding provisions in this field. Furthermore, Article 11 TFEU and Article 37 of the Charter, lay down criteria for assessing the EU's activities that are too vague to allow individuals to determine whether, in environmental matters, the European institutions have complied with the principle of integration between environmental protection and the European policies and initiatives[13].

Despite these normative shortcomings, the EU has taken targeted measures to respond to the environmental impacts of digitalization, embedding them within the broader twin transition strategies, with the *European Green Deal* and *Europe's Digital Transformation* serving as foundational pillars of the Commission's 2019-2024 agenda.

Firstly, on 11 December 2019 the European Commission presented the *European Green Deal* (hereinafter also EGD), a package of measures aimed at achieving climate neutrality by 2050. This goal is to be reached through a compensation mechanism intended to offset greenhouse gas emissions with their simultaneous absorption by forests, alongside biodiversity conservation, decarbonization, promotion of the circular economy[14], and the development

---

12 A. Festa, *Verso l'obiettivo climatico del 2030: su alcuni sviluppi attuativi del Green Deal europeo attraverso norme vincolanti. Il pacchetto "Fit for 55%"*, available at https://rivista.eurojus.it/wp-content/uploads/pdf/qui-35.pdf (last visited Jul. 24, 2025), p. 119 ff.; M. C. Gaeta, *Intelligenza artificiale sostenibile*, cit., p. 151 ff. For a detailed examination of the aforementioned articles, see S. Amadeo, *Art. 11 TFUE*, in A. Tizzano (a cura di), *Trattati dell'Unione europea*, p. 407-414 (2nd ed., Giuffrè, Milano, 2014); *Id.*, *Art. 191 TFUE*, *ibid.*, p. 1616-1637; *Id.*, *Art. 192 TFUE*, *ibid.*, p. 1638-1647; *Id.*, *Art. 193 TFUE*, *ibid.*, p. 1647-1650; M. Onida, *Art. 37 Carta*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, p. 691-707 (Giuffrè, Milano, 2017); P. A. Pillitu, *Art. 11 TFUE*, in F. Pocar, M. C. Baruffi (a cura di), *Commentario breve ai Trattati dell'Unione europea*, p. 173-175 (2nd ed., CEDAM, Padova, 2014); *Id.*, *Art. 191 TFUE*, *ibid.*, p. 1107-1112; *Id.*, *Art. 192 TFUE*, *ibid.*, p. 1112-1115; *Id.*, *Art. 193 TFUE*, *ibid.*, p. 1115-1116; *Id.*, *Art. 37 Carta*, *ibid.*, p. 1752. Moreover, according to authoritative scholarship, within the European legal framework the tension between economic development objectives and environmental protection should be addressed through the integration principle enshrined in Article 11 TFEU. This provision, in fact, confirms the cross-cutting nature of environmental protection and allows for a reconciliation of these competing interests from the perspective of sustainable development, by integrating environmental concerns into the European Union's policies across various economic sectors. In this regard, see again S. Amadeo, *Art. 11 TFUE*, *ibid.*, p. 408 f.

13 S. Amadeo, *Art. 11 TFUE*, *ibid.*, p. 411.

14 For the gradual shift from the linear economy paradigm to that of the circular economy in the context of the ecological transition, see M. Cocconi, *Il mosaico dell'economia circolare: Regole, principi, modelli*, 25 ff. (Franco Angeli,

of clean technologies, thus reducing environmental impact and safeguarding citizens' health[15].

More specifically, with a view to fostering economic and technological growth based on sustainability, the European Commission defined the EGD as **«**a new growth strategy aimed to transform the EU into a fair and prosperous society, with a modern, resource-efficient and competitive economy, where there are no net emissions of greenhouse gases in 2050 and where economic growth is decoupled from resource use**»**[16]**.**

Shortly after its adoption, the trajectory of the European Green Deal intersected with the outbreak of the COVID-19 pandemic. In response, during the summer of 2020, the European Union launched the *EU Recovery Plan* (known as *Next Generation EU*, or NGEU), a major recovery initiative designed to help Member States address the economic and social consequences of the pandemic, with a strong focus on promoting a greener and more digital Europe. Along the same lines, as an integral part of the Green Deal, in July 2021 the European Commission adopted *Fit for 55*, a package of proposals aligned with the aforementioned climate goals, with the specific aim of reducing greenhouse gas emissions by at least 55% by 2030. These projects, which position Europe as a global leader in the fight against climate change, were reaffirmed following the installation of the new Commission in 2024[17].

As for the digital transition, even prior to the pandemic, the European Union had already set itself the ambitious goal of achieving digital leadership, seeking to create the conditions necessary to make the Union technologically competitive while also respecting citizens' safety[18].

---

Milano, 2023); M. Montini, *Quali principi giuridici per l'economia circolare nell'Unione europea?*, available at https://www.dpceonline.it/index.php/dpceonline/article/view/2032 (last visited Jul. 24, 2025); L. Ricci, *La triade "rigenerazione, ambiente e consumo" nel "modello circolare"*, in Riv. quadr. dir. amb. (II, 2023).

15 European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Green Deal*, 11.12.2019, COM(2019) 640 final. On the *European Green Deal* see M. C. Carta, *Il Green Deal europeo. Considerazioni critiche sulla tutela dell'ambiente e le iniziative di diritto UE*, available at https://rivista.eurojus.it/wp-content/uploads/pdf/Il-Green-Deal-europeo.pdf (last visited Jul. 24, 2025); E. Chiti, *Managing the ecological transition of the EU: The European Green Deal as a regulatory process*, in Riv. quadr. dir. amb. (I, 2021); *Id.*, *Verso una sostenibilità plurale?*, cit.; E. Chiti, D. Bevilacqua, *Green Deal. Come costruire una nuova Europa*, 1 ff. (il Mulino, Bologna, 2024); J. Cowls, A. Tsamados, M. Taddeo, L. Floridi, *The AI gambit*, cit., p. 298 ff.; L. Fisher, *Challenges for the EU Climate Change Regime*, available at https://www.cambridge.org/core/journals/german-law-journal/article/challenges-for-the-eu-climate-change-regime/2AF8CF1DCFFBC5A2C4F5CC0E95D1310C (last visited Jul. 24, 2025), p. 5 ff.; M. E. Harris, *The normative values of the European Green Deal*, available at https://rivista.eurojus.it/wp-content/uploads/pdf/The-normative-values-of-the-Green-Deal.pdf (last visited Jul. 24, 2025); M. Montini, *La condizionalità della duplice transizione verde e digitale nel Recovery Fund dell'Unione europea*, available at https://www.rivistaianus.it/forum/covid-19/2020_06_26_Montini.pdf (last visited Jul. 24, 2025), p. 1 ff.; M. Onida, *Il Green Deal europeo*, in P. Manzini, M. Vellano (a cura di), *Unione europea 2020. I dodici mesi che hanno segnato l'integrazione europea*, 257-283 (Wolters Kluwer, Milano, 2021); C. Pesce, *Il Green Deal europeo e la neutralità climatica entro il 2050*, in L. F. Pace (a cura di), *Quo vadis Europa? Le sfide dell'Unione europea nel tempo delle crisi. Una riflessione multidisciplinare nel contesto della Conferenza sul futuro dell'Europa*, 359-371 (Edizioni Efesto, Roma, 2023).

16 European Commission, *The European Green Deal*, cit., p. 2.

17 F. Camisa, *Ambiente e tecnologia*, cit., p. 66; C. A. Ciaralli, *Intelligenza artificiale*, cit., p. 72; M. C. Gaeta, *Intelligenza artificiale sostenibile*, cit., p. 151 ff.; A. Festa, *Verso l'obiettivo climatico del 2030*, p. 122 ff.

18 J. Cowls, A. Tsamados, M. Taddeo, L. Floridi, *The AI gambit*, cit., p. 298 ff.; M. Montini, *La condizionalità della duplice transizione*, cit., p. 1 ff. See also European Commission, *Communication from the Commission to the European*

Given its dual nature, the digital transition must be closely linked to the green transition to ensure a balanced regulatory framework that reconciles environmental protection with technological development: whereas the green transition aims for climate neutrality by 2050 and emission reductions, rapid technological advancement inevitably contributes to carbon dioxide emissions, environmental waste, and global warming[19].
The need to integrate the EGD with the digital transition through the sustainable use of digital technologies was reiterated by the Commission in subsequent communications. Of particular note is the communication *Shaping Europe's Digital Future* of 19 February 2020, which emphasized how digital solutions can support the sustainability objectives of the green transition by promoting the circular economy, supporting the decarbonization of all sectors, and reducing the environmental and social footprint of products placed on the EU market[20]. This was followed by the *2022 Strategic Foresight Report: Twinning the green and digital transitions in the new geopolitical context*, issued in June 2022, which further addressed these same themes[21].
In light of these considerations, one can conclude by reinforcing the European Union's perspective that the regulation of the two transitions must be addressed jointly, through an integrated and synergistic approach in which the goals pursued by both are balanced and aligned[22].

## IV. The Implementation of the European Green Deal and AI

In the EGD, as previously mentioned, technological progress is intended to support long-term environmental sustainability. The communication explicitly states that digital technologies, including AI, «can accelerate and maximize the impact of policies to deal with climate change and protect the environment»[23]. This assertion was further supported in the *New Circular Economy Action Plan* of 11 March 2020, which added that new technologies,

*Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Commission Work Programme 2020. A Union that strives for more*, 29.1.2020, COM(2020) 37 final.
[19] F. Camisa, *Ambiente e tecnologia*, cit., p. 56 ff. On the convergence between the green and digital transitions, see M. Orofino, *La tutela dell'ambiente nella costruzione della società digitale europea*, in ASTRID Rassegna 387 (IV, 2024); M. Passalacqua, *Green deal e transizione digitale. Regolazione di adattamento a un'economia sostenibile*, in An. Giur. Ec. (I, 2022).
[20] In this sense, see European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Shaping Europe's Digital Future*, 19.2.2020, COM(2020) 67 final, p. 11 f.
[21] European Commission, *Communication from the Commission to the European Parliament and the Council. 2022 Strategic Foresight Report. Twinning the green and digital transitions in the new geopolitical context*, 29.6.2022, COM(2022) 289 final.
[22] Additionally, on 30 September 2025, the President of the European Commission, Ursula von der Leyen, announced that the EU would set new climate targets ahead of the COP30 summit, which took place in Belém in November 2025. The updated package aimed to strengthen the implementation of the EGD, with particular focus on reducing carbon dioxide emissions by 2040, promoting investment in renewable energy, enhancing energy efficiency, and developing a circular economy, thereby reconciling economic growth with environmental sustainability.
[23] European Commission, *The European Green Deal*, cit., p. 9.

particularly AI, «will not only accelerate circularity but also the dematerialization of our economy and make Europe less dependent on primary materials»[24].

Additionally, the Special Committee on Artificial Intelligence in a Digital Age (AIDA), a study commission established by the European Parliament during the 18 June 2020 plenary session with a 12-month mandate, confirmed the role of AI in its *Working Paper on Artificial Intelligence and the Green Deal*, asserting that AI systems are key tools for implementing the EGD, as they help to reinforce and facilitate the achievement of climate neutrality and the drastic reduction of harmful emissions[25].

Moving on to some of the EGD's concrete implementation measures concerning AI systems, the *European Climate Law*[26] must first be mentioned, that translated the EU's climate neutrality target by 2050 into a binding regulation. A reference to AI can be found in Article 3(3) of the regulation, which mentions the «best available and most recent scientific evidence» as a guiding principle for the European Scientific Advisory Board on Climate Change, an independent body that reviews and evaluates EU policies on the green transition to ensure their alignment with climate goals. The provision further strengthens the view of technological progress as a tool to mitigate the effects of environmental issues.

In terms of environmental sustainability, other implementing measures of the Green Deal include Regulation (EU) 2024/1991 on nature restoration[27] and Regulation (EU) 2024/1252 on critical raw materials[28]. While the EU's intention in the first case was to halt the degradation of ecosystems to rebuild them, some critical issues arise from the fact that, in this regulation, AI is mentioned only as a tool for monitoring the objectives set out therein (Article 20). As for the regulation on critical raw materials, although its aim is to ensure a more circular and sustainable supply of raw materials, it establishes a sustainability certification system involving certifying bodies and environmental standards that are often inadequate to protect local resources, especially in non-EU countries where most of the extraction activities take place[29].

Complementing these measures, Directive 2023/1791 on energy efficiency includes specific measures for data centers, recognizing their high energy consumption and environmental impact. These measures aim to promote energy-efficient technologies and monitor energy consumption, yet their actual effectiveness remains uncertain. The Directive prescribes reporting obligations and indicators for energy consumption, but implementation may vary

[24] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A New Circular Economy Action Plan. For a cleaner and more competitive Europe*, 11.3.2020, COM(2020) 98 final, p. 2.

[25] Special Committee on Artificial Intelligence in a Digital Age (AIDA), *AIDA Working Paper on Artificial Intelligence and the Green Deal*, March 2021, p. 2 ff.

[26] Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 (*European Climate Law*).

[27] Regulation (EU) 2024/1991 of the European Parliament and of the Council of 24 June 2024 on nature restoration and amending Regulation (EU) 2022/869.

[28] Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020.

[29] On the critical issues of the regulation on critical raw materials, see also C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 20 ff.

significantly across Member States, and, pursuant to Article 12, the current rules apply only to data centers above certain thresholds, excluding much of the on-site enterprise infrastructure. Furthermore, while systematic data collection could inform the development of sustainability indicators, greater coordination and support from national and regional authorities, involving sustainable energy agencies, would be pivotal for ensuring consistent application and promoting energy efficiency, as indicated in Recitals 38 and 39[30].
Finally, regarding electronic waste, another implementing act of the EGD worth mentioning is Regulation (EU) 2024/1157 on waste shipments[31], which mainly aims to monitor waste shipments within and outside the EU to prevent illegal disposal and environmental harm. However, despite the commendable intentions of the EU, the framework established by this regulation continues to clash with the persistent problem of illegal waste trade. According to recent data, between 15% and 30% of waste shipments are illegal: as a result, these shipments escape proper monitoring and carry a higher risk of improper disposal or treatment, thereby increasing their potential negative impact on the environment[32].

IV.1 *The Corporate Digital Responsibility*.

The deployment of AI technologies raises important questions about responsibility, notably with respect to their negative environmental impacts and who should bear accountability for these consequences. One possible answer is that responsibility should lie with those involved in the production or use of AI services, such as AI developers, tech workers, AI companies and governments, who should be transparent with the public on the emissions from training and deploying AI models. That said, it is also true that AI is used by consumers, who do not easily fit into this regulatory scheme, as unlike companies that develop and use AI services for profit, consumers act for non-commercial purposes.
While no clear answers have yet emerged, there have been some EU initiatives on corporate responsibility based on the principles of Article 191(2) TFEU, including the precautionary principle, preventive action, rectification at source, and the polluter-pays principle, which requires that those responsible for environmental damage bear the cost of environmental restoration[33].

[30] Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955 (recast).
[31] Regulation (EU) 2024/1157 of the European Parliament and of the Council of 11 April 2024 on shipments of waste, amending Regulations (EU) No 1257/2013 and (EU) 2020/1056 and repealing Regulation (EC) No 1013/2006 (*Waste Shipments Regulation*).
[32] C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 23 ff.
[33] For a detailed examination of the principles laid down in Article 191(2) TFEU, see S. Amadeo, *Art. 191 TFUE*, cit., p. 1622 ff.; P. A. Pillitu, *Art. 191 TFUE*, cit., p. 1109 ff. On Corporate Digital Responsibility see, *ex plurimis*, K. Crawford, *Atlas of AI*, cit., p. 41 ff.; M. C. Gaeta, *Intelligenza artificiale sostenibile*, cit., p. 155 ff.; C. J. Herden, E. Alliu, A. Cakici et al., *Corporate Digital Responsibility*, available at https://doi.org/10.1007/s00550-020-00509-x (last visited Jul. 24, 2025); L. Lobschat, B. Mueller, F. Eggers et al., *Corporate digital responsibility*, available at https://doi.org/10.1016/j.jbusres.2019.10.006 (last visited Jul. 24, 2025); A. Nordgren, *Artificial intelligence and climate change*, cit., p. 10; G. Schneider, *Le tecnologie societarie alla prova del governo sostenibile tra ESG, diligenza d'impresa e corporate digital responsibility*, available at

First and foremost, the *Corporate Sustainability Reporting Directive* (hereinafter CSRD) [34] introduces new sustainability reporting obligations for European companies, requiring them to issue a sustainability report based on ESG factors (Environmental, Social, and Governance), aimed at providing the public with information on the impact these companies have on the environment, and thus on a fundamental right. In practical terms, Corporate Digital Responsibility, through ESG reporting, considers several indicators under the Environmental factor, such as energy efficiency, greenhouse gas emission reduction, circular economy practices, management of e-waste, and the development of sustainable software. These indicators allow for an evaluation of the environmental impact arising from the production or use of AI systems by companies, as they cover the entire lifecycle of hardware, from production and operation to disposal and recycling of ICT devices and infrastructures[35]. Another key directive is the *Corporate Sustainability Due Diligence Directive* (CSDDD)[36], designed to make European companies more accountable for human rights violations and environmental harm across most phases of the AI systems' lifecycle, from production to distribution, transport, and storage of a product or the provision of a service. However, a limitation of the CSDDD lies in its focus on the earlier stages of a product's lifecycle: it does not require companies to assess the potential negative human rights or environmental impacts arising from the actual use of products and services that include AI systems and yet most harmful consequences linked to AI systems stem from their use (Article 3(1)(g))[37].

## V. THE AI ACT AND THE ENVIRONMENTAL PROTECTION

The application of AI technologies in the European Union is regulated by Regulation (EU) 2024/1689 (*Artificial Intelligence Act*, hereinafter the AI Act) [38], which represents the

https://www.rivistacorporategovernance.it/Article/Archive/index_html?ida=85&idn=10&idi=-1&idu=-1 (last visited Jul. 24, 2025).

[34] Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting (*Corporate Sustainability Reporting Directive*).

[35] Together with the Social and Governance factors, various aspects are taken into account, respectively, such as the social impact deriving from the use of digital products, like working conditions within the company, and all matters related to the company's management practices. For further insight into ESG factors and their inclusion in corporate sustainability reporting, see M. C. Gaeta, *Intelligenza artificiale sostenibile*, cit., p. 151 ff.

[36] Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859.

[37] C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 23 ff.

[38] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (*Artificial Intelligence Act*). For a legal perspective on the AI Act see M. Carta, *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, available at https://rivista.eurojus.it/il-regolamento-ue-sullintelligenza-artificiale-alcune-questioni-aperte/ (last visited Jul. 24, 2025); E. Cirone, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, available at https://www.aisdue.eu/wp-content/uploads/2024/06/Post-Enza-Cirone.pdf (last visited Jul. 24, 2025); M. Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, available at https://www.aisdue.eu/wp-content/uploads/2024/06/Post-Marco-Inglese.pdf (last visited Jul. 24, 2025); A. Volpato, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, available at https://www.aisdue.eu/wp-content/uploads/2024/06/Post-Annalisa-Volpato.pdf (last visited Jul. 24, 2025).

culmination of a series of initiatives supporting the development of trustworthy AI and aims to ensure both the safety of AI technologies and the protection of fundamental rights[39].
The EU Treaties contain no explicit provisions regarding environmental protection in connection with AI systems. However, among the general clauses that have served as the basis for regulatory action, we can mention Article 7 of the TFEU, which ensures coherence between the Union's policies, actions, and objectives while also affirming the principle of conferral of competences, and Article 11 of the TFEU, which provides for the integration of environmental protection into the Union's policies and actions, aligning with the principles set out in Article 37 of the Charter of Fundamental Rights[40].
Among the various steps that led to the adoption of the AI Act, the 2020 *White Paper on AI* initially stressed the importance of harnessing AI in support of the EGD and the fight against climate change, highlighting AI's potential to optimize resource use and energy consumption, and to guide environmentally positive choices. Nevertheless, it did not address the environmental impact caused by AI technologies themselves[41]. This aspect was instead considered in other contemporaneous documents, such as the 2019 *Ethics Guidelines for Trustworthy AI*, which identified respect for social and environmental well-being as a key requirement for making AI systems trustworthy. In this document, it is stated that AI systems should meet environmental sustainability standards throughout the entire supply chain, from design to final use by, for example, assessing resource use and energy consumption during the training phase, to enable the selection of less environmentally harmful options[42].
This path eventually led to the AI Act, which entered into force on August 1, 2024, as the world's first legally binding act governing the development, deployment and placing on the market of AI technologies. In its implementation, the AI Act is accompanied by the recent *AI Continent Action Plan*, a communication from the European Commission dated April 9, 2025, which outlines the next steps in the EU's AI strategy to become «a leading AI Continent». The Plan focuses on: (i) developing large-scale computing infrastructure, called AI Factories and Gigafactories, designed to promote scientific collaboration between researchers, entrepreneurs, and investors; (ii) improving access to high-quality data for AI innovators through targeted initiatives; (iii) advancing AI algorithm development and

[39] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Coordinated Plan on Artificial Intelligence*, 7.12.2018, COM(2018) 795 final; European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on boosting startups and innovation in trustworthy artificial intelligence*, 24.1.2024, COM(2024) 28 final. On the risk-based approach adopted in the AI Act for the assessment of AI systems, see V. D'Antino, *L'approccio basato sul rischio nell'AI Act: un nuovo paradigma di regolazione dell'intelligenza artificiale*, available at https://www.federalismi.it/nv14/articolo-documento.cfm?artid=52349 (last visited Jul. 24, 2025), p. 18 ff.
[40] For leading scholarly commentaries on the aforementioned articles, see S. Amadeo, *Art. 11 TFUE*, cit., p. 407-414; M. C. Baruffi, *Art. 7 TFUE*, in F. Pocar, M. C. Baruffi (a cura di), *Commentario breve ai Trattati dell'Unione europea*, p. 170-172 (2nd ed., CEDAM, Padova, 2014); M. Onida, *Art. 37 Carta*, cit., p. 691-707; P. A. Pillitu, *Art. 11 TFUE*, cit., p. 173-175; P. A. Pillitu, *Art. 37 Carta*, *ibid.*, p. 1752.
[41] European Commission, *White Paper on Artificial Intelligence - A European Approach To Excellence And Trust*, 19.2.2020, COM(2020) 65 final, p. 1 ff.
[42] Independent High Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, available at https://data.europa.eu/doi/10.2759/346720 (last visited Jul. 24, 2025).

promoting their adoption in strategic sectors to support industrial and scientific applications, public services, and uptake by SMEs, mid-sized enterprises, and public administrations; (iv) enhancing AI skills and literacy, promoting diversity, supporting education and research, and attracting and retaining talent from within and outside the EU; (v) leveraging the EU's single market, supported by the AI Act, to reinforce trust and security in AI while reducing fragmentation, with measures to ease compliance, particularly for smaller innovators[43].

However, the inadequacy of the AI Act in balancing environmental protection and technological development diverges from the intentions expressed in the preparatory documents preceding its adoption, which appeared to place greater emphasis on integrating digitalization within a green framework. As regards environmental protection in relation to AI systems, the references contained in the AI Act appear limited and insufficient to address the scale of environmental challenges and to ensure the ecological sustainability of such systems, as would be desirable[44].

In this respect, in Article 1(1) of the Regulation, environmental protection is merely mentioned in passing, stating that: «The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation».

Subsequently, Article 3(49)(d) sets an obligation for providers of general-purpose AI models to document the known or estimated energy consumption of the model, while providers of high-risk AI systems are required to report direct or indirect environmental harm and to consider such harm as serious incidents.

Environmental considerations are further reflected in Article 40(2), which foresees the development of standards «to improve AI systems' resource performance, such as reducing the high-risk AI system's consumption of energy and of other resources during its lifecycle, and on the energy-efficient development of general-purpose AI models».

A related concern arises from the use of general-purpose AI models with systemic risks, which, as provided in Articles 53(1)(a) and 112(6), may be subject to specific reporting obligations imposed by the Commission. These obligations, as set out in Annex XI, Section 1, aim to produce adequately measured and comparable information on the known or estimated energy consumption of the model. Yet, such reporting obligations only apply to the energy used during the development phase of the model and not during inference, meaning the actual use of the model is not considered. From this perspective, the use of AI systems, which involves processing inputs and data fed into the model to generate predictions or outputs, entails a significantly higher energy consumption than that required during their development.

---

[43] European Commission, *Proposal for a Regulation*, cit.; *Id.*, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. AI Continent Action Plan*, 9.4.2025, COM(2025) 165 final.

[44] P. Hacker, *Sustainable AI Regulation*, available at https://ssrn.com/abstract=4467684 (last visited Jan. 26, 2026), p. 20 f.

In addition to this, the provisions focus solely on the issue of energy consumption, without addressing other significant environmental impacts caused by AI that have already been highlighted, such as excessive water usage, pollution, and the high consumption of energy and water associated with the extraction of critical raw materials, or the lack of effective mechanisms to ensure the disposal of electronic waste[45].

Continuing through the provisions of the AI Act, Article 95(2)(b), echoing Recital 165, states that the European AI Office and Member States shall promote the drafting of codes of conduct for AI systems aimed at encouraging voluntary adherence to certain standards. These standards should include parameters such as the assessment and minimization of the environmental impact of AI systems as indicators of progress towards specific objectives. Nonetheless, the adoption of such codes of conduct is purely voluntary, meaning that they do not impose binding legal obligations on AI providers and deployers, who are more likely, in their economic activities, to prioritize profit over environmental concerns. For these reasons, the codes of conduct under Article 95 have been deemed inadequate for establishing coercive mechanisms that ensure their implementation[46].

Finally, Article 112(10) of the AI Act requires that the Commission may, where appropriate, submit proposals to amend the Regulation, considering several factors, including the impact of AI systems on health, safety, and fundamental rights, but without explicitly mentioning the environment. As can be observed, potential amendments to the Regulation aimed at protecting environmental sustainability could only be proposed by the Commission through an interpretation of this provision that includes environmental protection among the fundamental rights covered by the Fundamental Rights Impact Assessment (FRIA) of the regulation, a point that remains controversial in doctrine[47].

## VI. Concluding remarks: AI environmental challenges, opportunities, and possible solutions

As has been repeatedly emphasized, the use of AI is inherently ambivalent: while it can exacerbate challenges such as climate change, it also holds significant potential to advance the EU's environmental sustainability objectives. Some studies indicate that, in certain contexts, AI and ICT more broadly may generate environmental benefits that surpass their associated costs, highlighting the need to carefully consider and harness these positive applications, a few of which are discussed below.

To begin with, AI can help inform public decision-makers and private actors – including companies and individuals – about environmentally sustainable business practices and

45 In this sense, N. Alder, K. Ebert, R. Herbrich, P. Hacker, *AI, Climate, and Regulation: From Data Centers to the AI Act,* available at https://doi.org/10.48550/arXiv.2410.06681 (last visited Jul. 24, 2025), p. 3 ff.; C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 15 ff.; C. J. Wu, R. Raghavendra, U. Gupta et al., *Sustainable AI: Environmental Implications, Challenges and Opportunities*, available at https://doi.org/10.48550/arXiv.2111.00364 (last visited Jul. 24, 2025), p. 1 ff.

46 These critical issues have been highlighted by C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 15 ff.

47 For an overview of the scholarly debate on the inclusion of the right to a healthy environment among the fundamental rights protected by the Charter, see M. Onida, *Art. 37 Carta*, cit., p. 692 ff.

consumption habits, thereby guiding economic decisions and lifestyles toward greater responsibility, ethics, and sustainability. This role of AI would also further promote the economic paradigm of the circular economy across society, as AI could support the design of circular products, components, and materials, with more resilient and durable designs, ranging from urban buildings, bridges and infrastructure to consumer goods[48].

Still on the topic of circularity, the *European Parliament Resolution of 3 May 2022 on Artificial Intelligence in a Digital Age* states that AI systems have «the potential to benefit security of supply, especially in the operation, monitoring, maintenance and control of water, gas and electricity networks», thus helping to implement several of the European Union's circular economy principles, including ethical sourcing of raw materials, recycling of materials and waste reduction[49]. In addition, the resolution highlights that AI, in the energy sector, particularly through big data analytics, «can monitor, optimize and reduce energy consumption and production, as well as support the integration of renewable energies into existing electricity grids»[50].

Another significant function of AI is its predictive capability, which could process vast amounts of data to create environmental monitoring systems, tracking indicators such as temperature and carbon dioxide levels. This would enable more sustainable and rational management of resources, contribute to reducing greenhouse gas emissions, and provide a comprehensive overview of the climate situation to safeguard biodiversity, ecosystems, and forests[51]. Moreover, AI could assist in forecasting extreme weather events, such as storms, hurricanes, droughts, or flooding, mitigating their impacts and supporting planning in economic sectors like agriculture[52].

Nonetheless, the positive potential of AI must be balanced against its environmental impacts. As the data discussed above demonstrate, these impacts continue to aggravate ecological challenges as well as economic and social inequalities globally, particularly in less developed

---

[48] For further insight on these topics, see C. A. Ciaralli, *Intelligenza artificiale*, cit., p. 54; A. Nordgren, *Artificial intelligence and climate change*, cit., p. 5 f.; D. Rolnick, P. L. Donti, L. H. Kaack, *Tackling Climate Change with Machine Learning*, available at https://doi.org/10.48550/arXiv.1906.05433 (last visited Jul. 24, 2025); D. G. Victor, *How artificial intelligence will affect the future of energy and climate*, available at https://www.brookings.edu/articles/how-artificial-intelligence-will-affect-the-future-of-energy-and-climate/ (last visited Jul. 24, 2025).

[49] European Parliament, *European Parliament Resolution of 3 May 2022 on Artificial Intelligence in a Digital Age (2020/2266(INI))*, 6.12.2022, 2022/C 465/06, par. 41.

[50] European Parliament, *European Parliament Resolution*, cit., par. 40.

[51] For a more detailed analysis of these aspects, see. Aa. Vv., *The role of Artificial Intelligence in the European Green Deal* (study requested by the AIDA Committee), 16 ff. (Luxembourg, 2021); F. Camisa, *Ambiente e tecnologia*, cit., p. 68 f.; M. C. Gaeta, *Intelligenza artificiale sostenibile*, cit., p. 148 f.; A. Nordgren, *Artificial intelligence and climate change*, cit., p. 11; A. L. Stein, *Artificial Intelligence and Climate Change*, cit., p. 893 ff.; A. van Wynsberghe, *Sustainable AI*, cit.; S. Yadav, A. Samadhiya, A. Kumar, *Achieving the sustainable development goals through net zero emissions: innovation-driven strategies for transitioning from incremental to radical lean, green and digital technologies*, in *Resources, Conservation and Recycling*, available at https://doi.org/10.1016/j.resconrec.2023.107094 (last visited Jul. 24, 2025).

[52] On these topics see J. Cowls, A. Tsamados, M. Taddeo, L. Floridi, *The AI gambit*, cit., p. 284 ff.; C. Di Francesco Maesa, *Economia circolare e IA*, cit., p. 5 ff.; A. Naji Khallaf, N. Moneer Alqerafi, *Using AI to Help Reduce the Effect of Global Warming*, available at https://powertechjournal.com/index.php/journal/article/view/464 (last visited Jul. 24, 2025); A. Nordgren, *Artificial intelligence and climate change*, cit., p. 5 f.; D. Rolnick, P. L. Donti, L. H. Kaack, *Tackling Climate Change*, cit.

countries[53]. In view of these challenges and opportunities, this research now turns to the question of which solutions can promote what has been defined as an ethical, responsible, and sustainable use of AI[54].

In general, it is desirable for the European Union to strike a better balance between the objectives linked to the twin transitions by introducing more specific and binding regulations on the environmental impacts of digitalization and, more precisely, of AI. Indeed, rather than relying solely on transparency-based obligations, such as the disclosure of energy consumption or greenhouse gas emissions, a broader set of regulatory instruments at the EU level appears indispensable to effectively integrate environmental sustainability into AI governance[55].

Beyond this, a more nuanced and forward-looking approach could be envisaged, combining preventive forms of co-regulation and shared responsibility between public authorities, AI providers and deployers, intended to steer technological development towards environmentally sustainable outcomes before environmental harm materializes, covering, for example, product design and practices in supply chain management[56].

Thereafter, and as a complementary measure, another possible solution could consist of imposing penalties on those who use AI in ways that negatively affect the environment, such as causing pollution and other such harms, in line with the polluter-pays principle. However, the punitive approach appears to conflict with the fact that companies, within the EU's legal framework, are encouraged to adopt AI, and this raises the question of why they should be held accountable for the consequences of using a technology they are incentivized to implement.

Furthermore, there remains the issue of proving environmental harm, which is not easily achieved, particularly when such harm affects distant and developing countries[57]. Since one of the proposed solutions entails the imposition of penalties on actors whose use of AI causes environmental harm, the effectiveness of such an approach depends on the availability of reliable, transparent and comparable metrics capable of quantifying that harm. Nevertheless, at present, the environmental footprint of AI remains difficult to assess in a comprehensive manner; for instance, the indicators set out in Annex XI, Section 1 of the AI Act – applicable to AI models with systemic risks – focus primarily on energy consumption limited to the training phase, while overlooking other relevant impacts such as water use, raw material extraction, and electronic waste. This narrow focus risks underestimating the overall environmental costs of AI systems, particularly in the case of large-scale generative models, especially where such models qualify as AI models with systemic risks under the AI Act, as

53 On the economic and social inequalities that the ICT sector produces, see C. A. Ciaralli, *Intelligenza artificiale*, cit., p. 77 ff.; M. C. Gaeta, *Intelligenza artificiale sostenibile*, cit., p. 148 ff.; A. Nordgren, *Artificial intelligence and climate change*, cit., p. 9 ff.

54 F. Camisa, *Ambiente e tecnologia*, cit., p. 60 ff.; A. Nordgren, *Artificial intelligence and climate change*, cit., p. 4 ff.

55 P. Hacker, *Sustainable AI Regulation*, cit., p. 8 ff.

56 P. Hacker, *Sustainable AI Regulation*, *ibid.*, p. 22 f.

57 On the responsibility for environmental damage borne by high-income countries, see H. Sue, *Global Environment and International Inequality*, in S. Gardiner, S. Caney, D. Jamieson, H. Sue (eds.), *Climate Ethics: Essential Readings*, 101-111 (Oxford University Press, Oxford, 2010).

their deployment and repeated retraining entail significant and continuous resource consumption.

A possible way forward could therefore lie in the development of standardized, life-cycle-based assessment framework relying on composite indicators capable of capturing the overall environmental impact of AI systems beyond their development phase[58]. While such metrics may not allow for a perfectly accurate quantification of damage, they could nonetheless provide a solid basis for attributing environmental responsibility to actors exercising effective control over AI systems. This, in turn, could strengthen the enforceability of sanctioning mechanisms, including fines, corrective actions, compliance orders, temporary or permanent suspension of market placement or service, and, where appropriate, withdrawal of AI systems.

In light of the findings of this research, emphasis must be placed on the importance of ensuring the development of Sustainable AI, namely an AI that is fully compatible with the green transition. Against this backdrop, high-impact AI systems could be progressively integrated into existing environmental policy instruments, such as regulatory frameworks that set binding environmental standards and incentives that promote the development of greener technologies, thereby internalizing their ecological externalities and fostering technological innovation in support of broader sustainability objectives.

Within the EU framework, this approach would present institutions and Member States with the challenging task of carefully balancing the green and digital transitions, while simultaneously addressing the complex ethical and social questions raised by AI. By pursuing such a strategy, AI could be harnessed ethically, responsibly, and in alignment with the environmental sustainability goals promoted by the EU, ultimately serving as a tool to support both governance structures and society in confronting the increasingly urgent environmental challenges of our time[59].

[58] P. Hacker, *Sustainable AI Regulation*, cit., p. 23 f.

[59] European Parliament, *European Parliament Resolution*, cit., parr. 37-45 specifically dedicated to the relationship between AI and the EDG.

# THROUGH THE ARTIFICIAL INTELLIGENCE ACT: CROSS-SECTIONAL STUDY ON A PRO-INNOVATION LAW

*Gabriele Franco*[1]

TABLE OF CONTENTS:



*On August 1, 2024, Regulation (EU) 2024/1689 (the AI Act) entered into force, establishing the new EU regulatory framework for artificial intelligence (AI). This has reignited the debate on whether EU legislation support or, conversely, constrains innovation. Public and academic narratives about the AI Act's market impact often overlook a set of innovation-oriented measures provide by the law that could at least partially compensate for the potential restrictive effects arising from compliance obligations. This paper offers a cross-sectional study of the AI Act aimed at systematically identifying and examining those measures that are capable of supporting technological development, particularly in the business and workplace context. Methodologically, it introduces two conceptual categories to frame these measures, distinguishing between "explicit innovation measures" and "implicit innovation measures". Building on legal doctrine and empirical evidence from other regulated sectors, the article also advances a preliminary assessment of the likely effectiveness of these measures. The study also considers the proposed amendments to the AI Act contained in the Digital Omnibus on AI.*

**Keywords**: Artificial Intelligence Act - AI Act - pro-innovation regulation - regulatory sandboxes - AI literacy - risk-based approach - digital omnibus

## I. THE NEW EU LEGAL FRAMEWORK ON AI

On August 1, 2024, Regulation (EU) 2024/1689[2] came into force, establishing the new EU regulatory framework for artificial intelligence (the AI Act)[3]. In comparative terms, it is the first international legislation aimed at comprehensively governing the technical and social

[1] University of Udine, PhD candidate in Law and Innovation in the European Legal Space funded under Italy's National Recovery and Resilience Plan, D.M. 630/2024.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), in O.J. L of July 12, 2024.

[3] For a preliminary overview see, *ex multis*, G. Finocchiaro, F. Donati, F. Paolucci, O. Pollicino (eds.), *La disciplina dell'intelligenza artificiale* (1st ed. 2025); S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, *La regolazione europea dell'intelligenza artificiale nella società digitale* (1st ed. 2025); C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary* (1st ed. 2024); G. Taddei Elmi, A. Contaldo (eds.), *Intelligenza artificiale. AI Act - Regolamento (UE) 1689/2024. Il nuovo scenario giuridico europeo* (1st ed. 2024); G. Cassano, E.M. Tripodi (eds.), *Il Regolamento Europeo sull'Intelligenza Artificiale. Commento al Reg. UE n. 1689/2024* (1st ed. 2024); A. Mantelero, G. Resta. G.M. Riccio (eds.), *Intelligenza artificiale. Commentario*, (1st ed. 2025).

phenomenon of artificial intelligence (AI). This harmonized set of rules governs the placing on the market, putting into service and the use of "AI systems"[4] by providers[5] and deployers[6], with specific obligations for other operators as well[7]. The AI Act tailors the type and content of its rules to the scope and intensity of the risks that may arise from the provision and use of AI. Building on this risk-based approach, the regulation lays down prohibitions, requirements, and obligations, with specific provisions applying to general-purpose AI models[8]. The regulation becomes applicable progressively: on February 2, 2025, Chapters I and II became effective, followed by Chapters III (Section 4), V, VII and XII, and Article 78[9] on August 2, 2025, while most of the provisions will apply from August 2, 2026[10].

The stated goal of the AI Act is to introduce a legal framework to enable and facilitate the spread and development of this technology in the internal market, while supporting an anthropocentric and trustworthy vision of AI and ensuring respect for fundamental rights and EU values[11]. However, the regulation's attempt to express the tension between supporting innovation and protecting rights in a balanced rationale has generated intense debate. There is controversy over the ability of the AI Act to strike an appropriate trade-off between innovation and the protection of rights. In other words, there are growing concerns about whether the AI Act is a regulation that can support innovation or whether, by contrast, it may hinder it.

## II. The AI Act as a pro-innovation law

Economic and legal scholars have long debated the relationship between innovation and regulation[12]. This is a structurally ambivalent relationship, as regulation can both hinder and

[4] Pursuant to Article 3(1)(1), «*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*». On this point, see OECD, *Recommendation of the Council on Artificial Intelligence,* 2019, OECD/LEGAL/0449 and OECD, *Explanatory memorandum on the updated OECD definition of an AI system,* OECD Artificial Intelligence Papers, 8 (2024); EU Commission, *Commission Guidance on the definition of an artificial intelligence system as set out in Regulation (EU) 2024/1689 (AI Regulation),* Brussels, July 29, 2025, C(2025) 5053 *final.*

[5] «*[A] natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge*» (Article 3(1)(3)).

[6] «*[A]a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity*» (Article 3(1)(4)).

[7] Including, in particular, importers (*ex* Article 3(1)(6), «*a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country*») and distributors (*ex* Article 3(1)(7), «*a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market*»).

[8] Articles 51 et seq. On this topic, see EU Commission, *Approval of the content of the draft Communication from the Commission – Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act)*, July 18, 2025, C(2025) 5045 *final.*

[9] Except for Article 101.

[10] Article 6(1) and the corresponding obligations will become effective on August 2, 2027.

[11] Article 1(1).

[12] *Ex multis*, N.A. Ashford, R.P. Hall, *The importance of regulation-induced innovation for sustainable development*, in Sustainability, 3 (1, 2011); S. Ambec, M.A. Cohen, S. Elgie, P. Lanoie, *The Porter hypothesis at 20: can environmental regulation enhance innovation and competitiveness?*, in Review of Environmental Economics and Policy, 7 (1, 2013); J.

enable innovative processes[13]. On the one hand, there is the intensity and complexity of the obligations and requirements imposed by regulations[14]; on the other, their ability to create ecosystems that foster trust and new technological demand[15]. Ultimately, the impact of regulation on innovation is an empirical question, to be assessed on a case-by-case basis[16]. This also means that interpretations that automatically portray digital regulation as an obstacle to innovation should be avoided[17].

The debate on the ability of EU legislation to support or, conversely, limit innovation has returned to the forefront with the approval of the AI Act. This applies especially in the business and workplace context. Several factors may explain this renewed interest, including: i) the exponential growth of the global AI market, including in terms of adoption and impact on employment[18]; ii) the new "space race" for economic and political hegemony over AI technologies at the international level[19]; iii) the divergent approaches to AI regulation

Pelkmans, A. Renda, *Does EU regulation hinder or stimulate innovation?,* CEPS Special Report, 96 (2014); R. Engberg, P. Altmann, *Regulation and technology innovation: a comparison of stated and formal regulatory barriers throughout the technology innovation process*, in Journal of Technology Management & Innovation, 10 (3, 2015); N. Martin, C. Matt, C. Niebel, K. Blind, *How data protection regulation affects startup innovation*, in Information Systems Frontiers, 21 (6, 2019); B.Q. Cunha, F. Donadelli, *Mapping the relationship between regulation and innovation from an interdisciplinary perspective: A critical systematic review of the literature*, in Regulation & Governance, 19 (1, 2024); W. Zhang, B. Zhu, Y. Li, D. Yan, *Revisiting the Porter hypothesis: a multi-country meta-analysis of the relationship between environmental regulation and green innovation*, in Humanities and Social Sciences Communications, 11 (1, 2024).

[13] «[…] *the impact of a regulatory framework on innovation, competitiveness and investment depends on two contradicting factors. On the one hand, the additional compliance costs and administrative burdens make AI projects more expensive and hence less attractive for companies and investors. From an economic point of view, whether the obligations are imposed on the user or on the developer is irrelevant, since any costs the developer has to bear will eventually be passed on to the user. On the other hand, the positive impact on uptake is likely to increase demand even faster, and hence make projects more attractive for companies and investors. The overall impact will depend on the balance of these two factors*» (EU Commission, *Impact assessment accompanying the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative act*, 2021).

[14] For a more detailed discussion of the negative effects of AI regulatory policies based on the precautionary principle, see D. Castro, M. McLaughlin, *Ten ways the precautionary principle undermines progress in artificial intelligence*, Information Technology and Innovation Foundation, 2019.

[15] A similar debate interested the General Data Protection Regulation. See, *ex multis*, K. Blind, C. Niebel, C. Rammer, *The impact of the EU General data protection regulation on product innovation*, in *Industry and Innovation,* 31 (3, 2024).

[16] J. Pelkmans, A. Renda, *Does EU regulation hinder or stimulate innovation?*, *cit.*, 26.

[17] In this regard, see A. Tartaro, A.L. Smith, P. Shaw, *Assessing the impact of regulations and standards on innovation in the field of AI,* arXiv:2302.04110 (2023).

[18] By 2030, AI will contribute $15.7 trillion to the global economy, with the potential to increase GDP in local economies by up to 26% (PwC, *PwC's 2024 Global AI Jobs Barometer)*. From another perspective, the adoption of generative AI solutions could add between $2.6 trillion and $4.4 trillion per year to the global economy (McKinsey & Company, *The economic potential of generative AI: The next productivity frontier)*. Globally, 78% of organisations use AI in at least one business function (McKinsey & Company, *The state of AI: How organisations are rewiring to capture value)*. In the EU, 41.17% of large enterprises used AI technologies in 2024 (Eurostat, *Use of artificial intelligence in enterprises)*. In Italy, also in 2024, 59% of large companies had an active AI project (Artificial Intelligence Observatory of the Politecnico di Milano). On the employment front, AI could create 97 million new jobs globally by 2025, compared with the loss of 85 million jobs (World Economic Forum, *Future of Jobs 2020)*. The adoption of generative AI solutions could also automate activities that account for 60-70% of today's working time (McKinsey & Company, *The economic potential of generative AI: The next productivity frontier)*.

[19] See, for example, Y. Walter, *Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation - A contemporary overview and an analysis of socioeconomic consequences,* in Discover Artificial Intelligence, 14 (4, 1, 2024).

compared to the United States and China; iv) the lack of pre-existing EU harmonisation legislation, as in the case of Regulation (EU) 2016/679 (the GDPR).

These circumstances may have led to the perception that the AI Act will represent a barrier to technological innovation in the field of AI in Europe[20]. While recognizing the significant effort required to comply with the AI Act, as well as other factors that might negatively impact the market, another dimension of the law's content deserves attention. This perspective is often overlooked in narratives about the regulation's impact on the market. Within the AI Act, alongside those that can be defined as "protective measures," there are several "innovation measures" that could compensate, at least in part, for the potential restrictive effects on innovation arising from the law.

This paper offers a cross-sectional study of the AI Act to systematically detect and collect those measures capable of supporting and incentivizing technological development. Methodologically, two conceptual categories are suggested to classify these measures. The first includes "explicit innovation measures", while the second encompasses "implicit innovation measures". As it is not possible to provide an exhaustive analysis of each of these measures in this article, they will be examined from the perspective most relevant here – namely, their ability to facilitate and/or support innovation. Finally, some concluding remarks will be offered, including some predictions of the effectiveness of the measures based on comparative analysis.

## III. Explicit innovation measures

The "explicit innovation measures" category includes those measures that the AI Act expressly identifies as such. These are «*measures to support innovation, with a particular focus on SMEs, including start-ups*», which constitute an integral component of the subject matter of the AI Act[21] and to which Chapter VI of the regulation is dedicated. This systematic inclusion is particularly significant, both in terms of the mentioned balancing rationale and in terms of the empowerment of such measures.

[20] On this point, incidentally, it suffices to refer to M. Draghi, *The Future of European Competitiveness (Part B): In-depth Analysis and Recommendations,* September 2024: «*[…] while the ambitions of the EU's GDPR and AI Act are commendable, their complexity and risk of overlaps and inconsistencies can undermine developments in the field of AI by EU industry actors. The differences among Member States in the implementation and enforcement of the GDPR […], as well as overlaps and areas of potential inconsistency with the provisions of the AI Act create the risk of European companies being excluded from early AI innovations because of uncertainty of regulatory frameworks as well as higher burdens for EU researchers and innovators to develop homegrown AI. As in global AI competition 'winner takes most' dynamics are already prevailing, the EU faces now an unavoidable trade-off between stronger ex ante regulatory safeguards for fundamental rights and product safety, and more regulatory light-handed rules to promote EU investment and innovation, e.g. through sandboxing, without lowering consumer standards. This calls for developing simplified rules and enforcing harmonised implementation of the GDPR in the Member States, while removing regulatory overlaps with the AI Act […]. This would ensure that EU companies are not penalised in the development and adoption of frontier AI. […] While it is early to fully gauge the impact of these landmarks regulations, their implementation must avoid producing administrative and compliance burdens and legal uncertainties as the GDPR's and must be enforced within shorter timeframes and more stringent processes for compliance provisions*».

[21] Article 1(2). On this point, see P. Van Eecke, B. Regenhardt, *Article 1. Subject Matter,* in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary, cit.,* 18, which notes that «*Chapter VI contributes to the objective to create a legal framework that is innovation friendly*» through the measures provided for therein and analysed in the following paragraphs.

III.1 *AI regulatory sandboxes*

The AI Act defines AI regulatory sandbox as «*a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision*»[22]. Inspired by the success of sandboxes in various sectors, including fintech, and responding to calls from national AI strategies for the establishment of AI-specific sandboxes[23], the AI Act institutes this measure to provide «*a controlled environment that fosters innovation and facilitates the development, training, testing and validation of innovative AI systems for a limited time before their being placed on the market or put into service pursuant to a specific sandbox plan agreed between the providers or prospective providers and the competent authority*»[24]. Notably, by requiring each Member State to ensure that its competent authorities establish at least one AI regulatory sandbox at national level to be operational by August 2, 2026[25], the AI Act introduces a *de facto* mandatory pro-innovation measure[26].

AI regulatory sandboxes – which can be established in physical, digital or hybrid form and may host both physical and digital products[27] – are pioneered by the AI Act with the aim of: i) improving legal certainty for regulatory compliance; ii) supporting the sharing of best practices through cooperation with authorities; iii) promote innovation and competitiveness and facilitate the development of an AI ecosystem; iv) contribute to evidence-based

[22] Article 3(1)(55).

[23] N. de Andrade, *Article 57. AI Regulatory Sandboxes,* in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary, cit.,* 882.

[24] Article 57(5). In this paper, the analysis is limited to the context of the AI Act. For a broader overview see, *ex multis*, D.A. Zetzsche, R.P. Buckley, J.N. Barberis, D.W. Arner, *Regulating a revolution: from regulatory sandboxes to smart regulation*, in Fordham Journal of Corporate & Financial Law, 31 (23, 1, 2017); H.J. Allen, *Regulatory sandboxes*, in The George Washington Law Review, 579 (87, 3, 2019); B.R. Knight, T.E. Mitchell, *The sandbox paradox: balancing the need to facilitate innovation with the risk of regulatory privilege*, in South Carolina Law Review, 445 (72, 2, 2020); S. Ranchordas, *Experimental lawmaking in the EU: regulatory sandboxes*, in University of Groningen Faculty of Law Research Paper Series, 1 (12, 2021); OECD, *Regulatory sandboxes in artificial intelligence*, in OECD Digital Economy Papers, 356 (2023); S. Ranchordas, V. Vinci, *Regulatory sandboxes and innovation-friendly regulation: between collaboration and capture*, in Italian Journal of Public Law, 107 (16, 1, 2024); R. Nabil, *Artificial intelligence regulatory sandboxes*, in Journal of Law, Economics and Policy, 295 (19, 2, 2024); H.J. Allen, *Regulatory sandboxes: One decade on*, 2025, SSRN 5365057.

[25] Article 57 also allows for the establishment of AI regulatory sandboxes jointly between authorities of Member States, and additional sandboxes at regional or local level, or jointly with the competent authorities of other Member States.

[26] «*This clear and compulsory requirement for the implementation of AI regulatory sandboxes makes this provision concrete and actionable, ensuring that this new and innovative concept becomes a living reality in all Member States. The level of concreteness and actionability of this provision further strengthens the importance of its goals, namely the fostering of innovation, the development of an AI ecosystem and the acceleration of access to markets for European AI providers and deployers*» (N. de Andrade, *Article 57. AI Regulatory Sandboxes*, *cit.*, 891). In the EU Commission's proposal this measure was not envisaged as mandatory, thus demonstrating the «*confidence that institutions have in regulatory sandboxes in the context of European technological development*» (E. Perrone, *Regulatory Sandboxes. Spazi di sperimentazione normativa per l'intelligenza artificiale*, in Media Laws, 237 (1, 2025) – translated by the author). With regard to the changes made during the approval procedure, it has been emphasised that the rules on sandboxes ended up becoming «*very important for identifying, especially at Member State level, an innovative way to apply the new rules on AI*» (E. Longo, *Gli spazi di sperimentazione normativa o anche regulatory sandboxes nell'AI Act*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, *La regolazione europea dell'intelligenza artificiale nella società digitale*, *cit.*, 113 – translated by the author).

[27] Recital 138.

regulatory learning; v) facilitate and accelerate access to the EU market for AI systems, in particular when provided by SMEs[28]. However, these goals are not placed on the same level. The main aim is to promote innovation and contribute to the development of an AI ecosystem: the others appear to serve as means to achieve this primary objective, as is also evident from the systematic placement of the rules on the regulatory sandbox in Chapter VI[29].

Providers participating in AI regulatory sandboxes benefit from several significant advantages, including: i) the establishment of a qualified relationship and privileged exchanges with authorities with a view to compliance with the AI Act[30]; ii) the release of written proof of successfully completed activities and an exit report on activities carried out, results and learning outcomes that can be used to demonstrate compliance with the regulation[31]; iii) the non-application of administrative fines in the event of infringements of the AI Act for providers who comply with the specific plan[32] and the terms and conditions of participation and follow the guidance provided by the authorities in good faith[33]; iv) a facilitated regime for the further processing of personal data lawfully collected for other purposes for development, training and testing in the sandbox of certain AI systems in the public interest[34]. The practical implementation of these objectives is entrusted to the EU Commission, which is tasked with adopting implementing acts specifying the detailed arrangements for the creation, development, implementation, operation and supervision of regulatory sandboxes, outlining common principles and key outcomes that should be respected through these acts[35].

AI regulatory sandboxes have the potential to promote innovation and achieve the other goals outlined in the AI Act. Of course, this capacity will take time to be assessed. The adoption of implementing acts delegated to the Commission will also have to be awaited[36],

---

28 Article 57(8) and Recital 139.

29 N. de Andrade, *Article 57. AI Regulatory Sandboxes, cit.,* 888.

30 Article 57(6)(7).

31 Article 57(7).

32 The «*sandbox plan*» is «*a document agreed between the participating provider and the competent authority describing the objectives, conditions, timeframe, methodology and requirements for the activities carried out within the sandbox* (Article. 3(1)(54)).

33 Article 57(12). In N. de Andrade, *Article 57. AI Regulatory Sandboxes, cit.,* 892, reference is made to the exemption in terms of a «*safe harbour*». The provision is without prejudice to liability under applicable EU and national law for any damage inflicted to third parties as a result of the experimentation taking place in the sandbox. Furthermore, «*[w]here other competent authorities responsible for other Union and national law were actively involved in the supervision of the AI system in the sandbox and provided guidance for compliance, no administrative fines shall be imposed regarding that law*».

34 Article 59 and Recital 140. To further explore this topic, see T. Binder, I. Eisenberger, *Article 59. Further Processing of Personal Data for Developing Certain AI Systems in the Public Interest in the AI Regulatory Sandbox,* in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary, cit.,* 900, which also investigates the relationship between this provision and the relevant rules of the GDPR.

35 N. de Andrade, *Article 58. Detailed Arrangements for, and Functioning of, AI Regulatory Sandboxes, cit.,* 898, which also explains that «*[t]he rationale behind the need for these implementing acts is to 'avoid fragmentation across the Union', that is, contribute to the harmonization of procedures for setting up and running AI regulatory sandboxes. Ensuring that the rules of governance for AI sandboxes are consistent across Member States helps promote a level playing field for all stakeholders interested in participating in this type of program, while avoiding 'sandbox shopping'*». Similarly, E. Perrone, *Regulatory Sandboxes. Spazi di sperimentazione normativa per l'intelligenza artificiale*, *cit.*, 260.

36 E. Perrone, *Regulatory Sandboxes. Spazi di sperimentazione normativa per l'intelligenza artificiale, cit.,* 268.

but the basis appears well-grounded and valid[37], enabling a mandatory measure for encouraging innovation[38].

III.2 *Testing AI systems in real-world conditions*

Testing in real-world conditions is defined as «*temporary testing of an AI system for its intended purpose in real-world conditions outside a laboratory or otherwise simulated environment, with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of […] Regulation and it does not qualify as placing the AI system on the market or putting it into service within the meaning of […] Regulation, provided that all the conditions laid down in Article 57 or 60 are fulfilled*»[39]. Accordingly, the AI Act introduces a specific regime to allow providers and potential providers of high-risk AI systems listed in Annex III to test such systems in real-world conditions outside a regulatory sandbox[40]. The aim is to accelerate the development and placement on the market of these systems, while considering their potential consequences on individuals[41].

To this end, a framework of safeguards and requirements is established for providers and potential providers interested in such testing[42]. These cumulative conditions include: i) the

[37] N. de Andrade, *Article 57. AI Regulatory Sandboxes, cit.,* 892, for whom «*these provisions represent a significant and welcome regulatory innovation within the AI Act*». For E. Longo, *Gli spazi di sperimentazione normativa o anche regulatory sandboxes nell'AI Act*, *cit.*, 136 this is instead «*one of the most courageous gambles of the new AI Regulation*» (translated by the author). Furthermore, C. Cavaceppi, *Sviluppo e ricerca - Innovazione e sostegno - Sandboxes normativi - Spazi di prova in condizioni reali (artt. 57, 58, 59, 60),* in G. Taddei Elmi, A. Contaldo (eds.), *Intelligenza artificiale. AI Act - Regolamento (UE) 1689/2024. Il nuovo scenario giuridico europeo*, *cit.*, 169 also highlights the possibility that sandboxes could become «*ethical reference spaces where the relationship between artificial intelligence and human rights can be framed from the design stage onwards*» (translated by the author).

[38] The proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) presented by the EU Commission on November 19, 2025 proposes changes to Article 57, *inter alia*, by providing the legal basis for the AI Office to establish a sandbox on EU level.

[39] Article (3)(1)(57).

[40] As clarified in T. Binder, I. Eisenberger, *Article 60 Testing of High-Risk AI Systems in Real-World Conditions Outside AI Regulatory Sandboxes*, in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary*, *cit.*, 928, «[*r*]*eal-world testing may be conducted within and outside AI regulatory sandboxes; Article 60 regulates the latter. […] providers must comply with Article 60 in both situations, as made clear by Article 76(2). According to Article 76(2), the market surveillance authorities shall verify the compliance with Article 60 where AI systems are tested in real world conditions in an AI regulatory sandbox*».

[41] Recital 141.

[42] Outlined in Article 60. The need to impose strict rules to protect subjects undergoing testing in real-world conditions stems from the different conditions that characterise these cases compared to regulatory sandboxes: in the case of testing in real-world conditions, the competent authorities cannot exercise enhanced regulatory oversight or impose safeguards (T. Binder, I. Eisenberger, *Article 60 Testing of High-Risk AI Systems in Real-World Conditions Outside AI Regulatory Sandboxes, cit.,* 928). It is precisely because tests carried out outside regulatory sandboxes are supervised only by the provider or deployer that it is understandable why the legislator has not expressly provided for specific requirements for informed consent for participation in testing in real-world conditions within sandboxes. However, it can be expected that, in the agreements to be concluded between authorities and participants pursuant to Article 58(4), in the case of testing in real-world conditions within a regulatory sandbox, consent requirements similar to those laid down in Article 61 will be considered, «*thus making such requirements de facto applicable also to testing within a sandbox. This would be especially warranted to safeguard the human dignity and personal integrity of the subjects, which should be respected regardless of where the testing takes place*» (S.Y. Esayas, L. Tosoni, *Article 61. Informed Consent to Participate in Testing in Real World Conditions Outside AI Regulatory*

drawing up of a real-world testing plan[43], which shall be submitted and approved, together with the testing, by the authority; ii) the recording of tests in an EU database, subject to certain limited exceptions; iii) being established in the EU, or having appointed a legal representative who is; iv) the implementation of adequate safeguards applicable under EU law as a necessary condition for the transfer of data collected and processed for testing purposes to third countries; v) the provision of time limits for the duration of testing (six months, extendable by a further six months)[44]; vi) the application of additional safeguards in the case of persons belonging to vulnerable groups; vii) in the case of deployers' participation, the fulfilment of appropriate information obligations and the conclusion of a written agreement defining the roles and responsibilities of the parties; viii) effective supervision by competent personnel involved in the tests; ix) the implementation of supplementary safeguards to ensure that the predictions, recommendations and decisions of the AI system can be effectively reversed and disregarded; x) ensuring the possibility of withdrawal from the trials at any time, without prejudice and without justification on the part of the individuals, recognising their right to request the immediate and permanent deletion of their personal data; xi) requesting the informed consent[45] of individuals to participate in the testing. This latter guarantee is covered by a specific regime[46], which outlines the conditions for obtaining it and the related documentation requirements[47]. This combination of provisions strikes a balance between promoting innovation and respecting fundamental rights, which is the essence and objective of the regulation[48].

*Sandboxes*, in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary*, *cit.*, 951).

43 This is «*a document that describes the objectives, methodology, geographical, population and temporal scope, monitoring, organisation and conduct of testing in real-world conditions*» (Article 3(1)(53)).

44 On the comparison between this limit and the provisions for AI regulatory sandboxes, see T. Binder, I. Eisenberger, *Article 60 Testing of High-Risk AI Systems in Real-World Conditions Outside AI Regulatory Sandboxes, cit.,* 936.

45 Defined as «*a subject's freely given, specific, unambiguous and voluntary expression of his or her willingness to participate in a particular testing in real-world conditions, after having been informed of all aspects of the testing that are relevant to the subject's decision to participate*» (Article 3(1)(59)).

46 Article 61.

47 For further analysis, see S.Y. Esayas, L. Tosoni, *Article 61. Informed Consent to Participate in Testing in Real World Conditions Outside AI Regulatory Sandboxes, cit.,* 942, which also examines interactions with other regulations, including the GDPR. More generally, and along the same lines, it has been noted that this provision «*raises [...] the level of diligence required of AI providers during the testing phase: it does not merely ensure the technical compliance of AI systems, but aims to ensure that the information process meets high standards of clarity and completeness. It establishes detailed requirements for informed consent, reflecting a legislative commitment to the protection of individual rights, in line with other key legal documents of the European Union*» (G. Pollio, G. Crea, *Sviluppo e ricerca - Partecipazione - Prove reali - Spazio sperimentazione (artt. 61, 62, 63)*, in G. Taddei Elmi, A. Contaldo (eds.), *Intelligenza artificiale. AI Act - Regolamento (UE) 1689/2024. Il nuovo scenario giuridico europeo*, *cit.*, 180 – translated by the author).

48 «*Article 61 of the AI Act is intrinsically linked to Article 60 […]. Together, these provisions embody and further the central objective of the AI Act, in the sense that they aim to strike a balance between the promotion of innovation and respect for the interests and fundamental rights of individuals. While real world testing aims 'to accelerate the process of development and the placing on the market of the high-risk AI systems', the requirements for free and informed consent in Article 61 ensure that such testing is conducted in a way that respects individuals, especially their rights to human dignity and personal integrity*» (S.Y. Esayas, L. Tosoni, *Article 61. Informed Consent to Participate in Testing in Real World Conditions Outside AI Regulatory Sandboxes*, *cit.*, 945).

The rules dedicated to test in real-world conditions, while differing from those for AI regulatory sandboxes[49], therefore appear to introduce an (optional) framework capable of facilitating innovation in the field of AI within a perimeter that guarantees security and fundamental EU rights and values[50].

III.3 *Measures and derogations for SMEs, start-ups and specific operators*

Articles 62 and 63 complete the Chapter on measures in support of innovation by adopting an operator-based approach. As such, attention is focused on specific operators based on their intrinsic features, assessed in relation to the AI market.

Article 62 addresses the interests of SMEs, including start-ups[51], which are providers or deployers of AI systems. The provision lays down obligations for Member States and the AI Office (but not only for them), aimed primarily at developing capacity for SMEs, reducing regulatory burdens and improving market access[52]. More specifically, Member States are required to undertake a series of actions to «*promote and protect innovation*»[53]. These actions, which in most cases also extend to other parties (deployers, other innovators, local public authorities, other relevant stakeholders), include: i) priority access to AI regulatory sandboxes [54] ; ii) organising targeted awareness-raising and training activities on the application of the AI Act[55]; iii) the provision of dedicated channels of communication with these entities to provide advice and answer questions on the implementation of the

[49] In addition to the differences already mentioned, for the purposes of this article, attention is drawn to Article 60(9), which provides that providers remain liable for any damage caused during their testing in real world conditions. This is in line with Article 57(12) regarding liability for damages in the context of regulatory sandboxes. However, the exemption from administrative penalties for violations of the AI Act does not apply to testing in real world conditions. For this reason, «*[t]esting in real-world conditions in an AI regulatory sandbox may be more attractive to some (prospective) providers*» (T. Binder, I. Eisenberger, *Article 60 Testing of High-Risk AI Systems in Real-World Conditions Outside AI Regulatory Sandboxes*, *cit.*, 940).

[50] The Digital Omnibus on AI proposes amendments to the testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes pursuant by Article 60, *inter alia* extending this regime to high-risk AI systems covered by Section A of Annex I and creating a legal basis for interested Member States and the EU Commission, on voluntary basis, to enter into written agreements to test high-risk AI systems referred to in Section B of Annex I in real world-conditions.

[51] For an overview, also in terms of the historical evolution of the text of the AI Act, with regard to the concepts of SMEs and start-ups, see T. Binder, I. Eisenberger, *Article 62. Measures for Providers and Deployers, in Particular SMEs, Including Start-Ups,* in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary, cit.,* 965, where it is argued that «*[t]he final Article 62 […] refers to 'SMEs' in general, thus including medium-sized enterprises as well. This is a more appropriate approach to fostering innovation, as it covers more addressees*».

[52] T. Binder, I. Eisenberger, *Article 62. Measures for Providers and Deployers, in Particular SMEs, Including Start-Ups, cit.,* 964, which points out that Article 62 should be considered in the context of the EU's general measures to promote and support SMEs. Along the same lines, see G. Pollio, G. Crea, *Sviluppo e ricerca - Partecipazione - Prove reali - Spazio sperimentazione (artt. 61, 62, 63)*, *cit.*, 181.

[53] Recital 143.

[54] The incentive is linked to a location criterion – being aimed at SMEs, including start-ups, with their registered office or a branch in the EU – and requires that the eligibility conditions and selection criteria for regulatory sandboxes be met, without precluding other providers from accessing AI regulatory sandboxes.

[55] «*This provision is in line with the Commission's objectives to avoid disproportionate burdens on SMEs in the AI Act and to create a digitally literate population and highly skilled digital professionals. Furthermore, this provision helps to overcome the problem that SMEs and start-ups often lack skilled employees because they cannot afford to invest adequately in the training of their employees*» (T. Binder, I. Eisenberger, *Article 62. Measures for Providers and Deployers, in Particular SMEs, Including Start-Ups*, *cit.*, 966).

regulation; iv) facilitation of participation in the standardisation development process. This provision then requires notified bodies to take into account the specific interests and needs of providers that are SMEs, including start-ups, when setting fees for conformity assessment, «*reducing those fees proportionately to their size, market size and other relevant indicators*»[56]. Also under the logic «*to address the specific needs of SMEs, including start-ups*»[57], the AI Office is required to take action by: i) providing standardised templates for the areas covered by the AI Act; ii) developing a single information platform with easy to use information on the regulation; iii) organising communication campaigns to raise awareness of the obligations under the AI Act; iv) promoting the convergence of best practices in public procurement procedures in relation to AI systems.

Article 63 focuses, instead, on microenterprises within the meaning of Recommendation 2003/361/EC. Given the very small size of these operators, and «*in order to ensure proportionality regarding costs of innovation*», these operators are allowed to fulfil «*one of the most costly obligations, namely to establish a quality management system, in a simplified manner which would reduce the administrative burden and the costs for those enterprises without affecting the level of protection and the need for compliance with the requirements for high-risk AI systems*»[58]. Once again, the measure clearly reflects a pro-innovation stance[59], as it is designed to reduce potentially disproportionate regulatory burdens for smaller businesses while ensuring simplified compliance for them[60][61].

## IV. IMPLICIT INNOVATION MEASURES

The AI Act also encompasses a set of provisions which, although not expressly defined as «*measures in support of innovation*», can directly or indirectly encourage progress in the field of AI. These measures, which can be classified as "implicit innovation measures", find their rationale form the purpose of the regulation, as outlined in Article 1(1), which makes explicit reference to the promotion of innovation[62].

---

[56] Recital 143 also extends the intervention in question to the EU Commission and Member States.

[57] Recital 143 specifies that «*[m]edium-sized enterprises which until recently qualified as small enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC should have access to those support measures, as those new medium-sized enterprises may sometimes lack the legal resources and training necessary to ensure proper understanding of, and compliance with, […] Regulation*».

[58] Recital 146. The EU Commission is tasked with developing guidelines to specify the elements of the quality management system that micro-enterprises should comply with in this simplified manner.

[59] «*Article 63 aims for a regulatory balance that safeguards safety and trust without hindering innovation with undue obligations on microenterprises. Instead of applying the same strict standards across the board, it offers a degree of leeway specifically for microenterprises in terms of quality management, thereby encouraging AI innovation even among the smallest companies*» (A. Zarra, *Article 63. Derogations for Specific Operators*, in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary*, *cit.*, 973).

[60] A. Zarra, *Article 63. Derogations for Specific Operators, cit.,* 975, which also reports the data from the study supporting the impact assessment of the AI Act, according to which the total costs for setting up a quality management system range from approximately €193,000 to €330,000.

[61] The Digital Omnibus on AI propose adding legal definitions for micro, small and medium-sized enterprise (SME) and small mid-cap enterprise (SMC) to the definitions in Article 3, extending regulatory privileges for SMEs to SMCs on technical documentation and putting in place a quality management system that takes into account their size, and extending the derogation from micro-enterprises to SMEs to comply with certain elements of the quality management system in a simplified manner.

[62] The same reference also appears in Recital 1. On this point, see also P. Van Eecke, B. Regenhardt, *Article 1. Subject Matter, cit.,* 18, according to which «*[t]he promotion of AI-driven innovation is closely linked to the Data Act, the*

IV.1 *Exceptions to the material scope of application*

After defining the scope of the regulation from a material, personal and territorial perspective[63], Article 2 establishes a list of scenarios in which the regulation does not apply. Two cases are particularly relevant here, both concerning research activities.

The first provides that the AI Act does not apply to «*AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development*»[64]. The exclusion aims to «*support innovation, […] respect freedom of science, and […] not undermine research and development activity*» and its exceptional nature is confirmed by the express subjection of the AI Act rules to «*any other AI system that may be used for the conduct of any research and development activity*»[65].

The second, instead, excludes from the scope of the regulation «*any research, testing or development activity regarding AI systems or AI models*», but only «*prior to their being placed on the market or put into service*»[66]. This exception[67] shares the same rationale[68] and complements the exemption for scientific research by focusing on commercial research, testing and development activities[69]. In this case, however, a logical-temporal limit is introduced: only research, testing and development activities regarding AI systems or AI models before their commercialisation or deployment are exempt, with the obligation to comply with the AI Act if an AI system falling within the scope of the regulation is placed on the market or put into service as a result of such research and development activities[70].

---

*Data Governance Act, Common European Data Spaces, and other initiatives under the EU strategy for data, which are intended to establish trusted mechanisms and services for the reuse, sharing and pooling of data that are essential for the development of data-driven AI models of high quality*». For M. Orofino, *Obiettivi, ambito di applicazione e principi fondamentali dell'AI Act*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, *La regolazione europea dell'intelligenza artificiale nella società digitale*, *cit.*, 37, «*according to the EU's intentions, regulation should not be seen as a limitation (or obstacle) to private activity, but as an essential tool for strengthening citizens trust*» (translated by the author).

[63] For an overview of the discipline, see P. Van Eecke, B. Regenhardt, *Article 2. Scope*, in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary*, *cit.*, 22; M. Orofino, *Obiettivi, ambito di applicazione e principi fondamentali dell'AI Act*, *cit.*, 33; M. Bassini, *Oggetto, campo di applicazione e ambito territoriale*, in G. Finocchiaro, F. Donati, F. Paolucci, O. Pollicino (eds.), *La disciplina dell'intelligenza artificiale*, *cit.* 113; L. Marafioti, *Caratteri essenziali e ambito di applicazione del regolamento*, in G. Cassano, E. M. Tripodi (eds.), *Il Regolamento Europeo sull'Intelligenza Artificiale. Commento al Reg. UE n. 1689/2024*, *cit.*, 369.

[64] Article 2(6). The law does not define the meaning of «*specifically*» and «*[t]his could prove challenging, as research can explore potential scenarios where a research project might have both scientific and practical applications, calling into doubt the applicability of the exemption*» (P. Van Eecke, B. Regenhardt, *Article 2. Scope*, *cit.*, 43).

[65] Recital 25 also specifies that «*any research and development activity should be carried out in accordance with recognised ethical and professional standards for scientific research and should be conducted in accordance with applicable Union law*».

[66] Article 2(8). The provision also clarifies that such activities should be carried out in accordance with applicable EU law and that testing in real world conditions does not fall within the scope of this exclusion.

[67] According to Recital 25, the exclusion does not affect the application of the rules on regulatory sandboxes and testing in real-world conditions.

[68] For M. Orofino, *Obiettivi, ambito di applicazione e principi fondamentali dell'AI Act*, *cit.*, 45, «*this objective must also be interpreted as a limit on the intervention of Member States, which cannot exploit the exclusion to adopt national regulations that unduly restrict research activity*» (translated by the author).

[69] P. Van Eecke, B. Regenhardt, *Article 2. Scope, cit.,* 44.

[70] Recital 25. M. Orofino, *Obiettivi, ambito di applicazione e principi fondamentali dell'AI Act*, *cit.*, 45 qualifies the exception referred to in paragraph 6 as an absolute derogation and that provided for in paragraph 8 as a partial derogation.

The exclusion of scientific and commercial research and development activities from the scope of the AI Act can be considered as a key measure from a pro-innovation perspective, freeing these innovative processes from regulatory compliance duties. Moreover, the partial nature of the exemption for commercial activities also allows research activities to be set up in a logic of by-design and by-default compliance, in the absence of an immediate compliance burden, thus enabling the identification and testing of the best solutions to ensure innovation and (subsequent) sustainable compliance.

### IV.2 *The risk-based approach*

The risk-based approach – which, together with the ethical guidelines for trustworthy AI developed by the High-Level Expert Group on Artificial Intelligence appointed by the EU Commission[71], constitutes the foundation of the AI Act – is outlined in recital 26[72]. The latter explains the rationale behind this approach («*[i]n order to introduce a proportionate and effective set of binding rules for AI systems*»)[73], the *modus operandi* («*[t]hat approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate*») and the results of its application («*[i]t is therefore necessary to prohibit certain unacceptable AI practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems*»). The pyramid identified by this approach provides for: i) certain AI practices that pose an unacceptable risk – and are therefore prohibited – strictly listed by the regulation[74]; ii) high-risk AI systems that qualify as such according to the classification criteria referred to in Article 6 and Annexes I and III, for which several requirements and obligations should be met[75]; iii) certain AI systems specifically indicated in Article 50, which are subject to transparency obligations[76].

[71] Recital 27.
[72] For further analysis, in addition to the references cited below, see P. Dunn, *The Artificial Intelligence Act: a tile in the EU's digital risk-based approach*, in G. Finocchiaro, F. Donati, F. Paolucci, O. Pollicino, *La disciplina dell'intelligenza artificiale*, *cit.*, 141; G.M. Marsico, *L'approccio basato sul rischio*, in G. Cassano, E.M. Tripodi (eds.), *Il Regolamento Europeo sull'Intelligenza Artificiale. Commento al Reg. UE n. 1689/2024*, *cit.*, 377.
[73] «*Hence, the underlying objective of the AI Act's risk-based approach is to strike an optimal (or proportionate) balance between innovation and the benefits of AI systems on the one hand, and the protection of fundamental values such as safety, health and fundamental rights on the other*» (M. Ebers, *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, in European Journal of Risk Regulation, 685 (16, 2, 2025), which refers to G. De Gregorio, P. Dunn, *The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age,* in Common Market Law Review, 473 (59, 2, 2022), who emphasises that this objective, albeit by different means, is the same as that pursued primarily by EU risk-based digital policies, including GDPR).
[74] Article 5. For further analysis, see EU Commission, *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act),* Brussels, February 4, 2025, C(2025) 884 *final.*
[75] For the criteria for classifying high-risk systems, see Article 6.
[76] Article 50 AI Act.

Under this risk-based approach, the legislator predetermined the risk associated with AI systems[77] following a top-down approach[78]. Turning this theoretical pyramid upside down, this means that an AI system that does not fall within the risk categories listed in the AI Act is not bound by the regulation[79]. Although not free from criticism[80], this methodological choice can also be viewed from a different perspective, as far as it is of interest here. By preselecting only certain AI systems as risky, the legislator has effectively left all AI systems not expressly referred to in the regulation[81] free from constraints, thus also promoting the related innovative processes.

IV.3 *AI literacy*

The AI Act defines AI literacy as the «*skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of […] Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause*»[82]. The law therefore requires providers and deployers to take «*measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf*»: this should be done «*taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used*»[83]. The AI literacy requirement, although not appearing in the initial text of the

[77] The only exception to this rule is that provided for in Article 6(3), which allows an AI system not to be considered high risk «*where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making*», provided that at least one of the conditions listed in the provision is met and subject to the counter-exception in the case of AI systems that perform profiling of natural persons.

[78] «*In this case, the shift from a bottom-up to a top-down interpretation of risk-based regulation […] reached its apex. The categories of risk are defined directly by the EU Commission and set in stone within the law. The list of "unacceptable", and therefore prohibited, AI systems is directly set by the law and is independent of any a posteriori risk assessment by providers or users of those systems. The definition of high-risk technologies is also already defined by the law: in this case, the category is seemingly less stiff and more open to ex post change, since a procedure to amend the Annex III is possible. However, it is once again up to the EU Commission to make the necessary adjustments. The AI Act sets a range of risk criteria: however, in this case, they are meant as a guide for the Commission itself, and not for the targets of regulation*» (G. De Gregorio, P. Dunn, *The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age*, *cit.*, 492). Similarly, G.M. Marsico, *L'approccio basato sul rischio*, *cit.*, 383. Both sources also highlight the difference in approach compared to the GDPR.

[79] «*The spectrum embracing the set of AI applications with minimal risk is very broad and offers both the interpreter and the operator an opaque, albeit vast, range of application possibilities*» (G. De Gregorio, P. Dunn, *The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age*, *cit.*, 491).

[80] On this point, see the observations in M. Ebers, *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, *cit.* and in C. Novelli, *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in Federalismi, 95 (2, 2024).

[81] With a view to the voluntary application of the AI Act, rules on codes of conduct have been introduced. For further analysis, see N.E. Vellinga, J.M. Bonnici, *Article 56. Codes of Practice,* in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary, cit.*, 871.

[82] Article 3(1)(56).

[83] Article 4.

regulation[84], became a cross-referenced provision in the AI Act[85]. Despite being included in the Chapter containing the general provisions of the law, it is considered to apply only in cases of «*rights and obligations in the context of […] Regulation*» and not whenever there is an «*AI system*» within the meaning of the AI Act[86]. These training activities are aimed at the staff of providers and deployers, as well as «*other persons dealing with the operation and use of AI systems on their behalf*»[87]. To address the potential vagueness of certain elements of the obligation – such as the «*sufficient*»[88] or «*adequate*»[89] level of AI literacy and the concept of «*measures*»[90] to be taken[91] – the EU Commission has provided initial guidance on what the minimum requirement for compliance with the AI Act should be[92]. The regulation also provides incentives for the adoption of measures to support compliance with the new requirement[93].
First, it should be noted that it is the AI Act itself which suggests that the AI literacy obligation (also) serves as a measure to support innovation[94]. The law clarifies that this provision was introduced «*[i]n order to obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control*», also pointing out that «*the wide implementation of AI literacy measures and the introduction of appropriate follow-up actions could contribute to improving working conditions and ultimately sustain the consolidation, and innovation path of trustworthy AI in the Union*»[95].
Second, and more generally, the AI literacy requirement can operate as a pro-innovation measure from multiple perspectives. Acquiring an adequate level of AI literacy could be a significant factor in stimulating innovation, as it can help remove a bottleneck to innovation

[84] A provision on AI literacy appeared for the first time in the EU Parliament's negotiating position in June 2023. However, several significant changes were made to the originally proposed version. On this point, see M. Paolini e Silva, A. Tamò-Larrieux, O. Ammann, *AI Literacy Under the AI Act: Tracing the Evolution of a Weakened Norm,* in SSRN Electronic Journal, 2 (2025).
[85] See the provisions on technical documentation (Article 11), human oversight (Article 14) and the right to explanation of individual decision-making (Article 86).
[86] This is the interpretation proposed in T. Cabral, *AI Literacy Under the AI Act: An Assessment of its Scope,* in SSRN Electronic Journal, 1 (2025).
[87] Article 4. On this point, the EU Commission has clarified that these subjects are not employees, but persons who fall within the organisational sphere in a broad sense, such as contractors, service providers and clients (EU Commission, *AI Literacy - Questions & Answers).*
[88] Article 4.
[89] Recital 91.
[90] Article 4.
[91] E. Fernandes, W. Holmes, S. Zhgenti, *Article 4. AI Literacy,* in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary, cit.*, 93.
[92] EU Commission, *AI Literacy - Questions & Answers.* Further aspects clarified concern, for example, the format of training.
[93] On the one hand, one of the tasks of the European AI Board is to «*support the Commission in promoting AI literacy, public awareness and understanding of the benefits, risks, safeguards and rights and obligations in relation to the use of AI systems*» (Article 66(1)(f)); on the other hand, the EU Commission, through the AI Office, and the Member States are called upon to facilitate the development of voluntary codes of conduct «*to advance AI literacy among persons dealing with the development, operation and use of AI*» (Recital 20, which is applied in the subsequent Article 95(2)(c)).
[94] For an analysis of some outstanding issues on the interpretation and application of AI literacy rules, see L. Paseri, M. Durante, U. Pagallo, *The Legal Challenges of AI Literacy Between Enforcement and Compliance,* in Media Laws, 1 (1, 2025).
[95] Recital 20.

by bridging the technical skills gap that is often widespread in many countries[96] and professional sectors[97]. In addition, a higher level of AI competence can facilitate and speed up the adoption of this technology in the workplace[98]. Through appropriate AI literacy training, employee confidence in AI can be strengthened, thereby making the adoption of algorithmic systems faster and more scalable in business[99]. At the same time, such training may serve as a precondition for reducing implementation costs and preventing potential failures in implementation processes. Making training compulsory further increases the likelihood of achieving these outcomes[100].

## V. ASSESSMENTS OF EFFECTIVENESS AND FUTURE PERSPECTIVES

This cross-sectional study of the AI Act has highlighted the existence of a variety of measures that may support and encourage technological development, particularly in the EU business and employment context. A number of innovation measures within the AI Act, both explicitly and implicitly, have been identified and analysed. However, there are also other measures that can be considered to have implicitly positive effects on innovation. These include, for example: i) lower penalties for SMEs, including start-ups[101]; ii) the regime of (non-)application of the AI Act for AI systems already placed on the market or put into service[102]; iii) the gradual application of the AI Act rules[103], which has been defined *ex ante* by the EU lawmaker.

---

[96] A relevant analysis in this regard is offered by S. Denkowska, K. Fijorek, G. Wegrzyn, *Formal and Non-Formal Education and Training As an Instrument Fostering Innovation and Competitiveness in EU Member Countries*, in Journal of Competitiveness, 12 (3, 2020).

[97] In this regard, an interesting prespective is provided by C. Chatzichristos, G. Chatzichristos, I. Borremans, S. Gruyaert, I. De Vos, M. De Vos, F. De Backere, *Bridging the AI-Literacy Gap in Health Care: Qualitative Analysis of the Flanders Case Study*, J Med Internet Res 2025;27:e76709.

[98] In this regard, analysing the issue at the level of educational programmes, see T. Schultheiss, U. Backes-Gellner, *Does updating education curricula accelerate technology adoption in the workplace? Evidence from dual vocational education and training curricula in Switzerland*, in The Journal of Technology Transfer, 49 (1, 2024).

[99] For further analysis regarding the application of this requirement in the workplace, see G. Franco, *AI Literacy: l'alfabetizzazione sull'intelligenza artificiale nel prisma degli obblighi di formazione sul lavoro*, in Il Lavoro nella giurisprudenza, 7(2025).

[100] The Digital Omnibus on AI proposes transforming the obligation for providers and deployers of AI systems with regards to AI literacy to an obligation on the EU Commission and the Member States to foster AI literacy.

[101] Article 99(6). A Buchta, *Article 99. Penalties,* in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary, cit.*, 1348 explains that «*[f]or SMEs, the fines are capped at lower amounts, balancing the need for enforcement with the recognition of their limited financial capacity to avoid stifling innovation while ensuring that AI systems are developed and used responsibly*». The Digital Omnibus on AI proposes extending these regulatory privileges on penalties for SMEs to SMCs.

[102] Article 111 provides, *inter alia*, that the AI Act applies «*to operators of high-risk AI systems […] that have been placed on the market or put into service before 2 August 2026, only if, as from that date, those systems are subject to significant changes in their design*». The rationale for this provision is «*to ensure legal certainty, ensure an appropriate adaptation period for operators and avoid disruption to the market, including by ensuring continuity of the use of AI systems*» (Recital 177). A. Winkelmeier, C. Korab, *Article 111. AI Systems Already Placed on the Market or Put into Service and General-Purpose AI Models Already Placed on the Market*, in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary*, *cit.*, 1446 clarifies that «*[d]ue to a lack of special provisions in Article 111, compliance obligations for AI systems other than high-risk or GPAI systems – such as primarily the obligations in Article 50 – are relevant from the date of application of the act onwards*».

[103] See the timetable set out in Article 113. On this point, see C.N. Pehlivan, *Article 113. Entry into Force and Application,* in C.N. Pehlivan, N. Forgó, P. Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary, cit.*,

It is not yet possible to prove that these measures will be sufficient to support and stimulate the AI market in the EU, thereby offsetting any limiting effects resulting from compliance burdens. However, some preliminary assessments could be made from an *ex ante* perspective. For those provisions whose effects on innovation are difficult to evaluate in the abstract (*e.g.* the risk-based approach and the exceptions to the material scope of application), the actual impact will depend on how stakeholders and authorities approach the new legal framework, both from an implementation and an enforcement perspective.

For other provisions, experience from different sectors and/or jurisdictions may provide a basis for more informed predictions. This could apply in particular to provisions on AI literacy[104].

Similarly, with regard to regulatory sandbox, useful parameters for prediction can be drawn from experiences of countries that have adopted this measure in specific industries, specifically fintech. The adoption of sandboxes has produced significant positive effects, particularly in terms of venture investment[105], regulatory certainty, companies-regulator collaboration, and credibility[106], but also in operational continuity and patent ownership[107]. Comparative, multi-jurisdictional and multi-sector analyses of regulatory sandboxes regimes also allows for the identification of factors that can contribute to the production of positive impacts on innovative markets through these measures. These include, among others: the establishment of structured and clear regulatory framework for sandbox projects (setting out conditions for regulatory exemptions, application procedures, assessment criteria and exit strategies); systematic updates to these frameworks; the availability of adequate funding and support for innovators; the promotion of diversified and inclusive participation; and transparent reporting[108].

As a further consideration, the success of these measures also depends on broader systemic factors, such as the availability of adequate investment programmes and economic support for the market. In this respect, the example of other countries can also serve as a useful benchmark, in particular those with more advanced AI market, such as China and the United

1468 («*Rebalancing technological innovation with regulatory oversight, the AI Act, through its risk-based approach and phased implementation, strives to ensure that AI systems are deployed safely and ethically across the EU while providing sufficient time and guidance for stakeholders to conform to the new rules*»). The Digital Omnibus on AI proposes postponing the application of obligations for high-risk AI systems (scheduled for August 2, 2026) through a mechanism linking the application of these requirements to the availability of standards, common specifications and guidelines from the EU Commission, with deadlines of December 2, 2027 and August 2, 2028 (depending on the AI system concerned).

104 See the arguments already set out above in this regard.

105 See J. J. Goo, J. Y. Heo, *The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation*, in Journal of Open Innovation: Technology, Market, and Complexity, 6 (2, 2020), which considered nine countries in the study (United Kingdom, Singapore, Hong Kong, Australia, India, Canada, Malaysia, The Netherlands, and Japan).

106 See J. Kálmán, *The Role of Regulatory Sandboxes in FinTech Innovation: A Comparative Case Study of the UK, Singapore, and Hungary*, in FinTech, 4 (2, 2025).

107 See G. Cornelli, S. Doerr, L. Gambacorta, O. Merrouche, *Regulatory sandboxes and fintech funding: evidence from the UK*, in Review of Finance, 28 (1, 2024).

108 Z. Aydın, O. Yardımcı, *Regulatory sandboxes and pilot projects: Trials, regulations, and insights in energy transition*, in Engineering Science and Technology, an International Journal, 56 (2024), 12-15. The study covered twelve countries (Australia, Austria, Belgium, Canada, France, Germany, Italy, the Netherlands, Norway, Singapore, the UK and US).

States. In these jurisdictions, however, approaches to AI regulation differ significantly from the EU model[109], in some cases extending even to forms of deregulation[110]. This divergence represents an important factor to consider in any comparative analysis.

In conclusion, when assessing whether the identified pro-innovation measures will be able to boost innovation in the field of AI in Europe, the practical implementation phase and the enforcement policies adopted at the EU and national levels will play an important role. In this regard, Italy adopted national regulation on AI with Law No. 132/2025, whose provisions should be interpreted and applied in accordance with the AI Act[111]. However, the regulation's attempt to reconcile measures to protect fundamental rights with those to support innovation remains valid. This makes the AI Act a law that is also commendable in its pro-innovation dimension.

[109] For a preliminary comparative overview see, *ex multis,* J. Chun, C.S. de Witt, K. Elkins, *Comparative Global AI Regulation: Policy Perspectives From the EU, China, and the US,* arXiv:2410.21279 (2024); M. Nimrod, *Global Perspectives on AI Governance: A Comparative Overview,* in Third International Conference on Hybrid Human-Artificial Intelligence co-located with (HHAI 2024), Malmö (2024); F. Heymann, K. Parginos, A. Hariri, G. Franco, *Regulating Artificial Intelligence in the EU, United States and China - Implications for energy systems,* in 2023 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE), Grenoble (2023).

[110] See, for instance, the America's AI Action Plan issued under Executive Order 14179 in July 2025. For a detailed analysis, K.M. Belikova, *The global race for artificial intelligence: regulatory and other acts governing the development and application of artificial intelligence in the United States of America*, in Lobbying in the Legislative Process, 4 (3, 2025).

[111] Law No. 132 of September 23, 2025, "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*", in O.J. No. 223 of September 25, 2025. The law i) sets out principles on research, experimentation, development, adoption and application of AI systems and models; ii) promotes the correct, transparent and responsible use of AI in an anthropocentric dimension, aimed at seizing its opportunities; iii) ensures the monitoring of economic and social risks and the impact of AI on fundamental rights (Article 1). Applying the pro-innovation reading proposed in this article this law, Article 8 on scientific research and experimentation in the development of AI systems in the healthcare sector is notable. Pursuant to this provision, processing of both personal data and special categories of personal data, carried out by a number of public and private entities, is of significant public interest. The obligations to inform patients are also simplified, providing for the possibility of secondary use of data, including health data, without the need to obtain a second consent, for scientific research purposes, provided that de-identification measures are applied. Furthermore, without prejudice to the obligation to provide a notice, the law legitimises the reuse of both personal and health data to apply anonymisation, pseudonymisation or synthesisation measures to them, where this is carried out for the purposes of scientific research or for the planning, management, control and evaluation of healthcare.

# AI Regulatory Sandboxes as Legal Transplants: Governance, Regulatory Learning and Legal-Technical Interaction

*Fabio Seferi**

Table of Contents:



*This article analyses the AI regulatory sandboxes architecture under the AI Act through the lenses of "legal transplantation", advocating for a multilevel examination of their legal, institutional, and functional implications. AI regulatory sandboxes are conceived as controlled spaces for developing, training, validating, and testing AI systems subject to regulatory supervision. The article explores three key dimensions for their implementation, as key factors for a successful "transplant": governance, regulatory learning, and legal-technical interaction. Thus it first examines multilevel coordination problems at the interface between EU institutions, national and sub-national governments, and sectoral regulators, supporting harmonisation and structures of accountability. Then, it addresses the AI regulatory sandbox as a regulatory learning instrument, through which competent authorities may adapt not only the applicable rules but also their practices and regimes in response to sandbox experimentation. Lastly, the article addresses the fundamental issue of "substantial modification" in AI systems and the role of AI regulatory sandboxes in testing and supporting its assessment.*

**Keywords**: AI regulatory sandboxes – AI Act – artificial intelligence — AI regulation – legal transplants

## I. Introduction

This article examines AI regulatory sandboxes[1] envisaged under the EU AI Act[2] through the lens of legal transplantation, asking under which legal, institutional, and operational conditions this "double transplant" can succeed in EU and national legal orders. AI regulatory sandboxes are treated not merely as innovation-support tools, but as a legal

* PhD Candidate in Cybersecurity, IMT School for Advanced Studies Lucca and University of Florence, fabio.seferi@imtlucca.it. The author wishes to express his gratitude to the two anonymous reviewers for their valuable comments and insights. In addition, the author wishes to sincerely thank the participants in the Young Scholars' Workshop held at the University of Udine on 4-5 September 2025, and Prof. Federica Giovanella for having organised such a great event and learning opportunity.

[1] For a comprehensive work on regulatory sandboxes, see F. Bagni and F. Seferi (eds.), *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders*, CINI's Cybersecurity National Lab, (2025).

[2] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj (last visited Jan. 26, 2026). The AI Act has the purpose to promote the uptake of human-centric and trustworthy AI, while ensuring an important level of protection of fundamental rights, health and safety in the EU (refer to Article 1).

institution that has been first transplanted from national and sectoral experimentation into EU law and will then be transplanted again into Member States' frameworks through the AI Act's mandatory obligation to establish at least one national sandbox by 2 August 2026.[3]

Methodologically, the article combines doctrinal analysis of the AI Act with insights from the broader literature on legal transplants and regulatory experimentation, complemented by a structured reading of existing sandbox schemes and guidance at EU and national level. Starting from the legal definition of AI regulatory sandboxes, the study identifies the core features of this instrument. Then, it identifies and analyses three dimensions that need closer consideration for evaluating the degree of success of such transplantation: i.e. governance, regulatory learning, and legal-technical interaction. The argument is grounded in comparative and multi-level reasoning, drawing on selected use cases and policy documents to extract recurring operational practices.

In this view, the structure of the article reflects this threefold analytical focus. Section II frames regulatory sandboxes as legal transplants, distinguishing them from broader notions of legal diffusion and underscoring the "double transplant" dynamic specific to AI sandboxes under the AI Act. Section III then turns to governance, unpacking the multilevel coordination challenges that arise between EU-level bodies (in particular the AI Board and the AI Office), national competent authorities, and regional or local actors, as well as across sectoral regulators already operating sandbox schemes. Section IV focuses on regulatory learning, conceptualising AI regulatory sandboxes as structured experimentation spaces that should generate regulatory feedback and inform both national policy cycles and the EU-level review and impact-assessment processes foreseen by the AI Act. Section V addresses legal-technical interaction by zooming in on the contested notion of "substantial modification" of AI systems and exploring how sandbox activities can support the assessment, documentation, and risk management of such modifications along the AI system lifecycle. Finally, Section VI provides concluding reflections on AI regulatory sandboxes as hybrid instruments of legal and institutional transformation.

## II. FRAMING SANDBOXES AS LEGAL TRANSPLANTS

### II.1 *Brief remarks on legal diffusion and transplantation*

Legal transplants refer to the process by which a law or legal institution developed in one country is adopted or borrowed by another country or legal system, often with adaptations to suit the new local context.[4] While legal borrowing has resulted to be a common and effective process, "legal transplant" is a contested term, with research preferring

[3] Refer to Article 57(1) of the AI Act.

[4] J. W. Cairns, *Watson, Walton, and the History of Legal Transplants*, in Georgia Journal of International and Comparative Law 41(3), 637 (2013).

expressions such as "legal diffusion"[5] – albeit the growing success of the metaphor provided by the meaning of "transplantation".

Although both "legal diffusion" and "legal transplants" pertain to the phenomenon of transferring and moving laws or regulatory models across borders, the term "legal transplant" points not only to the act of borrowing but also to the challenges of adaptation and institutional integration faced by these models in their new environment. The legal transplantation debate focuses on the fact that a successful transfer relies on adjustments to legal, cultural, and policy contexts in understanding that not all institutions can be easily transported.[6]

The regulatory sandbox concept is a strong exemplary case today: its transfer and application from one sector or jurisdiction to another perfectly illustrates both the promise and the hard realities of legal transplantation in action. In this sense, regulatory sandboxes may be considered a form of "legal transplant".[7] Such frameworks allow for the controlled testing of innovative products under the oversight of a regulatory authority.[8] They were introduced in the financial sector, after an initial establishment in the United Kingdom, where the Financial Conduct Authority (FCA) launched its first regulatory sandbox in 2016 to support fintech innovation.[9] This first initiative has since inspired a wide range of applications in several jurisdictions and sectors, with financial services still being a key pillar.[10] Regulatory sandboxes can be considered as mechanisms for "structured experimentalism".[11] This represents another factor for adopting a "legal transplant" lens in analysing regulatory sandboxes: it is not only a specific law or *corpus* of laws, but a regulatory method – a legal institution and practice in itself – that is diffused, borrowed, and adapted into different legal systems and jurisdictions.[12]

---

[5] T. S. Goldbach, *Why Legal Transplants?*, in Annual Review of Law and Social Science, 15:583-601 (2019).

[6] J. W. Cairns, *cit.*

[7] This has been already analysed by Ford and Ashkenazy, who write that "[t]ransplants from one regulatory regime to another require careful thought, if they are to achieve the objectives the new context's regulators have in mind for them"; see C. Ford and Q. Ashkenazy, *The Legal Innovation Sandbox*, in The American Journal of Comparative Law, 72:3, 559 (2024). A more recent article has also shown how this is valid with respect to comparing U.S., EU and Chinese models, in particular by noting that "[t]hese models are not converging toward a single standard; rather, they reflect endogenous responses to regulatory, political, and economic constraints. This framework provides a useful lens for evaluating potential regulatory transplants, legal harmonization efforts, and the risks of conceptual misappropriation": see A. Stazi and R. Jovine, *A Comparative Analysis of Regulatory Sandboxes: Models, Evolution and Strategic Implications in EU, USA and China*, in Comparative Law Review, 16:2, 65 (2025).

[8] For an account of AI sandboxes, see Datasphere Initiative, *Sandboxes for AI. Tools for a new frontier*, Report (2025).

[9] For more information on the FCA Sandbox refer to: https://www.fca.org.uk/firms/innovation/regulatory-sandbox (last visited Jan. 26, 2026).

[10] F. Seferi, *A comparative analysis of regulatory sandboxes from selected use cases: Insights from recurring operational practices*, in F. Bagni and F. Seferi (eds.), *cit.*, (2025).

[11] D. A. Zetzsche, R. P. Buckley, J. N. Barberis, and D. W. Arner, *Regulating a revolution: From regulatory sandboxes to smart regulation*, in Fordham J. Corp. & Fin. L., 23:31-103 (2017).

[12] Several studies have also mapped how regulatory sandboxes have been diffused to different contexts and geographies; see, e.g., A. Attrey, M. Lesher and C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, Going Digital Toolkit Note No. 2 (2019); World Bank Group, *Global Experiences from Regulatory Sandboxes*, Fintech Note No. 8 (2020); Baker McKenzie, *A guide to regulatory fintech sandboxes internationally* (2021).

These efforts have led to a consolidation of such practice at EU level also.[13] In particular, the AI Act includes provisions on AI regulatory sandboxes in Chapter VI, which focuses on measures to support innovation. Albeit not being the only EU Regulation that foresees regulatory sandboxes in the digital domain,[14] the AI Act covers a key role since it mandates Member States to ensure that their competent authorities establish at least one AI regulatory sandbox at national level by 2 August 2026.[15] Thus, it is the only Regulation that clearly sets a mandatory provision regarding the establishment of such a scheme at national level in the EU.

Such obligatoriness underscores a distinctive feature of AI regulatory sandboxes, a case of a "double" transplant: first, the regulatory sandbox as a framework was transplanted from sectoral (thus, external) utilisation into EU law; second, due to their mandatory establishment at national level, AI regulatory sandboxes will be permanently transplanted further into national frameworks.[16]

### II.2 *AI regulatory sandboxes under the AI Act*

The AI Act defines AI regulatory sandboxes as "controlled framework[s] set up by a competent authority[17] which offer providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision".[18]

Starting from the "legal" definition, we can identify an array of features of AI regulatory sandboxes – thus, acknowledging how they have been "transplanted" into the AI Act. First, it is a *controlled framework*, thus assuming that the experimentation should be carried

---

[13] They are included as one of the approaches within the EU Better Regulation Toolbox, specifically under Tool #69 on emerging methods and policy instruments.

[14] Other two key examples being the interoperability regulatory sandboxes under the so-called Interoperable Europe Act (Regulation (EU) 2024/903 laying down measures for a high level of public sector interoperability across the Union, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj (last visited Jan. 26, 2026)), and cyber resilience regulatory sandboxes under the so-called Cyber Resilience Act (Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj (last visited Jan. 26, 2026)).

[15] Refer to Article 57(1) of the AI Act.

[16] This is also similar to the concept of "double transplantation" included in the taxonomy created by Ferreri and DiMatteo, who consider this as the case in which a country transplants a specific area of law and then uses that transplantation in the making of a broader law"; see S. Ferreri and L. A. DiMatteo, *Terminology Matters: Dangers of Superficial Transplantation*, in Boston University International Law Journal, 37:1, 54 (2019).

[17] Refer to Article 3(48) of the AI Act for the definition of "national competent authority", for which it relates to "a notifying authority or a market surveillance authority; as regards AI systems put into service or used by Union institutions, agencies, offices and bodies, references to national competent authorities or market surveillance authorities in this Regulation shall be construed as references to the European Data Protection Supervisor".

[18] Refer to Article 3(55) of the AI Act. On a systematic analysis of AI regulatory sandboxes under the AI Act, refer to L. Cotino Hueso, *Sandbox, controlled spaces and real-world testing of artificial intelligence systems in the regulation. Measures for SMEs, startups and micro-enterprises*, in L. Cotino Hueso and D. Galetta (eds.), The European Union Artificial Intelligence Act. A systematic commentary, Editoriale Scientifica, 867 ff. (2025). See also J. Ponce and A. Cerrillo-i-Martínez (eds.), *The EU Artificial Intelligence Act and the Public Sector - Humans and AI Systems in Public Administration in the light of the European Regulation on Artificial Intelligence of 2024*, EPLS Vol. CXXVIII (2025).

out in a protected manner, within specific safeguards. Such controlled framework is set up by a competent authority, posing the need also for a legal basis defining the scope, operational procedures and roles of the different actors involved.[19]

Second, the scheme foresees, at a minimum, the involvement of at least two *types of actors* with different *roles*: (i) the competent authority – in particular, the market surveillance authority – who establishes the framework and oversees experimentation; and (ii) the (prospective) AI provider who participates in experimentation with its innovative AI system.

Third, the *type of activities* that may be conducted are namely four: development, training, validating and testing of innovative AI systems. This highlights how AI regulatory sandboxes may be used in different moments in the systems' development lifecycle, also posing the issue of defining the right types of experimentation to be conducted in each activity.

Fourth, experimentation is carried out pursuant to a specific *sandbox plan*. The sandbox plan holds a key role, since it contains the details of the main elements of sandbox participation, such as objectives, conditions, timeframe, methodology and requirements for the activities conducted within the AI regulatory sandbox.[20]

Fifth, participation in the sandbox is *limited in time*. This ensures that such protected environment and controlled regulatory regime do not apply indefinitely to a specific project, giving it an undue condition with respect to other market players.

Sixth, participation in the AI regulatory sandbox may include *testing in real-world conditions*,[21] that is "the temporary testing of an AI system for its intended purpose in real-world conditions outside a laboratory or otherwise simulated environment, with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of [the AI Act]".[22]

All these features contribute to placing AI regulatory sandboxes in alignment with the types of regulatory sandboxes established in other sectors or geographies. The AI Act, however, does not expressly foresee the possibility of derogating or having possible legal leeway or exemptions from specific norms: this has indeed been a core feature of certain legal traditions on regulatory sandboxes.[23] This is also a core feature of experimental regulation at large, which implies the testing, piloting or trial of a new product, service, approach or process, in such a way as to generate and gather evidence that can inform the design or administration of a regulatory regime.[24] It remains to be seen how AI regulatory

[19] G. Mobilio and M. Giannelli, *Legal basis for regulatory sandboxes: Key aspects for a coherent theoretical and practical framework*, in F. Bagni and F. Seferi (eds.), *cit.*, 29-43.

[20] Refer to Article 3(54) of the AI Act.

[21] Refer to Article 58(4).

[22] Refer to Article 3(57) of the AI Act, for which consistent practices should be ensured across the EU through the cooperation between national competent authorities with respect to testing in real-world conditions.

[23] See, e.g., regulatory sandboxes established in Germany through experimentation clauses; refer to the German Federal Ministry for Economic Affairs and Energy, *Making space for innovation: The handbook for regulatory sandboxes* (2019).

[24] For an overview framing of regulatory sandboxes within experimental regulation, see also E. Longo and F. Bagni, *From legal experimentation to regulatory sandboxes: The EU's pioneering approach to digital innovation and regulation*, in F. Bagni and F. Seferi (eds.), *cit.*, 18-28. See also F. Costantini, *Società dell'Informazione e "diritto*

sandboxes will be deployed and evolve with respect to granting (or not) the availability of derogating from norms.

To prevent regulatory fragmentation within the EU,[25] the European Commission is mandated to adopt implementing acts that will define the provisions governing the "establishment, development, implementation, operation, and supervision of the AI regulatory sandboxes".[26] They will provide the ground rules of "orderly transplant" of the EU framework of AI regulatory sandboxes into Member States' legal frameworks. However, such acts should also provide for flexibility to establish and operate AI regulatory sandboxes at national level.[27] This is indeed a particular moment in time where, considering that the implementing acts and national AI regulatory sandboxes are under development, the diffusion of the legal institution is currently underway. This connects also to the role of legal culture(s) in shaping the success or failure of legal transplants.

Thus, as the implementation and operation of AI regulatory sandboxes generates more data from August 2026 onwards, more empirical sources will be available to assess their success. It is however important to highlight at present how such transplant may be carried out by defining some key dimensions based on the analysis of the legal text of the AI Act and of existing sandbox schemes.

## III. GOVERNANCE: NAVIGATING MULTILEVEL COORDINATION

### III.1 *Supra-national level*

Albeit mandating the setup of AI regulatory sandboxes at the national level, the AI Act institutes key bodies at the supra-national level to ensure coherent and effective implementation across the EU: first, the European AI Board, which comprises representatives from each EU Member State.[28] Its main function is to secure the uniform application of the AI Act by enabling cooperation between Member States and acting as an essential platform for gathering and exchanging regulatory and technical knowledge. The need of cross-border coordination is embedded in AI regulatory sandboxes since they should facilitate cooperation between national competent authorities of different Member

*tecnologico". Il caso delle norme "sperimentali"*, in R. De Giorgi (ed.), *Limiti del diritto. Prospettive di riflessione e analisi*, 617-629 (2018).

[25] For a first analysis on advantages and pitfalls of a possible harmonised EU legal framework for regulatory sandboxes see D. Ahern, *Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon*, in European Business Organization Law Review, Vol. 22 (2021).

[26] Refer to Article 58(1) of the AI Act, see F. Bagni and F. Seferi, *Commento all'Articolo 58*, in A. Mantelero, G. Resta, G. M. Riccio, *Intelligenza Artificiale - Commentario (I edizione)*, Commentari IPSOA, Wolters Kluwer (2025). The draft implementing act was made available by the European Commission for public consultation from 2 December 2025 to 13 January 2026: more information available at https://digital-strategy.ec.europa.eu/en/consultations/commission-seeks-feedback-draft-implementing-act-establish-ai-regulatory-sandboxes-under-ai-act (last visited Jan. 13, 2026).

[27] Refer to Article 58(2)(c) of the AI Act.

[28] Refer to Article 65 of the AI Act.

States.[29] The AI Board also provides important advice and guidance on draft delegated or implementing acts, such as the ones on AI regulatory sandboxes. National competent authorities are themselves directly required to harmonise their activities with respect to sandboxes through the AI Board [30] and to submit annual reports on sandbox implementation to it and the AI Office.[31]

The latter is also a key actor in the supra-national layer of governance. Indeed, the European Commission, through the AI Office, is mandated to adopt the implementing acts containing the detailed arrangements on AI regulatory sandboxes (see subsection II.2). In addition, the AI Office supports governance bodies in Member States by facilitating information exchange and providing technical support, advice, and tools for the establishment and operation of AI regulatory sandboxes.[32] It also actively coordinates with national authorities to promote cooperation among Member States regarding sandboxes and will maintain a publicly available list of all planned and existing sandboxes.[33]

The AI Office is also key since it receives notifications from national competent authorities regarding possible (temporary or permanent) suspensions of testing due to unmitigated risks.[34]

Moreover, another venue of required coordination concerns AI models. The extent to which model testing will occur within AI regulatory sandboxes, and how much (if any) attention general-purpose AI (GPAI) models[35] will be given, has yet to be clarified. However, since oversight of GPAI models lies with the European Commission, specifically the AI Office, coordination and responsibility mechanisms should be defined for those cases where the development, training, validation or testing of an innovative AI system in a national (or sub-national) AI regulatory sandbox may require an evaluation of the GPAI model on which it is based.[36] We would thus have the inclusion of a EU-level body in the operation of a national (or sub-national) AI regulatory sandbox.[37] This is important for the establishment of AI regulatory sandboxes, in particular with respect to

[29] Refer to Article 57(13) of the AI Act.
[30] Refer to Article 57(14) of the AI Act.
[31] Refer to Article 57(16) of the AI Act.
[32] Worth of mentioning, in this sense, is the EUSAiR project, i.e. the two-year Coordination and Support Action launched by the AI Office under the Digital Europe Programme in December 2024, which will support the implementation of AI regulatory sandboxes across the EU; for more information refer to: https://eusair-project.eu/ (last visited Jan. 14, 2026).
[33] Refer to Article 57(15) of the AI Act.
[34] Refer to Article 57(11) of the AI Act.
[35] As defined in Article 3(63), a GPAI model is "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market".
[36] For example, as referred to in Article 75(1) of the AI Act, "[w]here an AI system is based on a general-purpose AI model, and the model and the system are developed by the same provider, the AI Office shall have powers to monitor and supervise compliance of that AI system with obligations under [the AI Act]". In this case, the AI Office covers the role and has the powers of a market surveillance authority.
[37] This has been noted in the so-called Digital Omnibus on AI Regulation Proposal, i.e. the proposal for amendments to the AI Act, through which the AI Office may be given the possibility of establishing EU-wide AI regulatory sandboxes with respect to GPAI systems. For more information visit: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal (last visited Jan. 26, 2026).

their operating procedures, which should in case include such possibilities of coordination and collaboration with the AI Office and clarify which actor retains which responsibility. Ultimately, in the supranational layer, the legal transplant of AI regulatory sandboxes is mediated by EU-level coordinating bodies that act as the primary "host environment" for the new instrument, shaping how it will later take root in national systems. Through the AI Board's harmonising role and the AI Office's power to adopt implementing acts, issue guidance, and aggregate reports, the transplant is channelled into a shared governance framework that reduces the risk of divergent national interpretations of the sandbox model. At the same time, open questions around GPAI oversight show that this host environment is still evolving, so that sandboxes function simultaneously as transplanted instruments and as experimental interfaces feeding back into the further refinement of the EU-level legal architecture that received them.

### III.2 *National level*

Effective national coordination is foundational for the successful operation of AI regulatory sandboxes. National competent authorities are the central actors in sandbox operation.[38] Indeed, each Member State shall establish or designate at least one notifying and one market surveillance authority as national competent authorities under the AI Act.[39]

In addition, robust inter-agency cooperation with other relevant national authorities is essential, in particular with regard to national data protection authorities (DPAs): this is the case for those innovative AI systems that involve the processing of personal data.[40] Other authorities providing or supporting access to data may also be involved insofar as the AI system admitted for experimentation within the sandbox falls under their supervisory remit. This provision is also linked to the possibility of further processing personal data within sandboxes with the aim of developing AI systems for public interest.[41] The provision lays down the possibility of processing "personal data lawfully collected for other purposes"[42] for the development, training, and testing[43] specific AI systems under

[38] National competent authorities, as defined under Article 3(48) of the AI Act, are notifying authorities meaning "the national authorit[ies] responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring" (refer to Article 3(19)), or market surveillance authorities meaning "the national authorit[ies] carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020" (refer to Article 3(26)).

[39] Refer to Article 70(1) of the AI Act. For a more detailed analysis see E. Longo and F. Seferi, *Commento all'Articolo 70*, in P. Perri, G. Vaciago and G. Ziccardi, *Commentario Regolamento sull'Intelligenza Artificiale,* Giuffrè Francis Lefebvre, *forthcoming*.

[40] Refer to Article 57(10) of the AI Act.

[41] Refer to Article 59 of the AI Act.

[42] Refer to Article 59(1) of the AI Act.

[43] It is interesting to notice how, contrary to the activities foreseen by the AI Act for AI regulatory sandboxes (see paragraph II.2), the provision on further processing of personal data does not include the validation of AI systems (thus including only development, training, and testing). This opens a discrepancy when it comes to legally performing such activity within the sandbox.

specific conditions.[44] Multi-authority collaboration will most probably be a necessity with overlapping oversight, considering that the horizontal nature of AI application means that AI systems often lie at the intersection of various legal frameworks (e.g., medical devices, financial services, employment, critical infrastructure, cybersecurity). [45] Seamless collaboration between AI-specific national competent authorities and established sectoral regulators can be streamlined by either (i) coordinating multi-agency windows of applications on specific topics,[46] or (ii) by creating dedicated venues or committees within AI regulatory sandboxes where different (sectoral) regulators convene to oversee specific participating projects.[47]

Another aspect concerns existing regulatory sandboxes. As previously mentioned, before the AI Act had been adopted, several sectoral bodies had already launched their own regulatory sandboxes tailored to specific domains such as finance, healthcare, or mobility – and the trend is not slowing down.[48] While these efforts have provided valuable insights, they also risk contributing to fragmentation if not properly aligned. A coordinated approach is needed to ensure that such pre-existing initiatives can be integrated into an overall strategy:[49] such nested approach to sandboxing brings an increased need for common risk assessment and management methodologies across different frameworks, in view of harmonising activities and legal outputs of such sandboxes.[50]

---

[44] For a more complete analysis of the matter, also with respect to the overlaps with GDPR requirements, see D. Baldini and K. Francis, *AI Regulatory Sandboxes between the AI Act and the GDPR: The role of Data Protection as a Corporate Social Responsibility*, CEUR Workshop Proceedings, vol. 3731 (2024); and D. Baldini, *Legislative intersection perspectives on regulatory sandboxes: Navigating the interplay between the AI Act and the GDPR*, in F. Bagni and F. Seferi (eds.), *cit.*, 70-84.

[45] C. Novelli, P. Hacker, S. McDougall, J. Morley, A. Rotolo, and L. Floridi, *Getting Regulatory Sandboxes Right: Design and Governance Under the AI Act,* Working Paper, SSRN, June 30 (2025).

[46] Ibidem.

[47] For example, the Dutch proposal for an AI regulatory sandbox foresees a three-pillar structure: a core coordination team, a panel of experts for addressing domain-specific questions, and multi-session sandbox processes. This offers a practical model for structuring such inter-agency collaboration and integrating diverse expertise at the national level. For more information refer to: https:// www.autoriteitpersoonsgegevens.nl/en/documents/proposal-dutch-regulatory-sandbox (last visited Jan. 26, 2026).

[48] For example, in Italy two of the most well-known schemes include: (i) the Financial Services Sandbox scheme, established by the Decree of the Ministry of Economy and Finance 100/2021 and involving the market surveillance authorities in banking, insurance and financial markets (for more information refer to: https://www.bancaditalia.it/focus/sandbox/ (last visited Jan. 26, 2026)); and (ii) "Italy Experimentation", a more general and cross-sectoral framework Introduced by Article 36 of Legislative Decree 76/2020 (Urgent measures for simplification and digital innovation) converted by Law 120/2020 (for more information refer to: https://innovazione.gov.it/progetti/sperimentazione-italia/ (last visited Jan. 26, 2026)). For a critical assessment of such schemes see N. Maccabiani, *An empirical approach to the Rule of Law: the case of Regulatory Sandboxes*, in Osservatorio sulle fonti, n. 2 (2020); G. Lo Sapio, *Il regolatore alle prese con le tecnologie emergenti. La regulatory sandbox tra principi dell'attività amministrativa e rischio di illusione normative*, in Federalismi.it, n. 30 (2022); M. Trapani, *L'utilizzo delle sandboxes normative: una ricognizione comparata delle principali esperienze di tecniche di produzione normativa sperimentali e il loro impatto sull'ordinamento*, in Osservatorio sulle fonti, XV, n. 3 (2022); M. Romboli, *Sandbox normativa e temporanea disapplicazione delle regole amministrative*, in Il Diritto Amministrativo (2022); M. Milanesi, *Lo sviluppo delle sandbox regolatorie italiane tra dubbi e opportunità. Requiem per l'art. 223 dello «Schema definitivo di Codice dei contratti pubblici»*, in Federalismi.it, n. 15 (2023); N. Pini, *La regulatory sandbox nell'ordinamento italiano: profili critici e prime applicazioni*, in Queste istituzioni, n. 3 (2023).

[49] As noted also in Article 57(4) of the AI Act.

[50] On the role of regulatory sandboxes as risk management instruments see F. Seferi, *A working experimentation model for cyber resilience regulatory sandboxes*, in Joint National Conference on Cybersecurity Proceedings (ITASEC and SERICS) (2025).

All this considered, at the national level, the transplant of AI regulatory sandboxes becomes a question of how this externally driven legal institution can be integrated into existing administrative structures, sectoral regimes, and data-protection arrangements without generating fragmentation. Authorities must re-configure their cooperation practices, risk-assessment methodologies and data-access setups so that the incoming sandbox scheme complements, rather than conflicts with, pre-existing frameworks. Because many Member States already host sectoral sandboxes, the AI Act's sandbox is effectively transplanted into a crowded ecosystem, and its success hinges on whether national actors can nest this new, EU-mandated layer within domestic experiments, turning overlapping schemes into a coordinated family of transplants instead of isolated, competing organs.

### III.3 *Sub-national level*

The AI Act explicitly acknowledges the possibility of establishing additional AI regulatory sandboxes at regional or local level.[51] These sandboxes need however to be considered within the overall national system. One of the focal points is governance and accountability: this demands that it is made clear who should establish and operate the scheme. National competent authorities, charged with placing into effect and ensuring compliance with the provisions of the AI Act, offer bespoke guidance and legal clarification through the national sandbox. The issue is that if only regional or local authorities have responsibility for establishing and operating the scheme, then this may extend their duties beyond those established under the AI Act. According to this perspective, national competent authorities should continue to participate in the regional and local sandboxes and maintain a certain degree of accountability and oversight regarding their operation. Regional and local authorities may also have the opportunity for greater involvement, depending on the functions and powers assigned to them by their respective Member States.

All this considered, diverse types of mechanisms may be weighed. Where national competent authorities are subject to administrative capacity constraints, or subsidiarity considerations mandate experimentation on a localised scale, decentralisation of operational responsibilities to local or regional authorities can be both a practical and attractive solution. Such delegation should not be ad hoc or de facto, however, but rather clearly delineated, legally formalised, and supported by procedural safeguards. It is only through such formalisation that integrity in the regulatory system can be maintained with accountability and legal certainty of involved parties. Local and regional authorities, when they are given responsibility for running sandbox schemes within their areas, will have to

[51] In Italy, a prominent case is the one of Tuscany with the Regional Law 57/2024, which regulates digital innovation and the protection of digital citizenship rights in the region (available at: https://raccoltanormativa.consiglio.regione.toscana.it/articolo?urndoc=urn:nir:regione.toscana:legge:2024-12-09;57 (last visited Jan. 26, 2026)). Such regional law provides for the first transposition of sandboxes at the Italian regional level, in particular for AI regulatory sandboxes as defined by the AI Act. Indeed, Article 25(2) defines regulatory sandboxes as "a tool for studying and experimenting with processes and technologies in particularly innovative fields, including AI and cybersecurity".

do so within the competences allocated to them. That might involve, for example, the administration of sectoral pilot schemes or access arrangements to local infrastructures or datasets. [52]

While regional and local authorities may be tasked with monitoring sandbox regime day-to-day operations (functioning, thus, as coordinating bodies), the ultimate responsibility for regulation-related monitoring must rest within the national competent authorities. They are indeed the institutional actors best positioned to ensure consistency, proportionality, and policy conformity to national and supranational policy objectives. To maintain this decentralised model of implementation, national competent authorities will need to take an active role in constructing and disseminating the "secondary" rules that govern sandbox activity, for overall harmonisation and consistency of practices. These rules could include standardised entry criteria for participating, procedural guidelines for evaluation, data-exchange protocols, and indicators for measuring regulatory effect. The success of including local and regional authorities in the sandbox environment requires a governance system based on open delegation of responsibilities, legal formalisation of delegation agreements, and strong coordination tools backed by national supervision.

Finally, at the sub-national level, the sandbox transplant is further differentiated as regional and local authorities become potential operators of additional schemes, raising the issue of how far operational responsibilities can be devolved without undermining the integrity of the transplanted institution. Regional and local sandboxes can tailor the transplanted model to specific territorial needs and infrastructures, but they must remain normatively anchored to the national competent authorities through clearly formalised delegation, accountability chains, and harmonised "secondary rules" on entry, procedures, data exchange and metrics. In this perspective, decentralisation is framed as a controlled extension of the transplant into local legal tissues, where national supervision and common standards ensure that experimentation at the periphery does not mutate the core design of the AI regulatory sandbox as transplanted by the AI Act.

## IV. REGULATORY LEARNING: ITERATIVE POLICY FEEDBACK

### IV.1 *The regulatory learning space*

One of the core objectives of AI regulatory sandboxes is to enable regulatory learning and iterative policy-making. [53] AI regulatory sandboxes need not only to enable experimentation but also the development of tools and infrastructures necessary for testing AI systems: this includes metrics such as accuracy, robustness, and security that are

[52] For example, the role of dataset provisioning from public administration is key in the Zurich AI Innovation Sandbox (for more information refer to: https://www.innovationsandbox.ai/ (last visited Jan. 26, 2026)). For a detailed analysis on the Zurich AI Innovation Sandbox, see R. von Thiessen, *Learnings from the AI Sandbox in Zurich: A practical perspective*, in F. Bagni and F. Seferi (eds.), *cit.*, 177-191.

[53] Refer to Article 57(9)(d) of the AI Act, i.e. the contribution of AI regulatory sandboxes to evidence-based regulatory learning.

relevant for regulatory learning, along with provisions to safeguard essential rights and handle societal impacts.[54]

In brief, regulatory learning is the process through which evidence is collected in order to adapt the existing and applicable regulatory policy and framework:[55] it enables technology regulation to effectively respond to and accommodate rapid developments in both the capabilities and applications of regulated technologies.[56] Regulatory learning occurs when regulators acquire knowledge of the issues and possibilities offered by new technologies and innovations, as well as regarding any loopholes or shortcomings in existing regulatory and supervisory frameworks. Such a mechanism is even more pertinent in industries where innovative technologies can offer solutions to social problems. Regulatory learning allows decision makers to learn more about the possible risks as well as benefits and decide whether new interpretations or amendments to current laws are necessary to cope with technological advancements.[57]

The type of regulatory change should also be framed with respect to the specific geographic and sectoral scope (see also Section III). Although Member States are required to document regulatory learning from sandboxes through exit reports[58] and annual reports,[59] they could also implement broader evaluation mechanisms. Therefore, individual EU countries should consider going beyond the formal requirement and analyse how various aspects of the current EU regulatory framework impact businesses and consumers within sandboxes.[60]

### IV.2 *Integration into broader AI governance*

To fully harness the regulatory potential of AI regulatory sandboxes, their outcomes must be systematically integrated into the broader governance and implementation architecture of the AI Act. These sandboxes are not intended to be isolated experimental exercises with narrow relevance to specific innovators or individual national regulators.[61] Rather,

---

[54] Refer to Article 58(2)(i) of the AI Act.

[55] K. Kert, M. Vebrova, and S. Schade, *Regulatory learning in experimentation spaces*, European Commission, Joint Research Centre (2022), for which "[r]egulatory learning refers to the collection and use of any evidence or knowledge that is relevant to current or future regulatory policy, generated in the process of experimenting with an innovative solution" (p. 2).

[56] D. Lewis, M. Lasek-Markey, D. Golpayegani, and H. J. Pandit, *Mapping the Regulatory Learning Space for the EU AI Act*, in Computers and Society (2025).

[57] European Commission, *Staff Working Document, Regulatory learning in the EU: Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy*, Brussels, Belgium, p. 6 (2023).

[58] Refer to Article 57(7) of the AI Act.

[59] Refer to Article 57(16) of the AI Act.

[60] E. Longo, *Gli spazi di sperimentazione normativa o anche regulatory sandboxes nell'AI Act*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, and M. Orofino, *La regolazione europea dell'intelligenza artificiale nella società digitale*, 2025, Giappichelli Editore – Torino.

[61] Methodological concerns regarding the generalizability of the results and outputs stemming from regulatory sandboxes has been raised frequently; S. Ranchordás and V. Vinci, *Regulatory Sandboxes and Innovation-friendly Regulation: Between Collaboration and Capture*, in Italian Journal of Public Law, Vol. 1/2024.

they should function as structured and strategic sites of regulatory learning, providing real-world insights that inform the EU's evolving legal framework for artificial intelligence.[62]
Integrating sandbox outputs into the broader evaluation and review process under the AI Act is essential. This foresees periodic reviews to assess its implementation, proportionality, and effectiveness in light of technological and societal developments.[63] Findings from regulatory sandboxes should offer empirical data on how AI systems perform in practice, where compliance challenges emerge, and whether the current risk-based classification and risk categories are fit for purpose. In this view, a key factor is to establish reliable, standardised success and failure metrics that are applicable across different sandbox projects, by developing clear and consistent procedures for translating sandbox outcomes into concrete regulatory action, such as rule modifications or updated guidance documents.[64]
Such insights are particularly valuable when feeding into regulatory impact assessments (RIAs), which are fundamental tools for ensuring that new legislative proposals or regulatory revisions are proportionate, targeted, and effective.[65] RIAs are central to evidence-based policymaking in the EU legal system. They provide a structured method for evaluating the potential economic, social, and environmental impacts of new or revised regulatory measures. In the context of AI governance, integrating sandbox findings into RIAs would ensure that any future amendments to the AI Act or related legislative instruments are grounded in real-world experimentation and stakeholder feedback.[66]
To support this continuous learning and regulatory calibration, knowledge-sharing mechanisms must be institutionalised. A centralised, accessible digital platform will be established by the AI Office where all sandbox reports, tools, methodologies, and key findings should be published in a standardised and comparable format.[67] This platform should serve as both a repository and a dynamic knowledge hub, facilitating the replication of good practices, enabling benchmarking across Member States, and fostering inclusive engagement from industry, academia, and civil society. Moreover, a formalised institutional learning cycle is needed to ensure that sandbox findings systematically inform regulatory strategy. A dedicated annual AI Board meeting could serve such purpose, with a specific mandate to review sandbox outcomes and develop cross-cutting policy recommendations.

[62] On the possible role of AI regulatory sandboxes within broader governance of high-risk AI systems, see J. Truby, R. D. Brown, I. A. Ibrahim, and O. Caudevilla Parellada, *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*, in European Journal of Risk Regulation, vol. 13, n. 2, pp. 270-294 (2022).
[63] Refer to Article 112 of the AI Act.
[64] C. Novelli, P. Hacker, S. McDougall, J. Morley, A. Rotolo, and L. Floridi, *cit.*.
[65] C. M. Radaelli and F. de Francesco, *Regulatory Impact Assessment*, in R. Baldwin, M. Cave, and M. Lodge (eds.), *The Oxford Handbook of Regulation*, 279-301 (2010).
[66] Indeed, regulatory sandboxes could add value in other instruments for regulatory quality, since they are placed between ex-ante ones (like RIAs) and ex-post evaluations; S. Ranchordás, *Experimental Regulations and Regulatory Sandboxes: Law without Order?*, University of Groningen Faculty of Law Research Paper Series n. 10, 10 (2021).
[67] Refer to Article 57(17) of the AI Act.

IV.3 *Learning as an institutional transplant*

The regulatory learning dimension of AI regulatory sandboxes illustrates a particular complexity in the transplantation process: it concerns not a discrete regulatory rule or instrument, but rather a methodological and institutional shift in how regulatory authorities understand and relate to emerging technologies. When regulatory sandboxes are transplanted into new jurisdictions, the regulatory learning apparatus itself must be adapted to fit (and expand) existing institutional cultures, policy cycles, and evidence-based decision-making traditions.[68] This represents a transplant of regulatory practice rather than regulatory form.

The AI Act's embedding of regulatory learning within AI regulatory sandboxes reflects an acknowledgment that the sustainable transplantation of sandboxes depends on integrating their outputs into established governance architectures.[69] At the EU level, this integration occurs through the European AI Board's coordination role and the AI Office's function as a centralised repository of sandbox knowledge (see also subsection III.1). At the national level, however, the transplant faces contextual pressures: individual Member States possess different bureaucratic capacities, policy formulation windows, and established sectoral regulatory traditions.[70] A Member State's ability to translate sandbox findings into concrete regulatory adaptation may depend on the openness of its legislative cycle, the sophistication of its regulatory impact assessment practices, and the institutional embedding of evidence-based policymaking within its tradition of administrative law. Thus, at the national level, learnings from sandboxes may also be tied to the opening of formal windows within the policy lifecycle.[71]

The legal transplant literature has recognised that successful institutional transfers require not merely the formal adoption of a new instrument, but its integration into existing administrative feedback loops and decision-making structures.[72] In the case of AI regulatory learning through sandboxes, this means that merely establishing sandbox schemes and generating empirical data is insufficient: the success of the transplant depends

[68] Thus, in terms of "learning that can complement the long-term learning processes of the traditional policy cycle", A. Guio Español and P. D. Koenig, *Regulatory sandboxes for AI in the majority world: A learning-centric approach to legal adaptation*, in Cambridge Forum on AI: Law and Governance, 1:e42, 1 (2025).

[69] The potential for and scalability of regulatory learning has indeed been proposed in the draft implementing act as a selection criterion for admitting (prospective) providers in AI regulatory sandboxes (Article 3(3)(b), *supra*, note 26).

[70] D. Ahern, *Operationalising AI regulatory sandboxes under the EU AI Act: The triple challenge of capacity, coordination and attractiveness to providers,* in Cambridge Forum on AI: Law and Governance, 1:e35, 2025.

[71] See, e.g., the experience of the "France Expérimentation" initiative. Such framework identifies two types of obstacles to innovation: (i) a regulatory blockage, where flexibility can be more easily achieved by involving the specific market regulator; (ii) a legislative blockage, which requires the opening of a specific participation window, often linked to the timing of the official policy formulation cycle of legislative bodies, such as the prospect of an appropriate legislative vehicle (vote on a bill by the Parliament). This shows how regulatory adaptation still has different timeframes and complexities depending on the requirement. For more information, refer to: https://www.modernisation.gouv.fr/simplifier-la-vie-des-usagers-et-des-agents/france-experimentation/modalites-de-fonctionnement (last visited Jan. 26, 2026).

[72] Y. Marique and E. Slautsky, *Resistance to Transplants in the European Administrative Space: An Open-Ended Reading of Legal Changes*, in Review of European Administrative Law (REALaw), 1:7-36 (2021).

on whether and how Member States institutionalise mechanisms for converting sandbox findings into policy adaptation.[73]

Furthermore, the regulatory learning transplant involves a specific challenge with respect to sectoral variation. Sandboxes operating in the financial sector may generate learning applicable across fintech, while AI regulatory sandboxes cut horizontally across multiple regulatory domains. The success of this transplant thus depends on designing knowledge-integration mechanisms that account for both the need for sectoral sensitivity and for horizontal coherence in AI governance.[74]

## V. LEGAL-TECHNICAL INTERACTION: SUBSTANTIAL MODIFICATION

### V.1 *Defining substantial modification*

A substantial modification is defined as "a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AI system with the requirements [for high-risk AI systems] is affected or results in a modification to the intended purpose for which the AI system has been assessed".[75] This relates to modifying a product, either physically or digitally, in ways that can alter its nature and characteristics, not having been considered during the initial risk assessment: such changes could potentially affect the product's safety, and therefore should be considered as a substantial modification, with the product being considered as a new one.[76]

In this view, a substantial modification would require a new conformity assessment to the high-risk AI system whose intended purpose has been changed, or whose overall compliance posture with the AI Act has been affected. However, for high-risk AI systems that continue to adapt post-market deployment or after being put into service, modifications and performance changes anticipated by the provider at the time of the initial conformity assessment and documented in the technical documentation shall not be considered a substantial modification.[77]

Thus, inclusion of the possible changes in the technical documentation qualifies them as "non substantial". Indeed, to ensure suitable traceability for high-risk AI systems, logging

---

[73] A. Guio Español and P. D. Koenig, *cit.*, 8-13.

[74] For a deeper dive on policy implications see OECD, *Regulatory Sandboxes in Artificial Intelligence*, Digital Economy Papers, No. 356 (2023).

[75] Under Article 3(23) of the AI Act.

[76] Refer to Recital 35 of Regulation (EU) 2023/988 on general product safety, 23.5.2023, ELI: http://data.europa.eu/eli/reg/2023/988/oj (last visited Jan. 14, 2026). The recital also clarifies that "[i]n order to ensure compliance with the general safety requirement laid down in this Regulation, the person that carries out that substantial modification should be considered as the manufacturer and subject to the same obligations. That requirement should only apply with respect to the modified part of the product, provided that the modification does not affect the product as a whole. In order to avoid an unnecessary and disproportionate burden, the person carrying out the substantial modification should not be required to repeat tests and produce new documentation in relation to aspects of the product that are not impacted by the modification. It should be up to the person that carries out the substantial modification to demonstrate that the modification does not have an impact on the product as a whole."

[77] Refer to Article 43(4) of the AI Act.

must record events that help identify situations involving substantial modification to the system.[78] Additionally, these provisions are to be applied alongside more specific rules found in certain Union harmonisation legislation based on the New Legislative Framework.[79] For instance, Regulation (EU) 2017/745 specifies that certain changes are not considered modifications affecting compliance with applicable requirements; this remains applicable to high-risk AI systems classified as medical devices under that regulation.[80]

In any case, the European Commission will provide further guidance on the practical implementation of the requirements and provisions regarding substantial modification under the AI Act.[81]

### V.2 *The role of AI regulatory sandboxes*

In addition to the development, training, validation and testing of AI systems before they are placed on the market or put into service, AI regulatory sandboxes should also cover the supervision of AI systems with respect to the notion and occurrence of substantial modification.[82] This is connected also to the support that should be given within AI regulatory sandboxes to understand and prepare for the conformity assessment obligations.[83]

AI regulatory sandboxes may help in clarifying which changes should be accounted for in the record-keeping obligation and technical documentation, thus identifying which qualify as "non substantial". For the modification to clarify as substantial, it must be unforeseen or unplanned in the context of the initial conformity assessment.[84] This may place a burden on (prospective) providers to engage in proactive and comprehensive risk assessment and scenario planning before an AI system is introduced to the market.[85] By anticipating potential future updates, concept, model and semantic shifts, and evolving use cases during the design and development phases, providers can incorporate these possibilities into their initial conformity assessment.

---

[78] Refer to Article 12(2)(a) of the AI Act.

[79] Refer to Recital 84 of the AI Act.

[80] Refer to Article 16(2) of Regulation (EU) 2017/745 on medical devices, 5.5.2017, ELI: http://data.europa.eu/eli/reg/2017/745/oj (last visited Jan. 14, 2026).

[81] Refer to Article 96(1)(c) of the AI Act.

[82] Although not specified in an Article, such provision is included under Recital 139 of the AI Act. This aspect was although covered by the draft implementing act, which provides for a sandbox project to be eligible for participation if "the system will be subject to substantial modification" (Article 3(2)(b), *supra*, note 26).

[83] Refer to Article 58(2)(e) of the AI Act.

[84] Indeed, alterations that are integral to the system's predefined learning process are not regarded as substantial modifications; see Bird&Bird, *European Union Artificial Intelligence Act: a guide*, 28 (2025).

[85] Risk assessment and management is important also when implementing the AI Act's requirements – thus transitioning risk categorisation from a scope-oriented to a scenario-based model of multiple factors –, for the assessment of risk significance and when implementing internal risk management requirements; on the matter, see C. Novelli, F. Casolari, A. Rotolo, M. Taddeo, and L. Floridi, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in Digital Society, 3:13 (2024).

In this view, risk assessment activities within AI regulatory sandboxes have a determining role.[86] Future methodologies for such risk assessments should, in this view, consider and place a key focus on substantial modification. This strategic analysis would help to prevent such changes from later being classified as "substantial modification", thereby avoiding the associated regulatory triggers and potential re-assessment burdens. Thoroughly conducting risk and impact assessment on AI systems within AI regulatory sandboxes may also support in identifying strategies and recommendations to include in the proactive management process of the system: this can be key for enhancing the continuous monitoring and evaluation mechanisms of the (prospective) providers and deployers.
Another aspect to consider is post-modification participation in the sandbox: i.e., if and how substantially modified AI systems should be allowed for participation in AI regulatory sandboxes. Since the AI system has already been placed on the market or put into service, sandbox participation may focus more on validation and testing, with the aim of ensuring that the new risk posture of the system is correctly defined. Moreover, potential participation of substantially-modified systems may pose a tension also with respect to the formal admission procedure and to the selection criteria defined for assessing applications. Principles on defining such criteria will be included in the upcoming implementing acts:[87] however, commonly they include core criteria such as degree of innovativeness, public interest or societal benefit, and level of maturity of the product.[88] For example, in this view, a more comprehensive analysis of what constitutes an "innovative" AI system should be carried out to ensure that this does not rule out substantially-modified systems for products already deployed.

### V.3 *The "technical" frontier of transplantation*

The concept of substantial modification in the AI Act represents a particularly complex site of legal transplantation because it requires alignment between legal categories and technical realities. When AI regulatory sandboxes are established across Member States, they must operationalise the notion of substantial modification in ways that are both legally coherent and technically meaningful. This creates a transplant challenge that is genuinely novel: it is not simply a matter of importing a legal concept developed in another jurisdiction or sector, but of establishing shared understanding of a technical phenomenon (the modification and evolution of AI systems in deployment) through a fundamentally legal-administrative framing.[89]

---

[86] A. Alaassar, A. Mention, and T. H. Aas, *Exploring how social interactions influence regulators and innovators: The case of regulatory sandboxes*, in Technological Forecasting and Social Change, Vol. 160 (2020). Their research has shown how social interactions within regulatory sandboxes (in particular, in the financial sector) increase both the legitimacy and risk management capabilities of regulated entities, and the understanding of legal constraints and risks stemming from enabling technologies of regulators.
[87] Refer to Article 58(1). See also *supra*, note 26.
[88] F. Seferi, *A comparative analysis of regulatory sandboxes from selected use cases: Insights from recurring operational practices*, in F. Bagni and F. Seferi (eds.), *cit.*, 149-151.
[89] See M. E. Kaminski, *Regulating the Risks of AI*, Boston University Law Review Vol. 103:1347 (2023), on a more general analysis of (AI) risk regulation itself as a legal transplant.

This creates a second-order transplant challenge: AI regulatory sandboxes must not only operationalise existing legal categories but must themselves become laboratories for refining those categories. The legal-technical interaction dimension shows that sandboxes are expected to support understanding and preparing for conformity assessment obligations, whilst clarifying which changes should be accounted for. This is a form of regulatory learning, but it is distinctly technical in character: it concerns the translation of legal thresholds into operational metrics and assessment procedures.[90]

The transplantation challenge is amplified by the heterogeneity of technical expertise and practices across Member States and sectoral contexts. An AI system in healthcare may undergo modifications that are routine and anticipated in that domain but would constitute substantial modifications if transferred to a critical infrastructure context. National competent authorities operating sandboxes will need to develop and adopt shared methodologies,[91] also in view of assessing substantial modification, while accounting for sectoral variation without creating de facto harmonisation failures.

Furthermore, the notion of substantial modification invokes a legal-technical gap that transcends traditional regulatory transplantation challenges. Whereas the transplantation of governance structures or institutional learning mechanisms can be achieved through legal-administrative means, the transplantation of a meaningful, operationally coherent understanding of when AI system modifications trigger regulatory reassessment requires alignment between legal institutions, technical standards, and practical expertise. This alignment cannot be achieved through legal text alone; it demands that AI regulatory sandboxes serve as sites of collaborative knowledge production between regulators, developers, and technical experts.[92]

## VI. Conclusion

AI regulatory sandboxes, as defined in the AI Act and elaborated here further in this article, are a paradigmatic innovation of the EU's new technology regulatory governance. Instead of merely being compliance facilitators, they are hybrid instruments that combine innovation, regulation, and institutional transformation. Their architecture combines a logic of experimentation and iterated learning extending beyond the regulatory border and into the interior of how institutions perceive, process, and learn from technological transformation. This article has analysed AI regulatory sandboxes through the lenses of "legal transplants", thus regarding the moving of a rule or a system of law from one country or jurisdiction to another. AI regulatory sandboxes however provide for a

[90] Novel research has explored the possibility of using "technical" sandboxes for regulatory learning in the AI Act space, see T. Deckenbrunnen, A. Buscemi, M. Almada, A. Capozucca, G. Castignani, *The Bathtub of European AI Governance: Identifying Technical Sandboxes as the Micro-Foundation of Regulatory Learning*, (2026) arXiv:2601.04094.

[91] Refer to Article 58(2)(i) of the AI Act.

[92] On the knowledge gap between regulatory authorities and the technical specifics of the field to be regulated, see H. Ruschemeier, *Thinking Outside the Box? Regulatory Sandboxes as a Tool for AI Regulation* (2024), available at: http://dx.doi.org/10.2139/ssrn.4787008 (last visited Jan. 27, 2026).

"double" transplant activity since they were first introduced in EU law from widely growing adoption in mainly sectoral and national legislation, and they will be further transplanted into national legal frameworks in a permanent manner due to their mandatory establishment in EU Member States by 2 August 2026.

In this view, three core dimensions have been analysed as key for the success of such diffusion: governance, regulatory learning, and legal-technical interaction. From a governance point of view, sandboxes entail robust multilevel coordination at the EU, national, and sub-national levels, and horizontal coordination among sectoral regulators, so that regulatory experimentation does not equate with fragmentation. As far as regulatory learning is concerned, the true regulatory potential of sandboxes lies in the formalisation of feedback loops into broader legislative and governance cycles. Their output should not be stuck in the silos of individual projects or Member States but rather feed back into the evolving EU AI governance system: interpretive direction, conformity templates, and even future redraft of the AI Act itself. Moreover, coupling technical and legal efforts, AI regulatory sandboxes will play a pivotal role in discovering grey areas of AI Act's application, such as supporting in the assessment of possible substantial modifications to AI systems. Harmonised approaches, standardised measures, and distributed knowledge-sharing architectures will be critical.

# THE RIGHT TO GOOD ADMINISTRATION AND FOUNDATION MODELS: *:* A EUROPEAN GOVERNANCE PERSPECTIVE AND BEST PRACTICES

*Giulia Fantoni*

TABLE OF CONTENTS:



*As foundation models (FMs) – widely, yet inaccurately, also referred to as Generative AI (GenAI) or General Purpose AI (GPAI) – are increasingly used in public administrations, concerns arise regarding their alignment with fundamental rights and legal principles. This paper examines how the Right to Good Administration (Article 41 of the EU Charter of Fundamental Rights) can guide the adoption of foundation models in the public sector, treating it as a broader analytical benchmark for the administrative action, as it is often reflected in domestic constitutional and administrative traditions of EU Member States.*

*Given the black-box nature of FMs, the study focuses solely on their internal use by civil servants, excluding deployments that produce decisions directly impacting on the legal sphere of individuals. Citizen-facing applications for service delivery are likewise left outside the scope of the analysis.*

*By linking the principles of transparency, fairness, accountability, but also privacy and cybersecurity, to the risks posed by foundation models – including opacity, bias, security vulnerabilities, and unreliable outputs – the paper assesses how public authorities can integrate these systems while safeguarding the Right to Good Administration. It combines doctrinal analysis of the EU regulatory framework, particularly the AI Act, with a comparative qualitative study of national guidelines on the internal use of FMs in Denmark, Finland, Poland, and Sweden. The paper identifies key governance requirements and offers recommendations to support rights-aligned and trustworthy internal uses of foundation models in the public sector.*

**Keywords**: Public Administrations – Generative AI – AI Act – Right to Good Administration – Guidelines

## I. INTRODUCTORY REMARKS

Foundation models (FMs) – widely, yet inaccurately, known also as General-Purpose AI or Generative AI – are rapidly finding their way into European public administrations. While these tools promise to increase efficiency and support for civil servants, they also bring serious legal concerns, especially in the field of administrative law. This paper looks at how public authorities could adopt foundation models in ways that are compliant with the Right to Good Administration as per by Article 41 of the EU Charter of Fundamental Rights (CFREU)**.** In particular, the research reflects on how this right should guide the way FMs are used and governed in the public sector. To fulfil the research scope, the article considers already existing governance efforts. More precisely, by combining

comparative legal review and thematic qualitative analysis, it takes a closer look at national guidelines from Denmark, Finland, Poland, and Sweden. The goal is to highlight best practices and offer practical guidance to help policymakers in crafting guidelines for the internal use of FMs by public officials.

### I.1 *From AI to Foundation Models in the Public Sector: A Review of Academic and Institutional Perspectives*

In recent years, the disruptive impact of Artificial Intelligence (hereinafter, AI) has been recognised across multiple sectors, including public administrations.[1] In the public sector, its applications have been – and still are – analysed both from external and internal perspectives.[2] Scholarly discourse has predominantly focused on the external use of AI in the Public Sector, posing a particular attention on Government-to-Citizens (G2C) interactions, such as service delivery[3] or its (more complex) use in in decision-making proceedings.[4]

It is within this context that legal scholarship started acknowledging the difference between deterministic and non-deterministic algorithms, with the latter posing significant challenges due to their lack of explainability.[5] Despite ongoing efforts to enhance their interpretability through Explainable AI,[6] the inherent opacity of these systems – also known as the 'black-box' problem – remains a concern. As a result, scholars commenced to advocate for the need of a human-in-the-loop approach to ensure accountable decision-making.[7]

While AI – according to some – has the potential to enhance rights and freedoms, it also introduces novel legal challenges.[8] This particular concern has sparked calls for a 'good AI society'[9] and for a constitutionally-oriented use of AI,[10] especially within the public sector. In this regard, the Right to Good Administration (GA), as provided for by Article 41 of

---

[1] J. Berryhill, K.K. Heang, *et al.*, *Hello, World: Artificial intelligence and its use in the public sector*, OECD Working Papers on Public Governance, No. 36, OECD Publishing (2019); T. Kerikmäe, E. Pärn-Lee, *Legal dilemmas of Estonian artificial intelligence strategy: in between of e-society and global race*, AI & Society, 36 (2021); B. Marchetti, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, BioLaw, 2 (2021); I. Mergel, H. Dickinson, *et al.*, *Implementing AI in the public sector*, Public Management Review, 1 (XIV, 2023); F. Decarolis, B. Marchetti and L. Torchia (eds.), *The EU Digital Regulation and its Impact on Member States*, Springer (1st ed. 2025).

[2] T.Q. Sun, R. Medaglia, *Mapping the challenges of Artificial Intelligence in the public sector: Evidence from public healthcare*, Government Information Quarterly, 36 (II, 2019); C. van Noordt, G. Misuraca, *Artificial intelligence for the public sector: results of landscaping the use of AI in government across the European Union*, Government Information Quarterly, 39 (III, 2022).

[3] L. Floridi, *Artificial Intelligence as a Public Service: Learning from Amsterdam and Helsinki*, Philosophy & Technology, 33 (2020); Z. Engin, P. Treleaven, *Algorithmic government: Automating public services and supporting civil servants in using data science technologies*, The Computer Journal, 62 (III, 2019).

[4] B. Marchetti (2021). *Supra*, note n. 1.

[5] G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intelligibilità*, Editoriale Scientifica (2019); G. Lo Sapio, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*. Federalismi.it, 16 (2021).

[6] P. Linardatos, V. Papastefanopoulos, *et al.*, *Explainable AI: A Review of Machine Learning Interpretability Methods*, Entropy, 23 (I, 2021).

[7] B. Marchetti (2021). *Supra*, note n. 1.

[8] O. Pollicino, G. De Gregorio, *Constitutional Law in the Algorithmic Society*, in H-W Micklitz *et al.*, *Constitutional challenges in the algorithmic society,* Cambridge University Press (2022); B.W. Wirtz, J.C. Weyererm *et al.*, *Governance of artificial intelligence: A risk and guideline-based integrative framework*, Government Information Quarterly, 39 (IV, 2022).

[9] C. Cath, S. Wachter, *et al.*, *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach,* Science and engineering ethics, 24 (2018).

[10] C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, BioLaw, 2 (2019).

the CFREU (hereinafter, also referred to as Charter of Nice), has gained relevance as a guiding legal principle.[11]

In a situation that was already complex as it stood, with the launch of ChatGPT by OpenAI in November 2022, the emergence of foundation models (FMs) complicated even further the challenges faced by society as a whole.[12] These technologies are versatile and capable of generating outputs in various forms,[13] often blurring the line between human- and machine-generated content.[14] At the same time, they are inherently opaque and fallible.[15]

All these premises generated a regulatory response at the supranational level, with the adoption of Regulation (EU) 2024/1689 (hereinafter, AI Act) that includes a specific Chapter (the firth) fully dedicated to GPAI models.[16] While much discourse on its prospective uses has been focusing primarily on the private sector, FMs have been gaining momentum in the public sector as well.[17] For instance, several administrations – including the European Commission –[18] have implemented or are working on the development of internal GenAI-based tools.[19] This might be justified by the positive economic impact in terms of saving that these models are expected to come with.[20] Furthermore, initial

[11] I. Wróbel, *Artificial intelligence systems and the right to good administration*, Review of European and Comparative Law, 49 (II, 2022). See, also: M. Fink, and G. Gentile, *Article 41: the right to good administration*, in A. Giannopoulou (ed.), *Digital rights are charter rights*, Amsterdam: Digital Freedom Fund, 34-37 (1st ed. 2023).

[12] The G7 Leaders' Statement on the Hiroshima AI Process opens by stressing the 'innovative opportunities and transformative potential' of foundation models and generative AI, while calling to 'manage risks […] keeping humankind at the center.' See: G7 Leaders, *G7 Leaders' Statement on the Hiroshima AI Process*, Hiroshima (2023), available at https://www.mofa.go.jp/ecm/ec/page5e_000076.html. See also: European Commission, Communication on boosting startups and innovation in trustworthy artificial intelligence, COM(2024) 28 final (2024).

[13] N. Crafts, *Artificial intelligence as a general-purpose technology: an historical perspective*, Oxford Review of Economic Policy, 37 (III, 2021).

[14] T.J. Sejnowski, *Large Language Models and the Reverse Turing Test,* Neural Computation, 35 (III, 2023).

[15] For this reason, some describe them as forms of 'agency without intelligence.' See: L. Floridi, *AI as Agency Without Intelligence: on ChatGPT, Large Language Models, and Other Generative Models.* Philosophy & Technology, 36 (XV, 2023).

[16] As per art. 2 of the AI Act, the Regulation applies both to public and private providers and deployers of AI operating within as well as outside the EU whose AI systems enter the EU market or affect individuals within it. See: Regulation (EU) 2024/1689, OJ L. 2024/1689 (2024).

[17] OpenAI launched *ChatGPT Gov* in January 2025 – a GPT version tailored for U.S. government use. By 2024, it was reportedly used by over 90,000 users across 3,500+ public agencies. See: OpenAI, *Introducing ChatGPT Gov*, available at https://openai.com/global-affairs/introducing-chatgpt-gov/ (last visited Jul 15, 2025).

[18] In October 2025, the European Commission launched GPT@EC, a GenAI tool developed by the Directorate General DIGIT, based on the earlier GPT@JRC model. See: European Commission, *Commission launches a new general-purpose AI tool - GPT@EC,* available at https://commission.europa.eu/news-and-media/news/commission-launches-new-general-purpose-ai-tool-gptec-2024-10-22_en (last visited Jul 13, 2025).

[19] In June 2024, the Finnish Ministry of Transport and Communications piloted a Finnish-language GenAI tool to support legislative drafting, concluding that while promising, national models still lag in performance, requiring further investment, and recommending interim use of commercial models. See: Liikenne- ja viestintäministeri, *Liikenne- ja viestintäministeriö kokeilee luovaa tekoälyä lainvalmistelutyön tukena*, available at https://lvm.fi/-/liikenne-ja-viestintaministerio-kokeilee-luovaa-tekoalya-lainvalmistelutyon-tukena#:~:text=Liikenne%2D%20ja%20viestint%C3%A4ministeri%C3%B6ss%C3%A4%20kokeillaan%2C%20miten,hy%C3%B6dynt%C3%A4v%C3%A4n%20pilotin%20tuottaa%20Futurice%20Oy. (last visited Jul 7, 2025).

[20] In 2023, Boston Consulting Group estimated that by 2033, GenAI could yield an annual global return of $1.75 trillion in the public sector. See: M. Carrasco, C. Habib *et. al.*, *Generative AI for the Public Sector: From Opportunities to Value*, Boston Consulting Group, available at https://web-

evidence indicates that this technology could boost productivity in civil servants while lowering their cognitive load.[21]

Grey literature started acknowledging the increasing experimental use of FMs by civil servants. A study published by the EU Public Sector Tech Watch in April 2025 mapped 61 existing use cases of this technology in the public sector among 20 different EU Member States.[22] This confirms a growing institutional interest, which is also reflected in two recent EU initiatives: on one hand, the AI Pact, launched by the European Commission to help stakeholders prepare for the enforcement and implementation of the AI Act;[23] on the other hand, a dedicated EU call for funding to support up to four pilot projects promoting the use of European[24] GenAI-based tools in public administrations.[25]

Alongside the expected benefits of FMs, their introduction in the public sector also come with major legal and operational challenges, which public administrations increasingly recognise.[26] To ensure their responsible use, a variety of governance instruments have been developed at both national and supranational levels.[27] Existing scholarship has primarily focused on regulatory frameworks established by EU institutions and select U.S. States[28]; however, comparatively little attention has been given to the governance measures implemented at the national level within EU Member States. To address this gap, the present study conducts a focused analysis of a selected set of national guidelines, which were identified and examined in accordance with the methodology outlined in the following section.

### I.2 *Research Scope and Methodological Approach*

As mentioned, this paper addresses the gap in literature by focusing on the internal adoption and governance of FMs by public entities, through the lens of the Right to Good Administration under Article 41 of the Charter of Nice. On the matter, it could be (rightly) noted that the Charter formally binds national authorities only when they implement EU law (see, Article 51 CFREU). However, for the purpose of this study, it shall be clarified

assets.bcg.com/df/1e/9cde767044e5bc1d85f3e788f702/generative-ai-for-the-public-sector-from-opportunities-to-value.pdf (last visited May 4, 2025).

[21] In 2024, the Swedish municipality of Uddevalla piloted Microsoft Copilot M365 to support staff. Survey results showed 73% reported more enjoyable work, 67% improved quality, 57% less mental fatigue, and 32% reduced stress. T. Andersson, *Uddevalla kommun har under 2024 utvärderat Copilot M365*, MyAI, available at https://my.ai.se/usecases/623 (last visited July 8, 2025).

[22] The mapped use cases mainly referred to public services, and occasionally to strategic sectors such as security, economy and construction. Of these, over 60 percent are still in the planning, development or testing phase, while 17 cases are already in use. See: A. Brizuela, M. Combetto *et al.*, *Analysis of the generative AI landscape in the European public sector*, European Commission – Directorate-General for Digital Services (2025).

[23] The AI Pact includes webinars for all sectors and encourages AI providers and deployers to voluntarily disclose practices for compliance with transparency and high-risk obligations. For more, see: EU Commission, *AI Pact,* available at https://digital-strategy.ec.europa.eu/en/policies/ai-pact (last visited June 24, 2025).

[24] This prerequisite is in line with Article 12(6) of Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, OJ L 166, 11.5.2021, pp. 1-34.

[25] See: EU Commission, *Commission Implementing Decision of 28.3.2025 on the financing of the Digital Europe Programme and the adoption of the multiannual work programme 2025-2027*, C(2025) 1839 final (2025).

[26] On the matter, see: A. Brizuela, M. Combetto *et al.* (2025). *Supra*, nota n. 22.

[27] *Id.*

[28] S. Weerts, *Generative AI in public administration in light of the regulatory awakening in the US and EU,* Cambridge Forum on AI: Law and Governance, 1, 1-19 (2025).

that the Right to GA represents a broader analytical benchmark for administrative action, as its corollaries are often reflected in domestic constitutional and administrative traditions of EU Member States[29]. That said, the present article investigates the following research question (RQ): How should the Right to GA influence the adoption and governance of FMs in the public sector? To refine this inquiry, a sub-question (SQ1) is also explored: How do EU Member States integrate the principles of the Right to GA in their national guidelines on the internal use of FMs in the public sector?

The paper adopts a rights-based,[30] comparative legal methodology combined with qualitative thematic analysis, with Article 41 CFREU serving both as an analytical and governance framework. In fact, from it the author identified several corollaries – namely, publicity and transparency; the right to be given reasons; efficiency, effectiveness and cost-effectiveness; impartiality, objectivity, fairness and non-discrimination; data protection and cybersecurity. These principles were then used to carry out the thematic analysis of the national governance initiatives falling under the scope of the present research.

The study limits its geographical scope to EU Member States, which fall directly under the application of the AI Act, as including non-EU jurisdictions would have introduced a level of legal heterogeneity inconsistent with the comparative aims of the research. Additionally, the analysis focuses exclusively on the internal use of FMs within public administrations, adopting a Government-to-Government (G2G) approach rather than a Government-to-Citizens (G2C) one. This choice is not merely methodological but substantive. Due to their opacity and non-deterministic nature, foundation models make it difficult for authorities to comply with core procedural guarantees of the Right to Good Administration, particularly the duty to give reasons and to enable individuals to understand and contest administrative decisions. Their use in decision-making processes that directly affect individuals therefore appears difficult to reconcile with these requirements. The study accordingly limits its scope to internal uses. This position is consistent with national[31] and supranational case law, including the CJEU ruling in *Case C-203/22,* which emphasises the right of individuals to understand and challenge automated decisions – something particularly challenging with non-deterministic systems like FMs.[32]

---

[29] For details, see: par. III.I.

[30] This approach is rooted in constitutional scholarship. See: O. Pollicino, G. De Gregorio (2022). *Supra*, note n. 8; I. Wróbel (2022). *Supra*, note n. 11; C. Casonato (2019). *Supra*, note n. 10.

[31] The Swiss *Conseil des États* underlined, in November 2023, that model-based systems are less complex than GenAI since they adhere to set standards and generate findings that are transparent, consistent, and verifiable. Transparency is strengthened and the right to motivation is respected as a result of the ability to examine and explain administrative decisions. See: Conseil des États, *Réponse du Conseil d'Etat au Grand Conseil à l'interpellation David Raedler et consorts au nom Les vert.e.s vaudois.e.s - Quand l'administration s'automatise : quel est le niveau d'utilisation de systèmes algorithmiques dans l'administration vaudoise?*, available at https://www.vd.ch/actualites/decisions-du-conseil-detat/seance-du-conseil-detat/decision/id/b0f4c1a4-eb1c-4e16-9b9a-a7fb36186760 (last visited April 28, 2025). In similar terms, the Italian *Consiglio di Stato* explained that the application of an algorithm in administrative proceedings that result in a final decision is only permissible if the criteria are known, the decision is imputable to the deciding authority, the algorithm does not discriminate, and the reasoning is clear enough for the decision to be understood and challenged. See: Consiglio di Stato, Section VI, *Decision n. 8472/2019* and *Decision n. 5117/2023*. One shall note that the principles expressed by the Italian Council of State have now been incorporated into Article 30 of Legislative Decree No. 36/2023 (Public Procurement Code), which requires, in the case of the use of automated procedures in the lifecycle of public contracts, to respect the principles of 'intelligibility and comprehensibility', 'non-exclusiveness of algorithmic decisions', and 'algorithmic non-discrimination'. See: *Decreto Legislativo 31 marzo 2023, n. 36 – Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici,* GU n. 77, 31.3.2023 - Suppl. Ordinario n. 12.

[32] The ruling of the CJEU in Case C-203/22, even though it formally focuses on Article 15(1)(h) of the GDPR, offers an interpretative tool that is also relevant for the administrative context and the right to motivation under Article 41 of the EU Charter of Fundamental Rights. In the ruling, the Court clarifies that

Citizen-facing applications for service delivery are likewise left outside the scope of the analysis. While such uses may raise fewer concerns than automated decision-making – particularly where they involve informational support rather than legally binding outputs – their inclusion would require examining a distinct set of regulatory and operational considerations (such as accessibility standards or user experience design) that extend beyond the core focus of this study.

Among the multiple governance instruments currently used by public administrations to regulate FMs – such as policies, rules and regulations, protocols, and guidelines – this paper focuses exclusively on the latter. This choice is justified by two main aspects: first, the widespread use of guidelines across EU Member States compared to other governance tools;[33] second, their flexibility and practical orientation, especially for civil servants. From the available national instruments, only State-level guidelines explicitly addressed to civil servants and focused specifically on FMs (not AI broadly considered) were selected.[34] This choice was made to ensure homogeneity and comparability. Given these filters, the countries included in the present analysis are Denmark, Finland, Poland, and Sweden. Each set of guidelines was then analysed using the thematic categories derived from the Right to GA, in order to assess their alignment with Article 41, CFREU.

This approach, inevitably, has some limitations: it considers a selected number of guidelines available as of April 2025. Moreover, using the Right to GA as the primary analytical framework may overlook other relevant legal principles and/or ethical considerations (e.g. public procurement rules and/or copyright, etc.).

That clarified, the analysis aims to identify best practices and governance patterns through existing guideline that could guide future policymakers and support European public administrations in the responsible integration (and regulation) of FMs.

---

the 'meaningful information' that data controllers must provide in the case of automated decisions cannot be limited to the disclosure of the algorithm or a technical description of the decision-making process, but must consist of a concise, comprehensible, and concrete explanation of the criteria actually used. This serves to implement the right of the data subject to challenge the decision. Transposing these principles to the context of public administrations, it can be argued that – in the presence of opaque models such as foundation models, often closed-source – it is not realistically possible to provide effective, verifiable, and intelligible reasoning in cases where such systems directly impact the legal position of citizens. Consequently, the analysis conducted in this study focuses on the internal (G2G) use of foundation models, in which there is not a direct and immediate effects on the legal sphere of individuals. See: European Court of Justice, *CK v Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien*, *Case C-203/22* (2025).

[33] Of the 33 FM governance initiatives mapped by Public Sector Tech Watch (PSTW), 20 were classified as guidelines. See: A. Brizuela, M. Combetto *et al.*. *Supra*, note n. 22. However, this study partially diverges from that classification. Specifically, the document listed as a guideline by PSTW and published by the Estonian Ministry of Justice is, upon closer examination, an article with purely informational intent. The author refers to it as an '*artikli*' (article), indicating it does not serve a regulatory purpose. For this reason, the Estonian initiative was excluded from the present analysis. See: H. Trasberg, *Generatiivne tehisintellekt juristide ja ametnike töös*, available at https://www.justdigi.ee/sites/default/files/documents/2024-04/1.%20Trasberg.%20AI%20juristide%20ja%20ametnike%20töös.pdf (last visited June 24, 2025).

[34] This study again partially diverges from the classification made by PSTW, *id.* While the Danish guidelines are listed in their report as directed to both the public and private sectors, the original document explicitly targets only public authorities ('*til offentlige myndigheder*'). Digitaliseringsstyrelsen, *Guide til offentlige myndigheder om ansvarlig anvendelse af generativ kunstig intelligens*, available at https://digst.dk/media/g5tajoxm/110324-guide-til-offentlige-myndigheder-om-ansvarlig-anvendelse-af-generativ-kunstig-intelligens.pdf (last visited June 28, 2025). Moreover, this analysis includes the Finnish guidelines adopted by the Ministry of Finance in March 2025, which were not part of PSTW's dataset. See: Valtiovarainministeriö, *Ohjeistus generatiivisen tekoälyn hyödyntämisestä työn tukena ja apuvälineenä julkisessa hallinnossa*, available at https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/166199/VM_2025_9.pdf?sequence=1&isAllowed=y last visited April 28, 2025).

## II. UNDERSTANDING FOUNDATION MODELS: CONCEPTUAL, LEGAL AND TECHNICAL FRAMING

Before delving into the core analysis of the present article, it is necessary to briefly outline what are foundation models, how they are regulated under the AI Act, and clarify their technical peculiarities.

### II.1 *Definition and Regulatory Classification of Foundation Models*

FMs constitute a subset of artificial intelligence. Pursuant to Article 3(1) of the AI Act, an AI system is 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that […] infers, from the input it receives, how to generate outputs […].'[35] Scholarly literature has proposed a classification of these systems divided into three macro-categories:[36] first, expert systems that rely on symbolic knowledge (also known as model-based);[37] second, machine learning and deep learning systems; third, foundation models, which are built upon deep learning architectures.[38] For a visual representation, see *Figure 1*.

Although the EU Regulation does not explicitly refer to 'foundation models', it introduces the concept of General-Purpose AI (GPAI), defined under Article 3(63) as a model 'trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market […].'[39] This definition is partially aligned with the notion of 'foundation models' – coined by the Human-Centered Artificial Intelligence (HAI) Institute at Stanford University in 2021 – which describes any model trained on broad data (generally, through self-supervised learning at scale) and that is capable of adaptation across a wide range of downstream tasks (for example, through fine-tuning).[40]

The main examples of FMs currently existing are large language models (LLMs) – like ChatGPT,[41] Claude,[42] Gemini,[43] DeepSeek[44], or Grok.[45] These models are trained through self-supervised learning on vast datasets[46] and can generate a wide range of outputs in

---

[35] See: Article 3, par. 1, n. 1, *AI Act*. The same definition was given also by the Organisation for Economic Co-operation and Development. On the matter, see: OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2024).

[36] For an in-depth analysis of each different category, see: A. Santosuosso, G. Sartor, *Decidere con l'IA. Intelligenze artificiali e naturali nel diritto*, Il Mulino (2024).

[37] See also: B. Marchetti (2021). *Supra*, note n. 1.

[38] A. Santosuosso, G. Sartor (2024). *Supra*, note n. 32.

[39] GPAI providers are subject to transparency and documentation obligations under Article 53 of the AI Act. When a model poses systemic risk – as defined in Article 3(65) and under the conditions set out in Article 51 – additional obligations under Article 55 apply. Since these requirements target providers rather than deployers, and due to the limited relevance of the GPAI regime to the internal governance of FMs by public administrations, a detailed legal analysis falls outside the scope of this section. For further discussion, see: S. Wachter, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, Yale Journal of Law & Technology, 26 (2025).

[40] R. Bommasani, D.A. Hudston *et al.*, *On the Opportunities and Risks of Foundation Model* in ArXiv (2021).

[41] OpenAI, *ChatGPT*, available at https://chatgpt.com (last visited May 20, 2025).

[42] Anthropic, *Claude*, available at https://claude.ai (last visited May 20, 2025).

[43] Google, *Google Gemini*, available at https://gemini.google.com/?hl=it (last visited May 20, 2025).

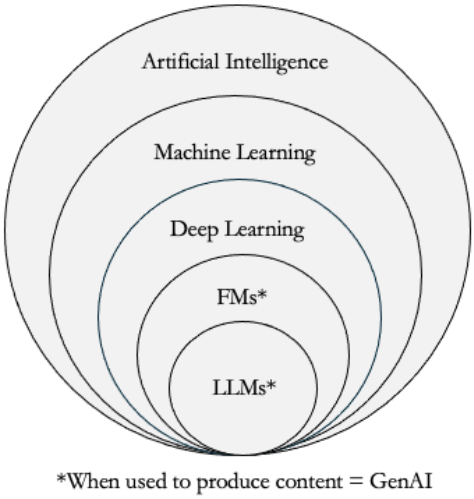
[44] DeepSeekAI, *DeepSeek*, available at https://www.deepseek.com (last visited May 20, 2025).

[45] xAI, *Grok*, available at https://grok.com (last visited May 20, 2025).

[46] In practice, given a textual input, the model learns to predict the most likely output – such as the next word in a sentence – based on patterns found in the training dataset. This process, known as self-supervision

response to natural language prompts.[47] Their development involves a training process including several phases: data collection, data pre-processing, training, fine-tuning and deployment.[48] When FMs are used to generate content – including, but not limited to, text, images and code –, they are referred to as Generative AI (GenAI).[49]

Figure 1 – Visual representation of different subsets of AI




*Source: author's own elaboration*

Due to their overlapping characteristics, terms such as 'FMs', 'GPAI', 'LLMs', and 'GenAI' are frequently used interchangeably in both public and academic discourse. On the matter, however, some clarifications are needed. As highlighted by the HAI Institute – and as argued in this paper – while alternative labels to describe FMs such as 'GPAI' or 'multi-purpose models' capture the versatility of these models, they fail to convey their 'unfinished character and the need for adaptation.'[50] Additionally, talking about GPAI may exclude smaller-scale models trained on domain-specific datasets,[51] which could be even more suitable for public sector applications, especially when fine-tuned on specific legal corpora or past administrative documents.

Given these considerations, this paper adopts the term 'foundation models' as the most inclusive descriptor. This terminological choice is further supported by the 'Guidelines on the scope of the obligations for general-purpose AI models established by Regulation',

at scale, allows models to be trained on massive amounts of text without the need for manual annotation. On the matter, see: A. Santosuosso, G. Sartor (2024). *Supra*, note n. 32, p. 34.

[47] *Id.*, pp. 47-74.

[48] The five-step training framework for LLMs is drawn from: Stanford University IT, *AI Demystified: Introduction to Large Language Models*, available at https://uit.stanford.edu/service/techtraining/ai-demystified/llm (last visited June 2, 2025). For a three-phase framework, see: Y. Liu, H. He, *et al.*, *Understanding LLMs: A Comprehensive Overview from Training to Inference*, in ArXiv (2025).

[49] H. Toner, *What Are Generative AI, Large Language Models, and Foundation Models?*, Center for Security and Emerging Technology, available at *https://cset.georgetown.edu/article/what-are-generative-ai-large-language-models-and-foundation-models/* (last visited Apr. 3, 2025). Additionally, Recital 99 of the AI Act explicitly identifies 'large generative AI models' as a primary example of GPAI models.

[50] R. Bommasani, D.A. Hudston *et al.* (2021). *Supra*, note n. 36.

[51] Small language models in healthcare, for instance, are gaining popularity. For more, see: M. Magnini, G. Aguzzi et al., *Open-source small language models for personal medical assistant chatbo*ts, Intelligence-Based Medicine, 11 (2025); H. Kim, H. Hwang *et al.*, *Small language models learn enhanced reasoning skills from medical textbooks*, Digital Medicine, 8 (2025).

published by the European Commission in July 2025[52]. Paragraph 17 of the Guidelines, in fact, introduce a dual criterion to classify a model as GPAI[53]: first, the use of training compute exceeding $10^{23}$ floating point operations (FLOPs)[54]; second, the capability of the model to generate content in the form of language, text-to-image, or text-to-video. However, paragraph 20 clarifies that models meeting this quantitative threshold still may not qualify as GPAI if they do not demonstrate a significant generality or the ability to perform a broad range of distinct tasks.[55]

The interpretative approach set forth by the European Commission – while useful for regulatory purposes – does not fully encompass the technical characteristics of foundation models. Limiting the analysis to GPAI, as defined in the AI Act and interpreted by the Commission, would result in an overly narrow analytical scope. Many models that fall outside the formal GPAI designation exhibit crucial features of FMs – such as scale, adaptability, and opacity – which pose critical concerns for public administrations.

II.2 *Technical Limitations of Foundation Models*

Outlined the legal framework surrounding the topic of the present article, it appears crucial to dive into the technical peculiarities of these models. While FMs promise to increase efficiency in the public sector[56] and – according to some –[57] reduce mental fatigue on civil servants[58], there are several aspects directly linked to the technical functionalities of these technologies that should not be overlooked.

First and foremost, one shall not be misled by the assertiveness and fluency of FMs.[59] Despite this, in fact, they do not *understand* the content they generate. Rather, they create outputs that are the most statistically probable based on their training data.[60] For this reason, even when prompted to explain their responses, the justification provided is typically an *ex-post* rationalisation, not an accurate reflection of the computational process behind it.[61] This phenomenon – often referred to as the 'black-box' problem –[62] characterises not only FMs but machine learning and deep learning systems more broadly.[63]

Another specific limitation of FMs are hallucinations, meaning the generation of factually incorrect or fabricated content[64]. In parallel, the reliance on web-scale datasets makes these

[52] European Commission, *Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act*, available at https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act (last visited May 5, 2025).

[53] Here GPAI refers generically to general-purpose AI models as defined in Article 3(63) of the AI Act, without distinguishing between models with or without systemic risk.

[54] For reference, the threshold for classification as GPAI with systemic risk is set at $10^{25}$ floating point operations (FLOPs) for training compute.

[55] Conversely, a model may still be considered a GPAI model even if it falls short of the compute threshold, provided it clearly demonstrates such general capabilities. *Id.*

[56] M. Carrasco, C. Habib (2023). *Supra*, note n. 20.

[57] Others, on the other hand, warn about potential negative impact of FMs on cerebral functions. See: N. Kosmyna, E. Hauptmann *et al.*, *Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task* in ArXiv (2025).

[58] T. Andersson (2024). *Supra*, note n. 21.

[59] See: Nature, *Why scientists trust AI too much – and what to do about it*, Editorial – Nature, available at https://www.nature.com/articles/d41586-024-00639-y (last visited May 15, 2025).

[60] A. Santosuosso and G. Sartor (2024). *Supra*, note n. 32, pp. 34 and 53-54.

[61] *Id.* p. 71.

[62] B. Marchetti, (2021). *Supra*, note n. 1 pp. 34 and 53-54.

[63] A. Santosuosso and G. Sartor (2024). *Supra*, note n. 32, pp. 30-58.

[64] Z. Ji, N. Lee, *et al., Survey of hallucination in natural language generation*, ACM Computing Surveys, 55, pp. 1-38 (XII, 2023).

systems prone to reproducing and reinforcing harmful stereotypes and biases.[65]
FMs are also problematic from a privacy standpoint, and this for several reasons.[66] Of these, two are the most relevant for public administrations: first, models might have been trained on personal and/or sensitive data accessed unauthorisedly [67] . Public administrations wanting to fully respect the Right to GA, comply with the GDPR, the AI Act,[68] and enforce a serious data governance framework should ideally consider the training datasets when choosing which FM tool to integrate into their work[69]; second, during the deployment phase, public officials could inadvertently enter unauthorised data through inputs therefore potentially exposing personal and/or classified data.[70]
From a cybersecurity point of view, FMs come with the risk of training datasets being manipulated by malicious actors if strong cybersecurity systems are not enforced. Furthermore, the risks related to the deployment of these technologies include possible unauthorised access to the model by malicious users, who could extract sensitive data. Therefore, this would require the implementation of robust authentication systems and periodic reviews of the deployment configurations, to identify vulnerabilities.[71]
Finally, public administrations should be conscious of the critical environmental impact of Generative AI. [72] Their development and deployment entail high electricity

[65] On the matter, see: R. Geirhos, P. Rubisch, *et al., ImageNET-trained CNNs are biased towards texture; increasing shape bias improves accuracy and robustness*, in ArXiv (2022); M. GLICKMAN and T. SHAROT, *How human–AI feedback loops alter human perceptual, emotional and social judgements*, in Nature Human Behaviour, 9, pp. 345-359 (II, 2025).
[66] For an extensive analysis of these risks, see: C. Novelli, F. Casolari *et al., Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, Computer Law & Security Review, 55 (2024), and I. Barberá, *AI Privacy Risks & Mitigations Large Language Models (LLMs), AI Privacy Risks & Mitigations – Large Language Models (LLMs)*, EDPS, available at: https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf (last visited May 6, 2025).
[67] C. Novelli, F. Casolari *et al.*, *id.*
[68] See: Article 10, AI Act.
[69] This is not possible, for instance, when a model is not 'open'. One shall mind, however, that this 'openness' should not be limited to the FM weights but should at least give access to the training datasets. For more on the different concepts of 'openness' of FMs, see: E. Gibney, *Not all 'open source' AI models are actually open: here's a ranking*, Nature, available at: https://www.nature.com/articles/d41586-024-02012-5 (last visited June 8, 2025).
[70] I. Barberá. *Supra*, note n. 66.
[71] These are present, with different degrees, in all FMs. For more, see: *id.*
[72] For an overview of the environmental costs and potentials of artificial intelligence, see: B. Marchetti, *I costi ambientali dell'IA*, BioLaw, 1, pp. 525-527 (2025); N. Rangone, *Intelligenza artificiale, tutela dell'ambiente e regolazione europea*, BioLaw, 1, pp. 529-548 (2025). More specifically, for an analysis of the debate on the environmental costs of artificial intelligence in the United States, see: M. Merler, *I costi ambientali dell'intelligenza artificiale: il dibattito negli Stati Uniti*, BioLaw, 1, p. 591-614 (2025). Furthermore, for an investigation of the possible application of the Do No Significant Harm (DNSH) principle to limit the negative environmental impacts of artificial intelligence, see: L. De Gaetano, *Il principio Do Not Significant Harm (DNSH) e i costi ambientali dell'intelligenza artificiale*, BioLaw, 1, pp. 571-590 (2025).

consumption,[73] intensive water usage,[74] and substantial $CO_2$ emissions[75].
Having clarified, even if just briefly, the technical peculiarities of FMs serves as the basis to understand the reason – presented in the following sections – why public administrations shall always uphold the Right to GA when introducing these models within their organisations.

## III. THE RIGHT TO GOOD ADMINISTRATION AS AN ANALYTICAL TOOL AND GOVERNANCE FRAMEWORK

As outlined in par. II, FMs present a series of technical peculiarities and associated potentials as well as risks that cannot be overlooked. Given their increasing adoption within the public sector, these aspects require some careful considerations. The present section, therefore, aims to assess whether the current governance framework, existing in some EU Member States in the form of guidelines, can be considered adequate in regulating the use of FMs in the public sector. To do so, the named guidelines will be read in the light of the Right to Good Administration.[76]
Article 41 of the Charter of Nice was chosen as an analytical tool and governance framework for two main reasons. Firstly, the principles it enshrines constitute foundational elements of administrative law not only at the supranational level but also within the constitutional and administrative traditions of EU Member States[77]. Secondly, this methodological approach fully aligns with the right-based approach of the AI Act.[78]
As clarified in the methodology section, Article 41 of the EU Charter is hereby used to analyse national guidelines issued by EU Member States up to April 2025. Other regulatory instruments – like policies, rules and regulations, and protocols – were purposely excluded,

[73] Each query submitted to ChatGPT is estimated to consume approximately ten times more electricity than a standard Google search. See: Electric Power Research Institute, *Powering Intelligence: Analyzing Artificial Intelligence and Data Center Energy Consumption*, available at https://www.epri.com/research/products/3002028905 (last visited Jun. 3, 2025).
[74] Shaolei Ren, a researcher at the University of California – Riverside, estimates that submitting a series of queries (ranging from 5 to 50) to ChatGPT results in the model consuming up to 500 milliliters of water. See: Associated Press, *Artificial intelligence technology behind ChatGPT was built in Iowa – with a lot of water*, available at: https://apnews.com/article/chatgpt-gpt4-iowa-ai-water-consumption-microsoft-f551fde98083d17a7e8d904f8be822c4 (last visited Mar. 7, 2025).
[75] A 2023 study on the LLM BLOOM, which has 176 billion parameters, estimated that its training phase emitted approximately 24.7 tons of $CO_2$ considering only dynamic energy consumption. When accounting for the entire lifecycle, including equipment production and operational energy use, total emissions rose to 50.5 tons of $CO_2$. For comparison, training OpenAI's GPT-3 generated over twenty times more emissions than BLOOM, approximately 500 tons of $CO_2$. See: A.S. Luccioni, S. Viguier *et al.*, *Estimating the Carbon Footprint of BLOOM, a 176B Parameter Language Model in Journal of Machine Learning Research*, Journal of Machine Learning Research 24, pp. 1-15 (2023).
[76] While Article 41 of the EU Charter explicitly refers only to EU institutions, case law and legal doctrine have gradually extended its scope to Member States when implementing EU law. See: M., Kristjánsdóttir, *Good Administration as a Fundamental Right*, Veftímaritið Stjórnmál og stjórnsýsla, 9 (2013).
[77] OECD, *European Principles for Public Administration*, SIGMA Papers No. 27 (1999), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/1999/01/european-principles-for-public-administration_g17a1de4/5kml60zwdr7h-en.pdf (last visited Mar. 3, 2025).
[78] This right-based approach is reflected in Article 1(1), AI Act. Moreover, it is also consistent with relevant Italian case law. More precisely, the already cited *Sentenza n. 2270/2019* of *Consiglio di Stato* recognised, alongside the pitfalls of automation, its alignment with efficiency and cost-effectiveness of the administrative action, and, therefore, its linkage with the so-called '*principio di buon andamento*' – a principle that now, through EU integration, has been elevated to a right (the Right to GA). See: Consiglio di Stato (2019). *Supra*, note n. 27; S. Cassese, *Il diritto alla buona amministrazione – Report on the "Day on the Right to Good Administration" for the 25th anniversary of the law on the "Síndic de Greuges" of Catalonia, Barcelona,* Istituto di Ricerche sulla Pubblica Amministrazione – IRPA (2009).

because less diffused. Only guidelines adopted at the State-level and specifically addressed to civil servants and focused exclusively on Generative AI were selected, to ensure consistency and comparability. Therefore, once again it is stressed that these are the reasons why the final sample includes guidelines from Denmark, Finland, Poland, and Sweden.

As a final clarification, it shall be pointed out that while this article focuses on FMs, the analysed guidelines refer more generally to 'Generative AI'.[79] This terminological gap does not affect consistency, as current GenAI tools used or considered by public administrations are predominantly FM-based (e.g. large language models for text generation or summarisation and data analysis). For the purposes of this study, such references are treated as practical examples of FM use. This approach ensures coherence while reflecting current terminology in public documents.

### III.1 *The Corollaries of the Right to Good Administration*

To assess the extent to which the considered guidelines align with the Right to GA, several sets of corollaries derived from Article 41 were identified.[80] These core principles were divided, in total, into four categories. Each of this category was paired with the corresponding technical risk and/or opportunity associated with the use of FMs in the public sector. For a visual representation, see *Table 1*.

The first set of corollaries includes publicity and transparency –[81] intended as the accessibility of administrative records and the intelligibility of administrative choices[82] – as well as the right to be given reasons, which functions as the procedural safeguard ensuring the practical application of the other two principles.[83] All these three corollaries are severely challenged by the opacity of FMs and public administrations shall be aware of

---

[79] For a broad overview, see: A. Brizuela, M. Combetto *et al.* (2025). *Supra*, note n. 22.

[80] These principles inform the administrative action in the so-called 'European Administrative Space'. See: *supra*, note n. 77. Out of the four Member States falling under the scope of the present research, the Right to GA is recognised at the constitutional level under Articles 51(1), 61(1), 63, and 77(1)of the Polish Constitution and §§ 17 and 21 of the Finnish Constitution. See: FRA, *EU Charter of Fundamental Rights. Article 41 – Right to Good Administration,* available at: https://fra.europa.eu/en/eu-charter/article/41-right-good-administration#national-constitutional-law (last visited Mar. 5, 2025). In Finland, there is a reference to the Right to GA also in Chapter 2 of the Administrative Procedure Act is titled '*Grunderna för god förvaltning*' meaning 'Foundations of good administration', which includes – among the others – the principles of equality, objectivity, proportionality, and the protection of legitimate expectations. See: Oikeusministeriö, *Förvaltningslag*, SDK 434/2003 (2003). On the other hand, in Denmark and Sweden, the Right to GA is not present in the Constitution. However, the principles informing this right are recalled in the Danish Administrative Procedure Act. See: Justis- og beredskapsdepartementet, *Lov om behandlingsmåten i forvaltningssaker – Forvaltningsloven*, LOV-1967-02-10 (1970). Similarly, the Swedish Administrative Law Act lists the principles informing this right are there listed and recalled. See: Justitiedepartementet, *Förvaltningslag*, 2017:900 (2019).

[81] Regarding the principles of publicity and transparency, it is worth noting that, in modern states, '*access to administrative acts and documents forms the foundation of administrative democracy, where transparency counters secrecy driven by personal or group interests*' (author's translation). See: M.A. Sandulli, *Accesso alle notizie e ai documenti amministrativi,* in Enciclopedia del Diritto, Giuffrè (4th ed. 2000).

[82] Most legal systems worldwide recognise the right to access administrative documents and impose transparency obligations, aimed at both enabling oversight of public action and protecting the rights of citizens. The so-called 'transparency model', introduced in the U.S. with the 1966 Freedom of Information Act, has gradually spread globally. For a comparative analysis of the principles underpinning the Right to GA, see: G. Napolitano, *Introduzione al diritto amministrativo comparato*, Il Mulino (1st ed. 2020).

[83] On the relationship between transparency and procedural instruments, see: E. Casetta, *Manuale di Diritto Amministrativo*, Giuffrè, (27th ed. 2024).

this. Since accessing to FM source code is typically restricted[84] or, when available, not easily interpretable,[85] this research considered the principles of publicity and transparency to be fulfilled when the guidelines mention the need for civil servants to disclose the use of FMs.[86] As anticipated, when it comes to the right to be given reasons, the challenges get even more complex. As stated by both supranational and national case law, individuals must be able to understand and challenge automated decisions.[87] This requires explainability, which current FMs cannot guarantee. For this reason, as previously noted, the research limited its scope to G2G uses of FMs, where decisions do not directly affect the juridical sphere of citizens. It shall be pointed out, moreover, that several guidelines refer to the use of GenAI for data analysis. While this use presents challenges, it cannot be categorically excluded without foregoing operational benefits. On the matter, the author believes that rejecting FM-based tools entirely would disregard their value, particularly in enhancing data analysis capabilities.[88] That said, the right to be given reasons was deemed respected in cases where guidelines clearly stated that FMs cannot be used for decision-making (G2C), only humans must remain responsible for a final decision and emphasised the accountability of civil servants in reviewing and interpreting FM outputs.
The second set of corollaries relates to efficiency, effectiveness, and cost-effectiveness, understood as the need for administrative action to achieve optimal results through the best possible use of available resources.[89] For the purposes of this research, the notion of 'resources' was intended not only as human and financial resources, but also as natural ones. Accordingly, the concepts of efficiency and cost-effectiveness are interpreted broadly, including also environmental sustainability. This set of corollaries was considered fulfilled when guidelines referred to the potential of FM-based tools to improve performance and reduce time and costs, and/or to the environmental impact of FMs and corresponding mitigation strategies. In addition, the corollaries were deemed met when the guidelines included a definition of FMs (and its peculiarities) as well as specific examples of potential use cases. Such examples, in the view of the author, reduce uncertainty for public officials by clarifying the appropriate scope of FM applications.
Impartiality, objectivity, fairness and non-discrimination are part of the third set of principles isolated from Article 41 of the EU Charter – all of which are substantial to ensure equality and protect individuals from arbitrary or discriminatory treatment[90].

---

[84] This is true in the case of proprietary or only open-weight FMs. See: E. Gibney (2025). *Supra*, note n. 63.
[85] See: paragraph II.II.
[86] This is in line with Article 50, par. 4, AI Act.
[87] *Supra*, note n. 27.
[88] It should be noted that, under Article 6(3) of the AI Act, AI systems used solely in preparatory phases, without making the final decision, are not classified as 'high-risk'. However, this exclusion appears not entirely justified. When such systems are used within domains listed in Article 6 and Annex III of the Regulation, they can significantly influence outcomes, even if they do not directly determine them. In these contexts, preparatory tools like FMs used to carry out data analysis may meaningfully shape the decision-making process, thereby affecting the legal or factual situation of individuals. Accordingly, they should be treated as high-risk.
[89] On the relationship between these principles, some scholars say that *'[...] il risultato è nozione riassuntiva del concetto di efficienza (oltre che di quello di efficacia ed economicità)*' to the point that the administrative action shall translate '[...] *concretamente nel migliore utilizzo possibile dei mezzi e delle risorse disponibili da parte dell'amministrazione'*. See: D. Vese, *L'efficienza dell'organizzazione amministrativa come massimizzazione dei diritti fondamentali,* P.A. Persona e Amministrazione, 1 (2019).
[90] According to some authors, the principle of impartiality is the application of the principle of legal equality. See: S. Lariccia, *Il principio di imparzialità delle pubbliche amministrazioni*, in U. Allegretti, L. Ammannati, *et al*., *Studi in onore di Giorgio Berti*, Jovene, Napoli, 2005. Note that the issues of bias and hallucinations also have a direct impact on the administrative activity. If GenAI would be used to support the adoption of administrative decisions, the use of discriminatory models could lead to their annulment for abuse of power.

However, the intrinsic bias and risk of hallucinations associated with FMs challenge these corollaries. For this reason, they were considered fulfilled when guidelines explicitly addressed such risks and raised awareness among civil servants on the matter.
Lastly, the fourth set of corollaries – though not traditionally linked to the Right to GA – emerges from an evolutionary interpretation of Article 41 read in conjunction with Article 8 of the Charter (titled 'Protection of Personal Data'), the GDPR, and the NIS2 Directive. In this context, data protection and cybersecurity form a 'necessary and powerful duo',[91] as robust cybersecurity is essential to safeguard personal data. Ensuring data protection, however, also requires civil servants to be aware of what information is appropriate to include in prompts when interacting with FMs.[92]

Table 1 – Visual representation of the corollaries derived from the Right to GA

| Mentioned aspects | Corollaries met |
|---|---|
| **Saying when GenAI is used** | Publicity and transparency |
| **Final decision taken by humans** | Motivation |
| **Optimised resource use* and improved performance** | Efficiency, effectiveness and cost-effectiveness |
| **Definitions and potential use cases included** | Efficiency and effectiveness: reduced risk of uncertainty |
| **Bias and hallucinations** | Impartiality, objectivity, fairness, non-discrimination |
| **Privacy and cybersecurity measures** | Data protection and cybersecurity |

*including environmental resources

*Source: author's own elaboration*

The four sets of corollaries outlined above provide the analytical framework for the qualitative thematic analysis conducted on the selected national guidelines. The results of this analysis will be presented in the next section.

## IV. A Taxonomy of National Guidelines on FMs – Denmark, Finland, Poland, Sweden: Key Findings

The present section presents the results of the thematic qualitative analysis carried out on the four selected guidelines. The Danish ones were adopted in March 2024[93] by *Digitaliseringsstyrelsen*, the Danish Agency for Digital Government.[94] In September of the

See: B.M. Armiento, *Pubbliche amministrazioni e intelligenza artificiale. Strumenti, principi e garanzie*, Editoriale Scientifica, Napoli (1st ed. 2024).

[91] W. Wiewiórowski, Cybersecurity and Data Protection: a necessary and powerful duo, European Data Protection Supervisor, available at https://www.edps.europa.eu/press-publications/press-news/blog/cybersecurity-and-data-protection-necessary-and-powerful-duo_en (last visited May 9, 2025).

[92] This notwithstanding the fact that subscription FMs claim not to retain data for training because public administrations should be the most careful.

[93] Digitaliseringsstyrelsen (2024). *Supra*, note n. 30.

[94] It was established in 2011, and starting from mid-December 2022 the Agency became part of the Ministry of Digital Government. For more, see: Digitaliseringsstyrelsen, *About the Agency for Digital Government*, available at: https://en.digst.dk/about-us/ (last visited May 3, 2025).

same year, Polish ones[95] were published by the *Ministerstwo Cyfryzacji*, the Polish Ministry of Digital Affairs.[96] More recent are the Swedish and Finnish ones. The former were adopted in January 2025 [97] by *Myndigheten för digital förvaltning* (Digg) and *Integritetsskyddsmyndigheten* (IMY) –[98] the Swedish Digital Governance Agency and the Privacy Protection Agency respectively.[99] The latter were published in March 2025 by *Valtiovarainministeriö*, the Finnish Ministry of Finance.[100]

IV.1 *Disclosure Requirements*

All guidelines require, to varying degrees, that civil servants disclose when content has been generated using FMs. Denmark gives public managers the choice to either pre-approve GenAI tools or mandate disclosure in outputs.[101] Finland requires open disclosure, though it is unclear whether this targets managers, the public, or both.[102] Poland explicitly mandates identification of the tool used, the date of generation, and whether human review occurred,[103] whereas Sweden is less specific, merely referring to 'communication' as part of building trust and ethical use, without outlining concrete obligations.[104]

IV.2 *Human Oversight*

The need for human decision-making is highlighted across all the guidelines, though with some peculiarities. For instance, Danish guidelines place the responsibility for the proper use of FM tools primarily on managers of each public entity, thereby partially shifting accountability away from civil servants. While they refer to the right not to face fully

[95] Ministerstwo Cyfryzacji, *Generatywna sztuczna inteligencja w służbie pracowników administracji publicznej - pierwsze kroki,* available at: https://www.gov.pl/web/ai/generatywna-sztuczna-inteligencja-w-sluzbie-pracownikow-administracji-publicznej---pierwsze-kroki (last visited May 3, 2025).

[96] See: Gov.pl, *Ministerstwo Cyfryzacji*, available at: https://www.gov.pl/web/cyfryzacja (last visited May 3, 2025).

[97] The exact date is not listed on the official webpage of the guidelines but is reported in the following press release: Regeringskansliet*, Regeringen har tagit emot nationella riktlinjer för generativ AI*, available at: https://www.regeringen.se/pressmeddelanden/2025/01/regeringen-har-tagit-emot-nationella-riktlinjer-for-generativ-ai/ (last visited May 3, 2025).

[98] The adoption of the Swedish Guidelines was specifically prompted by a directive from the Ministry of Finance to the Digital Governance Agency and the Privacy Protection Authority. See: Regeringskansliet, *Uppdrag till Myndigheten för digital förvaltning och Integritetsskyddsmyndigheten att ta fram riktlinjer för användningen av generativ artificiell intelligens inom den offentliga förvaltningen*, available at: https://www.regeringen.se/regeringsuppdrag/2024/08/uppdrag-till-myndigheten-for-digital-forvaltning-och-integritetsskyddsmyndigheten-att-ta-fram-riktlinjer-for-anvandningen-av-generativ-artificiell-intelligens-inom-den-offentliga-forvaltningen/ (last visited May 3, 2025). The initiative followed the acknowledgement by the said Ministry of an increasing diffusion of GenAI tools in Swedish public administrations. See: Regeringskansliet, *Ökad användning av generativ AI inom offentlig sektor*, aailable at: https://www.regeringen.se/pressmeddelanden/2024/07/okad-anvandning-av-generativ-ai-inom-offentlig-sektor/ (last visited May 3, 2025).

[99] Digg and IMY, *Riktlinjer för generativ AI inom offentlig förvaltning*, available at: https://www.digg.se/ai-for-offentlig-forvaltning/riktlinjer-for-generativ-ai (last visited May 3, 2025).

[100] Valtiovarainministeriö, *Ohjeistus generatiivisen tekoälyn hyödyntämisestä työn tukena ja apuvälineenä julkisessa hallinnossa,* available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/166199/VM_2025_9.pdf?sequence=1&isAllowed=y (last visited May 3, 2025).

[101] Digitaliseringsstyrelsen (2024). *Supra*, note n. 30.

[102] Valtiovarainministeriö (2025). *Supra*, note n. 93.

[103] Ministerstwo Cyfryzacji (2024). *Supra*, note n. 88.

[104] Digg and IMY (2025). *Supra*, note n. 92.

automated decisions, they then open for an exception 'if the assessment criteria are unambiguous or if there is a basis in national or EU law.'[105] This caveat is particularly problematic: as clarified, FMs cannot guarantee meaningful explanation of their output, thus this provision in the Danish guidelines is believed to possibly undermine the right to motivation.

Finland clearly states that officials remain fully responsible for decisions involving FMs and warns that the closer such tools are used to take decisions affecting individual rights, the stricter the limitations must be[106]. While this specification is surely right, further clarification would be needed on what constitutes such thresholds and which uses are prohibited.

Poland implicitly excludes decision-making from FM use by focusing only on summarisation and content creation, but fails to provide an explicit prohibition, leaving a problematic interpretive gap from which potential misinterpretation could derive.[107]

Finally, the Swedish guidelines explicitly call for a human-in-the-loop approach and provide, as an example, the possibility of having employees reviewing content generated by FMs. However, like the Danish ones, they are open to the possibility of using such tools if permitted by specific laws. This would be possible – they specify – only if such decision-making meets the requirements of proportionality, objectivity, and legality, ensuring that those decisions are predictable and free from irrelevant considerations.[108] This position is somewhat contradictory, as the opacity of FMs makes it unlikely that decisions could ever be truly 'predictable' in a way that fully upholds the right of a motivated administrative decision.

### IV.3 *Efficiency broadly considered*

All the analysed guidelines see the potential of FMs in relation to efficiency, effectiveness, and cost-effectiveness.

The Danish guidelines include a 'fact box' explaining how GenAI tools work, along with a visual chart distinguishing AI model – both enhancing conceptual clarity. They acknowledge the potential of FMs as a 'good chance' for improvement but merely list example use cases (e.g., automating repetitive tasks, data analysis, content generation)[109] without further detail.

Similarly, the Finnish guidelines acknowledge the potential productivity gains from using FMs and provide public employees with a clear 'AI vocabulary' through a dedicated terminology table, and they outline several use cases (mainly internal, such as content generation, data analysis, and summarisation). One external use is also mentioned: chatbots for citizen support. While it falls out of the scope of present research, it is worth saying that such use could be considered low risk as it does not affect the juridical sphere of citizens directly. Notably, the Finnish tool also includes a unique example not found in other policies: using FMs for shift planning within departments.[110]

The Polish guidelines offer a brief but accessible definition of GenAI, suitable for non-experts.[111] While they do not explicitly outline efficiency benefits coming from FMs, they

[105] Digitaliseringsstyrelsen (2024). *Supra*, note n. 30.
[106] Valtiovarainministeriö (2025). *Supra*, note n. 93.
[107] Ministerstwo Cyfryzacji (2024). *Supra*, note n. 88.
[108] Digg and IMY (2025). *Supra*, note n. 92.
[109] Digitaliseringsstyrelsen (2024). *Supra*, note n. 30.
[110] Valtiovarainministeriö (2025). *Supra*, note n. 93.
[111] It refers to GenAI as a tool that can be used to produce content. It also warns that the output is based on training dataset as well as prompts. See: Ministerstwo Cyfryzacji (2024). *Supra*, note n. 88.

provide detailed use cases, each accompanied by a warning on related risks –[112] an approach that could be extremely effective to reduce uncertainty in civil servants on what and what is not allowed.
Lastly, Swedish guidelines offer a clear definition of GenAI but the governance tool appears overall lengthy, fragmented, and it lacks detailed use cases of FMs. The Swedish approach, however, stands out for addressing the environmental impact of AI, urging administrations to assess sustainability and energy use on a case-by-case basis.[113] Similarly, while Finnish guidelines do not refer explicitly to the environment, they also make a reference to the fact that GenAI is not always the answer, yet in some cases other models would be more adequate.[114]

IV.4 *Impartiality and Fairness*

On impartiality, objectivity, fairness and non-discrimination, the Danish guidelines warn of hallucinations and bias risks, especially when using closed-source or publicly available models with limited transparency on training data. To address this, civil servants are advised to perform 'quality control' on all outputs.[115]
The Finnish ones highlight the risk of hallucinations, stressing the need to always verify FM outputs. They also address bias, noting its correction is crucial yet challenging with GenAI due to its opacity, which makes discriminatory outcomes harder for users to detect. To de-bias output, however, Finland does not dive into any practical tools to help civil servants deal with it.[116]
The Polish guidelines similarly highlight bias risks in FM training datasets and instruct officials to always verify outputs.[117] Hallucinations are also addressed: civil servants are encouraged to cross-check outputs with reliable sources or consult domain experts.[118]
Sweden, on the other hand, links hallucinations and bias to GDPR principles of correctness and accuracy, instead of relating these to the Right to GA.[119] It also provides no tools for identifying or mitigating such risks.

IV.5 *Privacy and Cybersecurity*

Lastly, on privacy and cybersecurity, Danish guidelines highlight the risk of data leakage when interacting with publicly accessible FMs. Civil servants are instructed to avoid inputting personal or confidential information and to use separate passwords for GenAI platforms. To strengthen safeguards, managers are encouraged to provide an approved list of GenAI tools, clarify permissible data inputs, and offer examples of acceptable and unacceptable prompts.[120]

---

[112] Specifically, this includes using GenAI as a source of inspiration (e.g., finding a project title), for summarising information, or conducting preliminary research on unfamiliar topics. *Id.*
[113] Digg and IMY (2025). *Supra*, note n. 92.
[114] Valtiovarainministeriö (2025). *Supra*, note n. 93.
[115] Digitaliseringsstyrelsen (2024). *Supra*, note n. 30.
[116] Valtiovarainministeriö (2025). *Supra*, note n. 93.
[117] The Polish guidelines refer to this issue as one of '*bezstronność*' (impartiality), supporting the present study's alignment of concerns about bias and hallucinations with the corollaries of impartiality, fairness, and non-discrimination. See: Ministerstwo Cyfryzacji (2024). *Supra*, note n. 88.
[118] *Id.*
[119] Digg and IMY (2025). *Supra*, note n. 92. Finland, by contrast, recalls specifically the principles of the right to GA, calling civil servants to always refer to them, also when using GenAI. Valtiovarainministeriö (2025). *Supra*, note n. 93.
[120] Digitaliseringsstyrelsen (2024). *Supra*, note n. 30.

Similarly, Finnish ones warn not to input in the FM tool confidential, non-public or personal data unless the tool has been approved by the organisation.[121]
The Polish guidelines prohibit entering classified, sensitive, or personal data into GenAI tools, warning that providers may store or reuse input content. However, their cybersecurity advice is vague – civil servants are simply told not to 'post content [they] wouldn't normally post on social media'. No concrete safeguards are outlined, and the only reference is to an external link on 'cyber hygiene'. As such, this fourth set of governance corollaries is only partially addressed in the Polish case.[122]
Sweden provides the most comprehensive guidance: it places liability on public bodies for any data leaked to private providers and mandates prior risk assessments, ongoing risk management, incident reporting, and technical safeguards such as encryption and access control.[123]

### IV.6 *Additional Observations*

Though not initially part of the thematic analysis, it is worth mentioning that all guidelines stress the importance of a compliance with intellectual property rights. This emerging focus suggests a broader trend toward embedding FM-related use within a rights-based framework of administrative legality[124].

## V. Final Reflections and Policy Considerations

The comparative review and qualitative thematic analysis undertaken in this study reveal an emerging institutional awareness of both the opportunities and risks associated with the integration of foundation models in public administration. Importantly, the findings indicate that ensuring alignment of these technologies with the corollaries of the Right to Good Administration necessitates structured and forward-looking governance strategies that translate legal principles into operational practice. In light of the best practices identified in the previous sections, the following policy considerations and recommendations are proposed.
To enhance efficiency and institutional effectiveness, guidelines should include clear and accessible definitions of foundation models (and related concepts). The Danish visual classification of AI types represents a notable best practice in this regard. In addition, civil servants would also need practical, context-specific guidance delineating permitted uses, prohibited applications. On the matter, grey areas would then require managerial oversight. Providing detailed illustrative use cases appears to be crucial to reduce uncertainty and support adequate and effective use of FMs by civil servants.
With respect to automated decision-making, the Danish and Swedish approaches recalled above – both of which allow exceptions when national or EU law permits – risk being overly permissive, as they fail to align with the opacity of current foundation models. As of today, therefore, a precautionary principle should apply: FMs could assist with content creation, summarisation or trend analysis, but should not be deployed for decisions directly affecting the rights or legal interests of individuals. In any case, human oversight shall be guaranteed, even when FMs are employed solely for internal administrative

121 Valtiovarainministeriö (2025). *Supra*, note n. 93.
122 Ministerstwo Cyfryzacji (2024). *Supra*, note n. 88.
123 Digg and IMY (2025). *Supra*, note n. 92.
124 Digg and IMY (2025). *id*; Digitaliseringsstyrelsen (2024). *Supra*, note n. 30; Valtiovarainministeriö (2025). *Supra*, note n. 93; Ministerstwo Cyfryzacji (2024). *Supra*, note n. 88.

support. This solution is believed to safeguard the right to motivated administrative decisions.

Consistently with the corollaries of transparency and publicity, guidelines should also include disclosure obligations. This would require civil servants to clearly indicate how and when content or analysis has been generated using FMs – both internally (to their supervisors) and externally (to the public). This solution would strengthen accountability and public trust in administrative processes, while reducing potential ambiguities in FM use. Additionally, disclosure enables traceability: when errors occur, administrators can determine whether they originated from FM outputs and, based on documented patterns, decide to restrict or exclude specific uses that prove unreliable or legally problematic.

Given the risks of bias and hallucinations inherent in FMs, governance measures should explicitly address these challenges. Civil servants must be required to verify outputs critically, and public authorities should prioritise the use of open-source or auditable models where possible.

When it comes to privacy and cybersecurity, robust data governance and cybersecurity protocols constitute essential safeguards. These include pre-deployment risk assessments, encryption, access control, and incident reporting mechanisms. Civil servants must be instructed to avoid inputting unauthorised or confidential data into FMs unless expressly permitted. On the matter, the lifecycle approach adopted in the Swedish guidelines offers a strong model to follow.

Importantly, sustainability considerations must also be carried out by public administrations. Civil servants should be aware of the ecological footprint of FMs deployment, including energy consumption, water usage and carbon emissions. The Swedish and Finnish guidelines offer promising examples by urging limitations and proportionality in FM use. Rather than a 'FMs-by-default' model, therefore, a principle of FMs-minimisation shall be favoured – meaning using these tools *only* when necessary, appropriate, and proportionate, not simply whenever possible.

Lastly, iterative review and continuous updating of guidelines will be critical. Public authorities should systematically integrate lessons learned, re-evaluate compliance with the corollaries of Article 41, and adapt governance measures in response to the evolving technical and legal landscapes.

The analysis confirms that existing guidelines constitute a crucial tool – at least in theoretical terms – for compliance with the corollaries of the Right to Good Administration. Their practical effectiveness, however, will ultimately depend on the extent to which they are actively integrated into the daily practices of civil servants. Assessing this dimension, including the role of formal training and capacity-building measures, opens a path for future investigation.

# AI IN THE LEGAL MARKET: ADDRESSING LEGAL AMBIGUITY THROUGH A CONSUMER-CENTRIC LENS

*Giovanni Chieco*[1]

TABLE OF CONTENTS:



*The legal classification of AI-based LegalTech tools (LT) under EU law remains uncertain, with major implications for liability allocation and consumer protection. The present article addresses this ambiguity through a consumer-centric and systematic interpretation of the EU legal framework, arguing that the qualification of LT as services or products cannot be determined in abstract terms but must depend on their mode of deployment—particularly on whether they are used by legal professionals or directly by consumers. The analysis first surveys the principal applications of LT within the European legal services sector and outlines the EU rules applicable to these technologies irrespective of their classification. It then examines the legal consequences of categorizing LT as services or products in two distinct scenarios: when AI systems are integrated into professional legal services, and when they are marketed directly to consumers as autonomous digital solutions. The article contends that a use-based, consumer-oriented approach offers the most coherent and protective framework. When employed by lawyers, LT should be treated as components of the service and governed by professional and contractual liability regimes. Conversely, when deployed autonomously by end-users, they should be regarded as digital products subject to EU product-related consumer protection rules. By aligning legal regimes with the risk profiles associated with different LT users, and building on a critical reading of the relevant EU legal landscape, the paper aims to promote an approach that reinforces legal certainty and ensures a coherent level of protection for clients and consumers, despite the absence of a clear categorization and a dedicated sector-specific framework for AI-enabled legal services.*

**Keywords**: LegalTech Tools – AI Law – Legal Services – EU Digital Framework

## I. INTRODUCTION

Artificial Intelligence (AI) is progressively reshaping the legal sector through the deployment of AI-powered LegalTech tools (LT), increasingly adopted by both legal professionals and consumers. In professional settings, LT enhance efficiency and productivity in multiple domains. They assist lawyers not only with basic document management tasks but also enable advanced legal research, using natural language processing algorithms to identify relevant statutes, case law, and scholarly references.[2] Moreover, LT can perform document analysis, encompassing contract review, due diligence, and compliance checks, identifying inconsistencies, key terms, or potential legal risks. Predictive analytics tools further support strategic decision-making, evaluating potential legal outcomes and informing risk assessments.[3] Lastly, LT can even

[1] PhD Candidate in Applied Data Science and Artificial Intelligence at the University of Trieste. E-mail: Giovanni.Chieco@phd.units.it

[2] D. Schwarcz et al., *AI Tools for Lawyers: A Practical Guide*, Minn. L. Rev., 2023, pp. 7–10.

[3] I. Atrey, *Revolutionising the Legal Industry: The Intersection of Artificial Intelligence and Law*, Int'l J.L. Mgmt. & Human., 2023, pp. 1075–1083.

autonomously generate tailored legal documents—such as contracts or motions—based on user's input, streamlining highly technical processes.[4]

By automating repetitive tasks, LT boost lawyers' productivity, enabling even small and medium-sized firms to serve more clients and expand into practice areas or client segments previously inaccessible due to knowledge, capacity, or staffing limits. Furthermore, the time and cost savings generated by these efficiencies could be passed on to clients through lower fees or flat-fee service options, potentially widening access to legal services for those who have historically been excluded[5]. This interconnected scenario enhances overall legal market competitiveness, creating—according to liberal economic theories—a win-win situation: consumers benefit from lower prices, improved quality, greater choice and better service, while businesses are incentivized to innovate, improve efficiency and remain relevant.[6]

Beyond their adoption by legal professionals, LT are increasingly accessible directly to consumers via online platforms, chatbots, and self-help applications.[7] These tools commodify legal knowledge into user-friendly, interactive formats, enabling consumers to prepare documents, assess the merits and risks of claims, and make informed decisions independently.[8] Offering 24/7 availability, geographic flexibility, and greater cost transparency, LT could help overcome social, cultural, and psychological barriers that traditionally limit engagement with the justice system, broadening access to legal assistance[9]—with the sole limitation that certain legal activities still require the personal authorship of a lawyer.

Despite the clear benefits of LT, their full potential remains constrained by legal uncertainty surrounding their classification as products or services. This ambiguity slows adoption and heightens perils linked to their development and deployment. To address these risks, this paper argues that national authorities and courts should adopt a consumer-centric approach: ambiguous LT outputs should be interpreted as products when they are used directly by end-users, while systems employed by lawyers should be treated as integral components of professional services. Such an approach not only aligns with core EU consumer protection principles but also enhances legal certainty and fosters trust in digital legal services.

To this end, the present paper begins by examining the main drawbacks of LT, as understanding these limitations is essential to assess the practical implications of the classification at stake (paragraph 2). Having clarified these aspects, the analysis proceeds with a brief examination of key EU provisions applicable to LT regardless of their categorization as services or products (paragraph 3). Indeed, such an overview represents a necessary preliminary step to determine the areas in which the legal classification at issue produces significant effects. At this stage, the discussion is sufficiently mature to address

[4] DRI, *Artificial Intelligence in Legal Practice: Benefits, Considerations, and Best Practices*, DRI, 2024, p. 89, available at https://www.dri.org/docs/default-source/dri-white-papers-and-reports/ai-legal-practice.pdf (last visited Jan. 23, 2026).

[5] N. Yamane, *Current Developments: 2019–2020: Artificial Intelligence in the Legal Field and the Indispensable Human Element Legal Ethics Demands*, Geo. J. Legal Ethics, 2020, pp. 885–888.

[6] D. Ferrar, *How AI Is Empowering Small Law Firms*, Artificial Lawyer. Legal Tech & AI News, 2025, p. 1, available at https://www.artificiallawyer.com/2025/04/11/how-ai-is-empowering-small-law/ (last visited Jan. 23, 2026).

[7] M. Fenwick et al., *The Lawyer of the Future as 'Transaction Engineer': Digital Technologies and the Disruption of the Legal Profession*, in M. Corrales et al. (eds), *Legal Tech, Smart Contracts and Blockchain*, Springer, Singapore, 2019, p. 255.

[8] Q. Steenhuis, *AI and Tools for Expanding Access to Justice*, in *The Cambridge Handbook of AI in Civil Dispute Resolution* (forthcoming, CUP), 2024, pp. 6–8.

[9] R. H. Brescia et al., *Embracing Disruption: How Technological Change in the Delivery of Legal Services Can Improve Access to Justice*, Alb. L. Rev., 2015, pp. 572–575.

the two interpretive paths available under EU law: classifying LT either as products or as services. Therefore, the paper first examines the implications of categorizing LT outputs as either services or products when used by legal professionals during their professional activities, highlighting the rationale behind these classifications and the relevant legal considerations (paragraph 5). Subsequently, the paper analyzes the implications of labeling LT directly utilized by consumers as either products or services, assessing potential benefits and drawbacks associated with each line of reasoning (paragraph 6). Based on the conclusions drawn from the inquiry, the paper then argues that the most appropriate approach is probably the one that prioritizes consumer protection. National authorities and courts should adopt a consumer-centric perspective, interpreting ambiguous LT as products when such classification affords consumers a higher level of protection. Conversely, when LT are employed in the delivery of professional legal services, they ought to be regarded as integral components of the lawyer's service provision. This consumer-oriented framework not only aligns with fundamental principles of EU consumer protection law but also promotes legal certainty and trust in digital legal services (paragraph 7).

## II. THE DRAWBACKS OF THE DIFFUSION OF LT IN LEGAL SERVICES WORLD

Despite the positive effects of LT diffusion in the legal services sector, AI-powered tools can also exacerbate existing risks and give rise to new vulnerabilities for clients and, especially, for consumers as end-users. This underscores the urgent need for a clear rights-protecting legal framework to mitigate such risks and legal uncertainty. In the absence of which, it falls to courts and academic scholarships to clarify the issues at stake and to advocate for a consumer-centric approach to the regulation of these technologies.

The dangers of LT seem to be related, in part, to their technical structure and, in part, to the lack of users' competence and means.

Let us start from AI's intrinsic technical problems. The fact that AI tools need to be trained on large amounts of data is a first structural limitation that affects the quality and accuracy of their responses as well as the privacy rights of the people concerned. The correctness of any answer depends on the data used to train the model: an algorithm cannot learn from information it was not exposed to. This limitation gives rise to a phenomenon known as exposure bias: models trained on specific dataset perform poorly when confronted with unfamiliar inputs, failing to interpret new data creatively and accurately. The issue is particularly problematic for generative AI, as the text they generate becomes part of the underlying data used for subsequent predictions. Consequently, an erroneously generated sentence can exponentially affect the accuracy of future predictions.[10]

Similarly, generative AI systems have exhibited a tendency to fabricate facts or legal information when faced with gaps in their knowledge. In the legal field, these hallucinations may result in the fabrication of fictitious court decisions or the misinterpretation of applicable legal provisions.[11]

What further undermines the accuracy of the outputs is the unstructured nature of legal data. Legal texts are often highly contextualized and polycentric, with significant variation in writing styles and reasoning approaches across lawyers, judges and jurisdictions. This variability, which is particularly acute in multi-cultural and multi-lingual Europe, can make

[10] C. Griffin et al., *A Preliminary Agenda for Using Generative AI to Improve Access to Justice*, Judicature, 2024, pp. 43–51.

[11] *Ibid.*, 47.

it difficult to identify consistent patterns and facilitating imprecise and uncontextualized outcomes.[12]

LT's technical architecture does not only impinge on the accuracy of the outcomes but also exposes users and clients' privacy rights to serious risks. LT are trained on large amounts of data, which may include personal data. Without proper oversight, there is the risk that this personal information could be stolen, processed or used to train AI models without prior notification or consent.[13] The risks for privacy are exacerbated by the fact that unstructured legal data are very difficult to anonymize: simply removing names and locations is not sufficient, as unique events or other context-specific information may make it possible to re-identify subjects. Consequently, privacy risks persist even if a data service provider anonymizes all stored data before using it. Furthermore, even if the output of training does not appear to be legible data at all, it is important to be mindful of the problem that the output of popular language embeddings can be used to predict the original text used for (pre)training and reverse-engineer to disclose sensitive information from the source.[14]

Furthermore, serious privacy and cybersecurity concerns arise from the most common way to create and/or deploy LT, which implies reliance on cloud computing services. Cloud computing-based tools are popular because they eliminate many of the difficulties and costs related to implementation and maintenance of technical infrastructure needed to use or build AI tools.[15] However, there are numerous privacy perils associated with this type of technology. Aside from the extraterritoriality problems, which, although still present, is mitigated by the Regulation 2016/679/EU (GDPR), a particularly widespread risk is unauthorized access to data. As long as the service provider (or any underlying infrastructure) has the technical ability to access and read the data, a data breach could not be excluded. Nor should the perils of *vendor lock-in* be underestimated: technical barriers or the behavior of the cloud provider can create serious difficulties in extracting and moving the data. Notwithstanding recent interventions, such as the Regulation 2022/868/EU (Data Act) and the Regulation 2022/858/EU (Data Governance Act), recovering the full set of uploaded data or transferring it intact to another provider can be particularly challenging.[16]

As anticipated, the other big potential source of risks associated with LT stems from the amounts of skills and resources that are required to manage them. Indeed, the accuracy and efficiency of LT depends, at least in part, on the level of competencies and means possessed by users–be they legally trained or not.

It seems evident that the lawyers' position differs from that of people lacking legal training, since lawyers' legal knowledge mitigates the risks associated with the use of incorrect AI-generated legal outputs. However, a factor that has the potential to create new vulnerabilities and limit the usefulness of LT, even for lawyers, is the technological skill gap. The successful adoption of LT requires technical proficiency and a deep understanding of the model, in the absence of which their utilization may easily turn out

[12] J. Gardner, *The Many Faces of Reasonable Person*, L.Q. Rev.*, 2025*, pp. 131–132.
[13] DRI, 2024, pp. 23–26.
[14] X. Pan et al., *Privacy Risks of General-Purpose Language Models*, IEEE Symposium on Security and Privacy, 2020, pp. 1314–1315, available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152761 (last visited Jan. 23, 2026).
[15] CCBE, *CCBE Considerations on the Legal Aspects of Artificial Intelligence*, CCBE, 2020, p. 3, available at https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf (last visited Jan. 23, 2026).
[16] *Ibid.,* pp. 44-48.

to be counterproductive, expensive and dangerous for clients' rights and for lawyers' reputation.[17]

Having adequate resources is another essential requirement for fully leveraging the potential of LT while minimizing its drawbacks. To gain a genuine marketable advantage, law firms should either use reliable yet costly LT, or, though at a significantly higher cost, develop their own proprietary tools exclusively for the benefit of their clients. Small law firms, however, are unlikely to be able to develop their own LT; more likely they will rely on ready-to-use third-party AI. In the long term, this reliance may undermine their independence. Lawyers who become reliant on a single tool for key aspects of their business processes may face interference from the AI provider in their professional activities and relationships with clients: the tech company could impose unilateral terms, potentially undermining lawyers' independence, professional judgment, authority, and reputation.[18]

The mentioned aspects have led many to think that LT will likely lead to the development of two-tiered systems of access to legal services[19]. Three predominant concerns regarding such scenario have emerged in the literature: (i) one in which expensive, but superior, human lawyers coexist with inexpensive, but inferior, AI-driven legal assistance;[20] (ii) one where only large law firms will effectively harness superior but expensive AI, thereby increasing their power and making more affordable service providers obsolete;[21] and (iii) one where AI's impact will not overcome the *status quo* and there will continue to be only a small portion of the public that can afford quality legal services, which are offered worldwide by few law firms.[22] None of these scenarios is particularly reassuring.

Even more serious are the vulnerabilities arising from the lack of sufficient legal and technological literacy among legally untrained LT users. Lay users typically do not have enough legal knowledge and technological skills to verify the automated answers. Therefore, they are always exposed to the risk of relying on technological systems that do not meet their needs, potentially exposing them to unintended and unexpected consequences[23]. Furthermore, even assuming that the legal information provided by the tool is correct, simply having easy access to legal knowledge through AI-generated answers is often not sufficient to resolve a legal matter. Instead, it is essential to critically analyze the information, its sources and its context, while recognizing that every case is unique and requires a specially designed strategy.[24]

The potential positive impact of these technologies on lay users and the improvement of access to justice is further limited by the fact that many LT companies may use technology

---

[17] IBA, *The Future Is Now: Artificial Intelligence and the Legal Profession*, IBA, 2022, pp. 15–16, available at https://www.ibanet.org/document?id=The-future-is%20now-AI-and-the-legal-profession-report (last visited Jan. 23, 2026).

[18] CCBE, 2020, pp. 51–52.

[19] M. Infantino et al., *AI, Lawyers, and Consumers*, in L. A. Di Matteo et al., (eds), *AI and Consumer Law,* Cambridge University Press, Cambridge, 2024, p. 265.

[20] R. Kunkel, *Rationing Justice in the 21st Century: Technocracy and Technology in the Access to Justice Movement*, U. Md. L.J. Race, Religion, Gender & Class, 2018, pp. 372, 382–383.

[21] F. Pasquale et al., *Four Futures of Legal Automation*, UCLA L. Rev. Discourse, 2015, pp. 35–36.

[22] J. A. Guttenberg, *Practicing Law in the Twenty-First Century in a Twentieth (Nineteenth) Century Straight Jacket: Something Has to Give*, Mich. St. Int'l L. Rev., 2012, p. 480.

[23] H. J. Escajeda, *The Vitruvian Lawyer: How to Thrive in an Era of AI and Quantum Technologies*, Kan. J.L. & Pub. Pol'y, 2020, pp. 472–474.

[24] M. L. Koenig, J. A. Oseid, A. Vorenberg, *Ok, Google, Will Artificial Intelligence Replace Human Lawyering?*, Marq. L. Rev., 2019, pp. 1274–1279.

to determine which cases to pursue and to filter out economically unviable cases or legally risky claims from the outset[25]—excluding the people who might need them the most.
From the points highlighted above, it is clear that the widespread use of LT by lawyers and consumers entails significant vulnerabilities and exacerbates longstanding barriers to access to justice. This situation calls for an adequate legal framework capable of addressing these risks. However, in the absence of clear EU-level regulatory guidance, doctrine and jurisprudence should adopt an approach that mitigates such risks while preserving the technology's benefits. Accordingly, the paper argues that LT should be classified as services when used by lawyers in the provision of legal services, and as products when employed directly by end-users. This dual classification better reflects the service–product distinction and enhances protection for both clients and consumers.

## III. LT AS SERVICES OR PRODUCTS: COMMON PROTECTION LEGAL FRAMEWORK

Before addressing the regulatory differences that arise from the classification of LT as either products or services, it is necessary to clarify the European legal framework applicable regardless of this distinction. Only once the common rules governing the use of LT are identified can the legal implications of their classification be properly understood. This step makes it possible to distinguish clearly between cross-cutting regulatory elements—those that apply irrespective of whether LT are considered goods or services—and those whose applicability depends directly on such classification.
In adopting this perspective, particular attention should be paid to the Unfair Contract Terms Directive (UCTD) 93/13/EEC and the Unfair Commercial Practices Directive (UCPD) 2005/29/EC, which play a crucial role in shaping consumer protection standards. The UCTD seeks to prevent standard terms in business-to-consumer contracts from creating a significant imbalance to the detriment of the consumer (art. 3). It requires terms to be drafted in clear and intelligible language, with any ambiguity interpreted in the consumer's favor (art. 5), and provides that unfair terms are not binding, while the remainder of the contract remains valid if it can continue to operate without them (art. 6). The UCPD establishes protections against commercial conduct that breaches professional diligence, misleads consumers or employs aggressive tactics. Potential violations include misrepresenting staff qualifications, mishandling complaints, lacking fee transparency and coercing or intimidating clients (arts. 6-9). Both texts are concerned with what happens at the precontractual stage and largely disregard whatever problem may occur during or after the performance of a contract. Moreover, neither of them addresses the unique risks posed by digital applications, such as issues related to transparency, quality or accountability. Finally, while the UCTD is arguably the most rigorously enforced EU contract law instrument, the UCPD leaves enforcement largely to the discretion of member States (arts. 11–13) and has notoriously been underenforced.[26] Nonetheless, these instruments offer important baseline protections, ensuring fairness in consumer contracts and promoting trust in digital markets—principles that remain relevant even in the evolving context of LT.
Similarly, the information obligations set out in the Consumer Rights Directive (CRD) 2011/83/EU provide only limited protection for consumers engaging with LT. CRD imposes standardized duties, requiring traders to inform consumers, clearly and comprehensibly, about the characteristics of their products and/or services, pricing and

[25] M. Ebers, *Legal Tech and EU Consumer Law*, in L. A. Di Matteo et al., (eds), *Lawyering in the Digital Age*, Cambridge University Press, Cambridge, 2021, pp. 198–199.
[26] M. Infantino et al., *The Interplay Between the CJEU and National Courts in the Case Law on Unfair Contract Terms in Foreign Currency Loans: A Comparative Overview*, Eur. Rev. Contract L., 2023, pp. 346–348.

associated rights and obligations (arts. 6-8). However, the effectiveness of CRD is significantly constrained in digital contexts, where interactions often occur through software interfaces and information is hidden in standard terms and conditions that everybody accepts but nobody reads. Furthermore, CRD does not provide specific remedies in cases of non-compliance except from the right of withdrawal (arts. 11-16). As a result, enforcement largely depends on the national contract laws of the Member States (arts. 23-24), which may lead to insufficient and inconsistent consumer protection across the EU.[27] Despite its limitations, the CRD contributes to increasing transparency and supporting informed consumer choices in digital environments, thereby fostering trust in the use of emerging technologies such as LT.

Wherever personal data are involved, the development and deployment LT must comply with the General Data Protection Regulation (GDPR) 2016/679/EU, which protects not only consumers but also lawyers. Both the training and deployment of LT are subject to specific obligations: personal data must be processed lawfully, fairly and transparently and must rely on a legitimate legal basis (arts. 5-11). Furthermore, the GDPR grants data subjects a range of rights, including the right to information and explanation, rectification, erasure, objection and data portability (arts. 12-23). However, ML models embedded in most LT typically do not rely on personal data, but rather on abstract patterns and statistical inferences concerning categories of individuals. As the embedded correlations apply generically to individuals sharing similar characteristics, the majority of data used by these applications do not generally fit in the category of personal data and therefore do not trigger the application of the GDPR.[28] As a result, while in theory data subjects can check how their personal data is collected and processed, in practice they have very little control over it (CJEU in *C-434/16*; *C-141/12*; *C-372/12*). Furthermore, article 82 of the GDPR establishes that individuals who suffered material or non-material damage due to violations of the Regulation have the right to claim compensation against the author of the breach, provided that they can prove the breach of the GDPR, the damage suffered and the causal link between the breach and the damage.[29] While the provision offers crucial protection for solo lawyers, clients and consumers, it however presents significant challenges in practice. It sets a very high burden of proof for data subjects, that is even exacerbated in cases involving complex AI-driven processing where the link between the processing of data and the harm may be indirect or unclear. Moreover, the room for exemptions from liability is broad: courts interpret the absence of fault as well as the fact that controllers or processors have taken all reasonable precaution in an extensive way, reducing substantially the possibility of obtaining damages.[30]

Finally, Regulation EU 2024/1689 (AI Act) classifies certain AI systems that involve the interpretation or application of the law as high-risk (art. 6 and Annex III, point 8), subjecting them to a set of obligations, including requirements on risk management, high-quality training data, technical documentation, transparency, human oversight, accuracy, robustness and cybersecurity measures (arts. 9-27). However, LT are not explicitly listed in Annex III, and thus fall outside the defined high-risk categories, evading this regulatory framework. While the Act imposes additional duties on General-Purpose AI (GPAI) models (arts. 51–56), LT do not themselves qualify as GPAI and are therefore largely

[27] A. Biard, *The Age of Consumer Law Enforcement in the European Union: High Hopes or Wishful Thinking?*, Eur. J. Risk Regul., 2023, pp. 625–627.

[28] M. Ebers, 2021, pp. 214–216.

[29] B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, JIPITEC, 2016, pp. 282–290.

[30] T. Karjalainen, *All talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm*, Eur. Data Prot. L. Rev., 2022, pp. 19–30.

exempt from these obligations. The duties in articles 51–56 apply specifically to providers and, in some cases, deployers of GPAI (arts. 3 nn. 63, 66, and recital 97), not to third parties who adapt or integrate GPAI models for narrow, sector-specific purposes and applications, such as legal services provision (recital 100). By contrast, article 50 of AI Act, which imposes transparency obligations on providers of AI systems, particularly those designed for direct interaction with natural persons, applies to LT. Under this provision, providers must ensure that users are informed they are interacting with an AI system, unless this is evident to a reasonably well-informed person considering the context and circumstances of use (recitals 132, 133). However, while this transparency measure represents a step toward user protection, it may be insufficient to address deeper concerns: users may still attribute undue credibility to AI-generated outputs, and its effectiveness relies on the assumption that users are sufficiently informed and attentive, which may not always hold.[31]

The EU law examined thus far offer meaningful protections to LT users, regardless of how these technologies are legally classified. They contribute to building trust in the digital market, safeguarding fundamental consumer rights, and promoting freedom of choice. However, the current framework also reveals significant shortcomings. These include the limited scope of certain instruments, the inadequacy of available remedies, and the wide discretion left to member States in transposing and enforcing EU rules. As such, it is necessary to assess how the classification a stake may help bridge existing legal gaps and whether it does so effectively.

The next sections will explore the legal consequences that stem from this classification, distinguishing between scenarios in which LT are used by legal professionals and those in which they are accessed directly by end-users. The primary objective is to shed light on a complex and largely underexplored legal issue, and to propose an interpretative approach that coherently fits within the EU legal framework and upholds strong safeguards.

## IV. LT IN LEGAL PROFESSION: FUNCTIONAL SERVICES, NOT CONSUMER PRODUCTS

In general terms, although the distinction between goods and services may appear straightforward, clearly defining these concepts has long posed a challenge across various disciplines. Goods are typically understood as tangible, physical items that possess exchangeable value. They can be owned, transferred, and traded, exist independently of their owners, and retain their physical characteristics over time[32]. While the characteristics of goods are relatively well-established, the definition of services remains more contested. Services are often described by four key features: intangibility, heterogeneity, inseparability, and perishability[33]. However, in a technological society, these criteria are increasingly inadequate for clearly distinguishing between products and service[34]. For example, the criterion of intangibility is not enough to distinguish service from products, since digital outputs like AI-generated text are intangible, yet can be stored, copied and distributed like physical goods; or, when a human performs a specific task, it's clearly a service, but when a machine performs it on-demand, instantly, and without ongoing

[31] E. Mišćenić, *Information, Transparency and Fairness for Consumers in the Digital Environment*, in C. Crea et al. (eds), *The New Shapes of Digital Vulnerability in European Private Law*, Nomos, Baden, 2024, pp. 89–126.
[32] G. Parry et al., *Goods, Products and Services*, in M. Macintyre et al. (eds), *Service Design and Delivery*, Springer, 2011, p. 20.
[33] S. Moeller, *Characteristics of Services—A New Approach Uncovers Their Value*, J. Serv. Mark., 2010, p. 359.
[34] M. Loos et al., *The Regulation of Digital Content Contracts in the Optional Instrument of Contract Law*, Eur. Rev. Priv. L., 2011, p. 732.

personal input, it starts to resemble a product—something you "use" rather than "receive".[35]

This ambiguity, exacerbated by the lack of specific indications offered by EU law, highlights the need for clearer legal guidance on how to classify emerging technologies. To this purpose, the paper adopts a user-focused approach to classify LT: in this paragraph, the survey considers whether LT should be treated as product or services when used by lawyers then, in the following one, it will examine their classification when utilized directly by end-users; in both cases, it explores the legal impact of each option, aiming to identify which approach best protects consumer rights and better fits with current EU legal framework.

Despite the aforementioned challenges, when LT are used by lawyers to provide legal assistance, they can hardly be regarded as standalone products, rather than as integral components of a comprehensive legal service. The intrinsic nature of legal services seems to support this perspective, as legal assistance is defined by the exercise of professional judgment tailored to clients' circumstances and accompanied by personal responsibility and ethical oversight. Lawyers' professional duties, liability regimes, and responsibility for acts of supervised collaborators confirm that LT used by lawyers should be considered as part of the service offered: the nature of the relationship and the client's expectations prevail over the technical classification and functioning of the means used to deliver the service.

Starting with lawyers' professional duties, it should be emphasized that these duties are built around lawyer's role and expertise. This circumstance not only reinforces the idea that lawyers provide legal service regardless of the tools employed, but also allows for the regulation of different situations, including evolving ones, to ensure the responsible, appropriate, and lawful delivery of legal services. The duty of competence (e.g., art. 14 Italian Code of Forensic Ethics (ICFE)) requires lawyers to possess not only the necessary legal knowledge and skills for representation but also to ensure the accuracy and reliability of AI-generated outputs. This duty extends to maintaining awareness of available technological tools that may serve the client's interests and performing ongoing oversight in accordance with the "trust but verify" principle.[36] Similarly, the duty of transparency (e.g., art. 35 ICFE) entails that lawyers must communicate clearly with clients about the strategies and technologies employed, including the use of LT. This involves obtaining informed consent, explaining the function, rationale, and potential risks of such tools, and outlining available remedies in the event of errors or complications.[37] The duty of confidentiality (e.g., art. 9 ICFE) also plays a central role, requiring lawyers to understand and mitigate risks related to data security and privacy when using AI. This includes secure data handling, due diligence on AI providers, and contractual safeguards—such as limiting data use to authorized purposes, prohibiting resale or AI training with client data, and mandating robust protection protocols.[38] All the mentioned duties—the violation of which may result in liability for damages caused by lawyers to clients— confirm that, even when certain means, such as LT, are employed in the provision of legal assistance, the central aspect lies not in the tools or technologies used but rather in the role and expertise

[35] J. Hojnik, *Technology Neutral EU Law: Digital Goods within the Traditional Goods/Services Distinction*, Int'l J.L. & Inf. Technol., 2017, pp. 64–66; H.-W. Micklitz, *The Price to Pay for Pick-a-Pack Dependency: Consumer Policy and Law Between Internal Market and Digital-Green Economy*, J. Cons. Pol'y, 2025, pp. 346–349.

[36] DRI, 2024, pp. 9, 18–19; CCBE, 2020, p. 32,

[37] J. Cook et al., *AI-ready Attorneys: Ethical Obligations and Privacy Considerations in the Age of Artificial Intelligence*, U. Kan. L. Rev., 2024, pp. 335–340, 361–363.

[38] D. Simshaw, *Ethical Issues in Robo-lawyering: The Need for Guidance on Developing and Using Artificial Intelligence in the Practice of Law*, Hastings L.J., 2018, pp. 198–200.

of the professional as well as in the relationship established with the client. Italy seems to confirm this interpretation through its recent legislation implementing the AI Act (Law No. 132/2025). In particular, article 13—which applies to intellectual professions—indicates that the use of AI systems in professional practice is not an independent activity but a supporting tool that must remain subordinate to human intellectual work (art. 13(1)). Article 13(2) further requires that professional users inform the client, in clear and exhaustive terms, about the use of AI, thereby strengthening their fiduciary relationship with clients and their duty of transparency. As the first national implementation of the AI Act in the EU, this provision appears to support the view that LT used by lawyers should be treated as an integral part of the professional service, rather than as a standalone product, and that liability should therefore be assessed within the framework of professional duties and contractual responsibility.

With regard to lawyers' accountability regime, it is important to note that generally, in EU member State, establishing lawyer's liability requires the claimant to demonstrate the existence of a legal services agreement and that the damage suffered has been caused by lawyer's fault or negligence (including the violation of lawyers' professional duties).[39] Despite the conservative application of these liability regime—grounded in the idea that lawyers' obligations are "obligations of means rather than results"[40]—, it remains sufficiently robust to afford meaningful protection to clients. Indeed, this regime allows a client harmed—directly or indirectly—by the improper use of LT, or by the LT itself, when employed by a lawyer, to obtain compensation more easily than by holding the tech company responsible—this is due, among many, to the evidentiary challenges arising from the complex nature of AI-based tools, to the considerable economic power typically held by tech firms, and to the difficulties in identifying the responsible party. Nonetheless, the paper argues that, where courts acknowledge clients' difficulties in meeting the standard burden of proof, they may consider interpretative approaches that relax evidentiary requirements or reallocate burdens of proof in light of LT' distinctive features, such as opacity, automation, and third-party involvement. However, such developments remain largely theoretical at this stage, and judicial practice in this regard is still evolving. Overall, the existing liability framework seems adequately prepared to accommodate the integration of AI into legal services without necessitating immediate structural reforms, as it clearly affirms that lawyers provide a professional service for which they remain responsible, regardless of the tools employed.

As anticipated, another argument supporting the thesis at stake is the analogy that can be drawn with the responsibility lawyers bear for harm caused by trainees or other professionals acting under their supervision. In most of EU legal systems, lawyers bear a non-delegable ethical and professional responsibility to supervise all individuals (including non-legal experts) involved in the provision of legal services (e.g. art. 2322 Codice Civile, art. 7 ICFE). Through an analogical reasoning that remains faithful to the underlying rationale of the norm—which consists in the closely personal nature of the mandate—, it is reasonable to argue that the same principle should apply even more strongly to activities performed with the assistance of a self-learning, autonomous machine.[41] Lawyers' duty of supervision—and the corresponding responsibility in the event of harm caused by human or, through the mentioned interpretation, non-human collaborators—supports the idea

[39] T. Vilchyk, *Duties of Lawyer to a Court and to a Client*, Russ. L.J., 2018, pp. 88–97.

[40] C. P. Economides, *Content of the Obligation: Obligations of Means and Obligations of Results*, in J. Crawford et al. (eds), *The Law of International Responsibility*, Oxford University Press, Oxford, 2010, pp. 371–382.

[41] A. Bertolini, *Artificial Intelligence and Civil Liability*, European Parliament, 2020, p. 73, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf (last visited Jan. 23, 2026).

of identifying LT as a part of the professional service personally delivered by lawyers employing the means that they consider most appropriate.

Transposing the analysis to the EU level, only limited relevance may be attributed to the Services Directive 2006/123/EC (SD). While primarily aimed at facilitating the free movement of services, it nonetheless contains some ancillary safeguards for service recipients that also apply to legal services (recitals 33, 36; arts. 2, 4). Specifically, the SD provides for non-discriminatory access to services across member States (arts. 19–20), basic transparency and information obligations for recipients (arts. 21–22), and general duties facilitating complaint handling and dispute resolution (art. 27). Although their practical impact depends on national implementation, these provisions may offer a residual baseline of protection for clients when LT are employed within legal services.

Regarding the possible applicability of Digital Content Directive (DCD) 2019/770 EU,—if LT are considered as part of the service offered by lawyers—it seems to be not applicable, not only because it is not enforceable when the principal subject matter of a contract is the provision of professional services—such as legal one—regardless of whether digital means are (recitals 12, 27), but even because LT are not services that serves to create, store, process, check data in digital form or share data uploaded, stored or interact with other users (arts. 2(1) point 2; 3(5) a)).[42] Therefore, in assessing the applicability of the DCD, it is necessary to distinguish between the provision of automated legal services and the supply of legal digital content. Specifically, when LT are employed by legal professionals in the course of their work, they generally fall outside the DCD's scope. However, this exclusion may not apply to situations in which LT are used directly by end-users. This issue will be explored in greater depth in the following section, where the analysis focuses on LT as products, based on the premise that digital content may be encompassed within the broader category of products.

The absence of robust theoretical foundations and normative references supporting the qualification of LT as standalone products—an exception can be find it the General Product Safety Regulation (GPSR) 2023/988/EU, which extends its scope to any item that is supplied or made available, including in the context of service provision (recital 17), and it will be examined in greater detail in the following section—suggests that, when employed by lawyers in the delivery of legal services, LT should be regarded as an integral component of the overall professional service, rather than as independent products. This conclusion holds regardless of the lawyer's personal involvement, as legal practice remains immaterial, intellectual, personalized, and grounded in a fiduciary relationship—a characterization further supported by a consumer-centric approach aimed at protecting vulnerable clients, particularly in the absence of specific regulation. By contrast, if LT were classified as products even when used by lawyers, consumer protection rules would apply: the lawyer would act as seller, the LT output as product, and the client as buyer. Yet such a classification is conceptually problematic, conflicting with intrinsic nature of legal services. Even if it could theoretically enhance consumer protections, it risks oversimplifying the relational and fiduciary dimensions that distinguish legal services from standard commercial transactions.

While the categorization of LT when used by lawyers presents relatively few difficulties or uncertainties, significantly greater challenges arise when LT is used directly by consumers—an issue that will be addressed in the following section.

[42] S. Navas, *The Provision of Legal Services to Consumers Using LawTech Tools: From 'Service' to 'Legal Product'*, Open J. Soc. Sci., 2019, pp. 85–86.

## V. LT WHEN USED BY CONSUMERS: AI-DRIVEN PRODUCTS NOT SERVICE-BASED SOLUTIONS

As noted in the previous paragraph, the classification of LT as services appears relatively uncontroversial when such tools are employed in the provision of professional legal services delivered to clients. Conversely, the classification becomes more complex when LT are employed autonomously by end-users, necessitating a detailed legal analysis to ascertain their appropriate categorization and the corresponding legal framework. Therefore, this section will first examine whether LT may be considered as services, with particular attention to the relevant legal framework and its adequacy in ensuring the protection of consumers' rights. Then, the analysis will turn to the alternative classification of LT as products, assessing the legal implications arising from such a qualification; as will be demonstrated, this pathway proves to be the most practicable one and better suited to safeguard the interests of the involved parties.

As previously noted, legal assistance is increasingly being provided through LT that, to varying degrees, replicate functions traditionally performed by lawyers. These tools convey specialized knowledge tailored to users' needs, thereby supporting the performance of technically complex legal tasks.[43] The resemblance to legal services delivered by professionals may suggest that, even in the absence of lawyers' intervention, LT could still be classified as services when used directly by end-users. The absence of appropriate normative foundations to support such an interpretative stance not only weakens its legal plausibility but also raises significant concerns regarding consumer protection.

In this regard, it is important to highlight that, even considering LT as a form of legal services, it is evident that, in the absence of licensed lawyers, the professional duties governing lawyers do not currently apply to LT services offered by tech companies. It would be worthwhile to consider extending such professional obligations to LT providers. National bar associations and courts, for example, could play a pivotal role in advocating for the application of professional obligations to technology companies that offer legal services or products, thereby ensuring accountability and ethical standards in the delivery of such services. This would help promote greater accountability, strengthen consumer protection, and uphold ethical standards in the digital delivery of legal services. However, this approach is likely to encounter substantial resistance—not only due to the legal and interpretive difficulties courts face in extending sector-specific professional rules to actors beyond the established scope, but also because of the strong opposition that LT companies themselves are likely to mount.[44]

Considering EU level, the only regulatory provision that could apply is the E-Commerce Directive 2000/31/EC (ECD). It defines information society services as any service normally provided for remuneration at a distance, by electronic means, and at the individual request of a recipient of services (recital 17). These services encompass a wide range of online economic activities (recital 18), excluding legal representation before courts from its scope (art. 1(5) d)), but not legal advice or legal assistance—activities that may be performed by LT. The ECD primarily focuses on service providers and the proper functioning of the internal market, but it contains certain provisions that relate to service recipients. In particular, it requires member State to ensure that providers supply clear, comprehensible, and unambiguous information—before ordering—on matters such as the steps involved in contract formation, the languages of the contract, and whether the contract will be accessible. However, these requirements do not apply where contracts are concluded exclusively through e-mail or equivalent individual communications (art. 10).

---

[43] M. Ebers, 2021, p. 205.

[44] G. Chieco, *Digital Vulnerability and AI-powered Legal Services*, in M. Infantino et al. (eds), *Remedies to Digital Vulnerability in European Private Law*, forthcoming, Springer.

Member States must ensure that, when orders are placed electronically, providers acknowledge receipt promptly and both order and acknowledgment are deemed received once accessible to the parties (art. 11). Furthermore, the ECD requires member States to establish mechanisms for the out-of-court resolution of disputes (art. 17), as well as the possibility of seeking interim relief in the context of judicial proceedings (art. 18).[45] As is evident, the ECD does not offer strong or specific protections for consumers of LT, relying predominantly on information obligations, procedural mechanisms, and on national implementation, leading to a fragmented regulatory landscape that fails to guarantee consistent minimum standards of consumer protection across the EU.

The conceptual limits and the scarce legal references supporting the interpretation of LT as services, when used directly by consumers, suggest that it may be more appropriate to classify LT as products. In this regard, the diffusion of LT has enabled the delivery of practical legal knowledge via processes analogous to mass production, yet tailored to the specific needs of individual consumers—a phenomenon referred to as *mass customization*.[46] This approach is exemplified by computer-based document assembly systems, which, following a series of user-generated inputs (questions and answers), modify legal templates by removing or inserting clauses, ultimately generating documents customized to the user's personal circumstances.[47] As a result, practical legal knowledge is increasingly becoming a *commodity*, allowing tasks to be standardized and performed by laypersons, provided they have access to the appropriate technological tools.[48] Such commodified legal outputs are best conceptualized as *information goods* or *consumer products*, which possess distinct characteristics: first, they are non-rivalrous, meaning their use by one person does not deplete their availability to others; second, they are often non-excludable, as others may access and use them once they are made available; and third, the iterative use and reuse of such knowledge contributes to the generation of further knowledge.[49] As noted above, these features sharply contrast with traditional legal services, where the value lies in how and by whom the service is delivered. When human discretion and personalization are absent, and the task is performed by a machine, the output ceases to be a service and instead constitutes a product. The key classificatory criterion is therefore the nature of what is delivered and not by whom. Accordingly, these standardized and scalable legal outputs are best understood as goods—specifically digital goods—created at the time of the transaction and delivered via automated, algorithmic processes.[50]

Considering LT as products not only aligns with the just-mentioned conceptual framework but also permits wider and stronger protection of consumers than classifying them as services.

In this regard, it is worth mentioning the GPSR. It applies to any item—whether or not interconnected with other items—that is supplied or made available, including in the context of a service provision (recital 17), to consumers or is likely, under reasonably foreseeable conditions, to be used by consumers, even if not specifically intended for them, provided that no sector-specific legislation applies (arts. 2, 3). The GPSR imposes general safety requirements (art. 5), requiring operators to ensure products pose no risk under normal or foreseeable use. Safety assessments must consider design, presentation,

[45] J. Radler, *The Electronic Commerce Directive*, J. Direct, Data & Digital Mark. Pract., 2000, pp. 171–177.
[46] J. Tiihonen, *An Introduction to Personalization and Mass Customization*, J. Intell. Inf. Syst., 2017, pp. 1–7.
[47] R. Whalen, *Defining Legal Technology and Its Implications*, Int'l J.L. & Inf. Technol., 2022, pp. 52–58.
[48] S. Navas, 2019, pp. 82–83.
[49] J. S. Webb et al.,, *Setting Standards: The Future of Legal Services Education and Training Regulation in England and Wales*, 2013, p. 4, available at https://letr.org.uk/wp-content/uploads/LETR-Report.pdf (last visited Jan. 25, 2026).
[50] S. Navas, 2019, pp. 82–84.

labelling, user characteristics—including vulnerable consumers—and evolving functionalities like cybersecurity or adaptive features (art. 6). Critically, recital and provisions emphasize the inclusion of non-tangible or mixed products such as software and apps (recitals 25, 26). Therefore, when LT are classified as products rather than services, they fall within the scope of these safety obligations: LT manufacturers must undergo internal risk assessments, maintain technical documentation, and carry traceability information. Accordingly, a manufacturer who considers, or has reason to believe, that a product placed on the market is dangerous must immediately take appropriate corrective measures to ensure its compliance—including, where necessary, withdrawal or recall—while also informing consumers in accordance with articles 35 and 36, and notifying the relevant market surveillance authorities via the Safety Business Gateway (art. 9).[51] Furthermore, products offered online or via distance selling must clearly display essential information, such as operator identity and product details (art. 19). The application of GPSR to LT offers consumer protections via mandatory safety and transparency requirements, partially bridging the gap when LT function autonomously outside professional oversight. It also shifts regulatory responsibility onto LT producers and distributors, aligning them more closely with product liability regimes rather than pure service-based frameworks, as noted in recital 17. However, the product-based approach set by GPSR is residual in nature (art. 2) and therefore applies only in the absence of specific sectoral legislation. In this regard, it seems appropriate to address the issue of producer liability as defined by the Product Liability Directive (PLD) and the Revised Product Liability Directive (RPLD).

As widely known, the PLD does not appear to apply to damages caused by AI tools, unless they are integrated into products–understood as tangible movable goods (art. 2). As a result, the PLD does not seem to offer protection in cases of harm caused by LT. To address this gap in protection and to modernize a directive conceived in the pre-digital era, the RPLD was adopted. The RPLD, compared to its predecessor, sets a wider definition of 'product', covering software and AI systems (art. 4). This confirms the RPLD's applicability to LT, insofar as AI-based legal tools marketed to the public and used autonomously by consumers qualify as digital products in their own right and therefore fall within the RPLD regime. The RPLD also enlarges the scope of the parties in the supply chain who may potentially be liable (art. 8), reflecting the complex ecosystem of AI development and distribution. Furthermore, it expands the definition of damage by including material losses resulting from inadequate cybersecurity measures and destruction or corruption of data that are not used for professional purposes in case of product defectiveness (art. 7). This extension is particularly relevant for LT, which often process sensitive legal data and operate in environments where cybersecurity vulnerabilities or data integrity failures may cause significant harm. In this respect, the RPLD reinforces the centrality of cybersecurity and data integrity, recognising that insufficient protection, missing updates, or inadequate system design may themselves constitute a source of compensable damage, leading to both financial and non-financial losses deriving from the destruction or corruption of private data or systems, pursuant to article 6(1)–(2). The burden of proof remains with the plaintiffs, who must prove the product was defective, that they suffered damage and the causal link between the damage and the defect (art. 10); yet, under certain conditions, the RLPD establishes a presumption of defectiveness and causal link and the plaintiffs' right to ask manufacturers to disclose necessary information in court (art. 9). It should however be kept in mind that article 13 limits liability where the

[51] J. Ruohnen, *A Review of Product Safety Regulations in the European Union*, Int'l Cybersecurity L. Rev., 2022, pp. 352–358.

injured person has contributed to the damage through negligent behaviors. Nevertheless, recital 55 clarifies that the liability of the economic operator should not be reduced or disallowed when the damage is caused, in addition to the defectiveness of the product, by the acts or omissions of users or third parties. In other words, the producer cannot rely on article 13 where the damage results not only from the consumer's misconduct but also from a defect or vulnerability that could have been prevented through appropriate design, security measures, or user guidance. Therefore, while article 13 may operate as a defence in theory, its practical applicability in the LT context is limited when the producer has not fulfilled its duties of safety, updating and information provision. Importantly, the practical relevance of disclaimers is also limited in the LT context. This is because the harms contemplated by the RPLD—such as damages resulting from data destruction, corruption, or cybersecurity failures—are typically beyond the consumer's capacity to cause through ordinary use. A generic disclaimer is thus unlikely to shift liability away from the producer when the product's defectiveness causes such damages in the course of its intended use, especially if security standards are not met. In light of the foregoing, the most significant limitation, of the RPLD lies in the narrow scope of compensable damage, which is confined to specific cases. However, the RPLD provides an additional layer of consumer protection for autonomously deployed LT, offering a targeted and concrete avenue for redress in clearly defined scenarios, effectively complementing other EU consumer-protection measures.

Considering now the DCD, it is important to note that it leaves room for different interpretations due to the generic definition of "digital content", which consists in data that are produced and supplied in digital forms (art. 2), that includes for example, computer programs, applications, video files, audio files, or other e-publications (recital 19).[52] Furthermore, the DCD does not define the legal nature of contracts for the supply of digital content and digital services, leaving this matter to national legislation (recital 12). As a result, fundamental aspects of such contracts are governed by national laws, with the aim of ensuring a high level of consumer protection, regardless of the contractual form or the legal definitions adopted.[53] Therefore, through a straightforward interpretative approach, the—open and wide—category of digital content could be subsumed under the broader category of products. Indeed, this line of reasoning is supported by the analogy between digital products and digital content. The purchase of digital content entails the electronic transfer of digital data to the consumer and requires a medium through which the content can be accessed and used. Similarly, digital products are goods that can be reduced to digital data and are acquired through electronic transmission. Their use presupposes compatible hardware or software on which the data can be stored and through which the contractual purpose can be fulfilled. Although intangible in nature, the digital data effectively becomes part of a tangible product once it is transmitted to and stored on the consumer's hardware.[54] Consequently, LT, when deployed by end-users and fitting within the definition of digital contents, could also fall within this classification and be regulated accordingly under DCD. This approach also aligns well with the consumer-centric perspective adopted both in this paper and in the EU legal framework governing the digital realm. DCD requires that digital content conform to the terms of the contract

[52] M. Farinha, *Modifications on the Digital Content or Digital Service by the Trader in the Directive (EU) 2019/770*, RED, 2021, pp. 89–90.

[53] S. Navas, 2019, p. 9.

[54] M. Schmidt-Kessel, *The Application of the Consumer Rights Directive to Digital Content*, European Parliament, 2010, p. 3, available at https://www.europarl.europa.eu/document/activities/cont/201101/20110113ATT11670/20110113ATT11670EN.pdf (last visited Jan. 25, 2026).

with regard to description, quantity, and quality, and that it possesses features such as functionality, compatibility, interoperability, and security (arts. 6, 7). Furthermore, the content must be fit for the agreed purpose and meet the quality and performance standards that consumers can reasonably expect, including continuity and accessibility (art. 8). Traders are obliged to provide all necessary updates to ensure ongoing conformity (art. 9). Failure to supply the content or a lack of conformity at the time of supply renders the trader liable (art. 11), and the burden of proof is reversed in favor of the consumer (art. 12). Where the trader fails to supply the digital content or service within the agreed timeframe, or with undue delay after a consumer's reminder, the consumer is entitled to terminate the contract (art. 13). In the case of non-conformity, the consumer may demand that the product be brought into conformity unless this is impossible or would impose disproportionate costs. If the trader fails to provide a remedy, the consumer has the right to a proportionate price reduction or to terminate the contract altogether (art. 14). Upon termination, the trader must fully reimburse the consumer, except for any period during which the content or service was compliant with the contract (art. 16).[55]

From both a logical and normative standpoint—even acknowledging that the applicable legal provisions are currently limited and insufficient—it becomes evident that LT, when used directly by end-users, should be classified as products rather than services. Failing to do so would mean disregarding fundamental principles that underpin the distinction between products and services. More critically, it would leave consumers largely unprotected, exposing them to the unchecked power and potential impunity of legal tech companies. In such a scenario, the imbalance between end-users and technology providers would be further exacerbated, undermining core objectives of consumer protection law and market fairness.

## VI. Conclusions

The widespread use of AI in the European legal sector undeniably brings significant opportunities and benefits—such as enhanced productivity for law firms, improved access to justice, and broader dissemination of legal knowledge. However, it simultaneously introduces novel vulnerabilities and exacerbates pre-existing ones. The opaque technological architecture of LT, the limited resources as well as the legal and technical literacy of users, and insufficient safeguards in their development and deployment all contribute to exposing users to potential risks.

The benefits may be constrained, and the risks amplified, by the legal uncertainty surrounding the classification of LT as either products or services—an ambiguity that directly impacts the applicable legal framework, with direct consequences for consumer protections and legal certainty for providers.

In the absence of clear definitions or precise normative references, the most viable path forward is to adopt an interpretative approach that best aligns with both the conceptual distinctions between services and products and the objective of maximizing consumer protection under EU law. This paper has aimed to demonstrate that LT, when deployed by lawyers as part of their professional activities, should be regarded as services. This position is supported not only by the intrinsic nature of legal practice but also by the existence of professional duties that bind lawyers. If these duties are breached, including through negligent use of LT, clients are entitled to seek compensation—an avenue that is often more practical and accessible than pursuing claims directly against LT providers.

[55] J. Morais Carvalho, *Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directive 2019/770 and 2019/771*, J. Eur. Consum. & Mark. L., 2019, pp. 194–201.

Moreover, should courts find that clients face significant challenges in proving the necessary elements to obtain compensation for damages caused by LT, they should consider interpretative solutions to alleviate the evidentiary burden, such as presumptions or reversal of the burden of proof.

Conversely, when legal technologies are used directly by end-users—without the intermediation of legal professionals—they should be classified as products. This classification better reflects the nature of LT, which are typically offered on the open market as standardized, commodified solutions, rather than as tailored professional services. Recognizing these technologies as products not only aligns with their functional and commercial characteristics but also provides stronger and more appropriate safeguards for consumers. Under the EU consumer law framework, this classification enables access to a range of protections, including compliance with general safety requirements, the obligation of conformity with the terms of the contract, and recourse to producer liability in the event of damage. These mechanisms are particularly important in scenarios where the user lacks the expertise to assess the reliability or limitations of the technology, thus reinforcing the principle of effective consumer protection.

Ultimately, in the absence of a comprehensive regulatory framework, the interpretative strategy that best reconciles the dual goals of legal coherence and consumer protection is to classify LT as services when used by legal professionals in the course of representing clients, and as products when used directly by consumers. This dual approach is both doctrinally sound and practically necessary to uphold the rights of consumers and to foster trust in the use of legal technologies across the European legal landscape.

# ESCAPING THE EU REGULATORY LASAGNA: HOW THE AI LIABILITY LEGISLATION MUST MOLT TO SURVIVE

*Beatrice Marone*

TABLE OF CONTENTS:


*On February 11, 2025, the EU Commission declared that the Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (AILD) was to be withdrawn, due to the fact that no agreement was foreseeable. Drawing lines from both the key features of the directive proposal and the inputs deriving from the EU efforts on the topic of AI regulation, this paper aims at providing a recollection of the core themes, along with the suggestions to go beyond the original scope in order to expand the applicability to non-AI software. Moreover, it will address the proposed change of skin from directive to regulation including an examination of the recent trends in the EU legislation about the so-called "directivization" of regulations.*

**Keywords:** Artificial Intelligence – Liability – AILD – harmonization – directivization – regulation.

## I. THE TURNING POINT

### I.1 *The Commission's 2025 Work Programme and the reactions*

The most unexpected news coming from the EU Commission's 2025 Work Programme[1], published on February 11, 2025, was not in the thirteen pages of the text, but in its Annex IV[2]. Among the proposals for acts that the Commission intended to withdraw within six months from the publication of the Programme, precisely at page 26, row 32, of the table, it stood the Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability). The legislative text, commonly addressed with the acronym "AILD", should have constituted one of the pillars of the EU regulatory framework for AI. The reasons explicitly stated as backbone of the Commission's choice were that no agreement was foreseeable and, thus, the Commission had to assess whether another proposal should be tabled, or another type of approach should be chosen.

---

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Commission Work Programme 2025 "*Moving forward together: A Bolder, Simpler, Faster Union*", February 11, 2025, available at https://commission.europa.eu/document/download/f80922dd-932d-4c4a-a18c-d800837fbb23_en?filename=COM_2025_45_1_EN.pdf (last visited Aug. 12, 2025).

[2] Annex IV: Withdrawals, February 11, 2025, available at https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c-249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf (last visited Aug. 12, 2025).

Despite hidden in the depth of a Communication whose effects can be properly addressed only throughout a suitable amount of time, the Commission's radical decision was not taken lightly by the EU lawmakers. A vast gap has formed between two different currents of thought around the Commission's latest steps. In particular, soon after the publication of the Work Programme, the Internal Market and Consumer Protection Committee (IMCO) voted to maintain its agenda around liability rules for products including or making use of AI[3]. Subsequently, members of both the civil society and consumer groups penned a letter to the Commission, closing it with a powerful call to action: "If the Commission wants to improve EU consumers and citizens' trust in AI, its priority should be on new EU AI liability rules. A consistent and ambitious AI liability framework would also contribute to the social acceptance of this technology, which would have a positive spillover effect on the uptake of this technology and, in turn, on innovation and growth"[4].
At first glance, such position can seem rather simplistic, but the sentences actually echo the key points of the AI strategy envisioned at the EU level. Such strategy dates back even before the Proposal of the Commission dated April 2021 that ended up becoming Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. It goes back, first, to the Commission's Communication entitled "AI for Europe"[5] of April 2018 and, then, to the principles established by the High-Level Expert Group on AI in the "Ethics Guidelines for Trustworthy AI"[6] that followed one year later. The absolute need for AI to be trustworthy has been the recurring theme of the EU effort on the topic, as enshrined in the White Paper of February 2020, coherently entitled "A European Approach to Excellence and Trust"[7].
In order to understand the current dialogue on the contemporary state and perspectives of survival of the AILD, an exchange of ideas that, in some instances, devolves even into harsh confrontation, it has to be considered its place in the landscape of the EU past and recent struggle to reach and maintain a prominent role in the guidance for AI regulation. While the direction followed by the EU institutions has been rather consistent throughout the last decade, it has to be remembered that the Union is not an isolated entity. Its proposals, its policies and its solutions have to coexist with the approaches chosen by other national and international entities.

---

[3] C. Kroet, *Lawmakers reject Commission decision to scrap planned AI liability rules*, available at https://www.euronews.com/next/2025/02/18/lawmakers-reject-commission-decision-to-scrap-planned-ai-liability-rules (last visited Aug. 12, 2025).
[4] Open Letter to the European Commission on the announced withdrawal of the AI liability Directive, available at https://cdt.org/wp-content/uploads/2025/04/AILD-withdrawal-Joint-Open-Letter-.pdf (last visited Aug. 12, 2025).
[5] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "*Artificial Intelligence for Europe*", April 25, 2018, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237 (last visited Aug. 12, 2025).
[6] Ethics Guidelines for Trustworthy AI, April 8, 2019, available at https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (last visited Aug. 12, 2025).
[7] White Paper On Artificial Intelligence - A European approach to excellence and trust, February 19, 2020, available at https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf (last visited Aug. 12, 2025).

It has been highlighted by specialized observers that the EU Parliament's Committee on Legal Affairs (JURI) voted in December 2025 against the recommendation of suing the Commission over the decision to withdraw the AILD, despite concerns being raised over the timing of the decision, after encounters at the Paris AI Action Summit with US executives[8]. Everyone can notice how the US perspective on regulation had entered a rather dramatic inversion of trend after the latest presidential election. Such circumstance is even more evident simply reading the title of the executive order signed by President Biden in October 2023, i.e. "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"[9], and of the executive order of President Trump dated January 2025, i.e. "Removing Barriers to American Leadership in Artificial Intelligence"[10]. The second, in substance, erased the previous one. Taken into consideration the above, it is not naïve to state that, before, the EU strategy, along with the so-called Brussels effect, could count on a powerful link not only to the other side of the ocean, but also to a State at the head of technological development. It is now, instead, realistic to accept that that era ended, maybe even before the coming back to the White House of the forty-seventh President. The common views of the Trump administration and of the CEOs of the tech giants have certainly expedited the process, giving rise to the so-called Washington effect for de-regulation. Nevertheless, the issue was already systemic and, even more dangerously, already embedded inside the same EU strategy on AI.

### I.2 *The "regulatory lasagna" and its dangers*

The AILD path and its destiny are strictly linked to the need to urgently address the issue efficiently summarized by the same commentators with an easily understandable metaphor: the "regulatory lasagna". It was coined around the end of 2022 to address the challenges arisen in the medical sector from an increasing use of technology and, after the exponential growth registered in the AI subfield in 2023, has widened its reach (more among experts than within the general public) to encompass all the industries touched by the provisions included in the EU normative acts. Despite seeming trivial, the metaphor has the power to include in an image simple to grasp the feature of the EU approach on AI that has been subject to the harshest critiques: the inability to provide a coherent normative framework for a specific domain, due to the fact that it is regulated through an overlapping of different bodies of law, many times incapable of efficiently connect to each

[8] M. Henning, *Parliament won't take Commission to court for ditching AI liability law*, available at https://www.euractiv.com/news/parliament-wont-take-commission-to-court-for-ditching-ai-liability-law/ (last visited January 24, 2026).

[9] Executive order 14110 of October 30, 2023, available at https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence (last visited Aug. 12, 2025).

[10] Removing barriers to American Leadership in Artificial Intelligence, available at https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/ (last visited Aug. 12, 2025).

other. The result is a fragmented legislation, with many different layers leading to inconclusive outcomes and inefficient results.

The latest piece of legislation to fall victim of the issue it has been, unsurprisingly, the AI Act. While it should have become the master for a new age for the EU regulation, it has been, in reality, dispossessed piece by piece of its strongest features. This is due, on one side, to the need to approve it as a Regulation, hence as a legislative text immediately enforceable in all the twenty-seven Member States. On the other side, the willingness to provide an all-encompassing discipline led to an enormous text, with provisions that are seemingly heavy per se and also in contrast with each other.

This consequence represents only the latest and extreme extension of a trend already present in the General Data Protection Regulation[11]. Despite being data privacy, data security and data safeness  relevant aspects to be incorporated into the AI strategy, the structure of the GDPR has proved not to be transferable to the AI domain without being subject to a proper rethinking. The key element manifesting why the same point of view is not suitable for data protection, on one side, and AI, on the other side, comes into the picture already at article 3 of the GDPR, when the territorial scope of the Regulation is described establishing three clear-cut criteria in the different paragraphs: establishment of controller or processor, targeting of the data subject and application by virtue of public international law[12]. It is way more difficult to specifically pinpoint the territorial scope of the AI Act, as evidenced by the fact that, first, no provision mirrors the article of the GDPR just mentioned and, secondly, article 2, entitled simply "Scope" includes in the only paragraph 1 seven different scenarios that actually may overlap with each other. This is because the AI features may experience different levels of embedding in the products used by the natural persons.

Besides, it has to be recalled that even the same definition of "AI system"[13] has been at the center of long discussions and brought a strong clash that even threatened to impede the conclusion of the works relating to the AI Act before the fast-approaching deadline laid out for its adoption. First, because such definition represents a wording born in the legal landscape to enshrine a technical concept; secondly, due to the fact that such technical concept has not remained the same, but it has, instead, undergone deep transformation even just considering the years between the proposal (2021) and the approval (2024) of the AI Act, with the most striking consequences due to the

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (last visited Aug. 12, 2025).

[12] European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, available at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf (last visited Jan. 24, 2026).

[13] Now included under article 3, letter a) of the AI Act as "*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*".

proliferation, in 2023, of large language models and of the so-called general purpose AI systems.

Thus, the EU tendency to overregulate might have been the tombstone of the past era, but the institutions seem to have become rather aware of the critics' words. This emerges from the title of the Commission Work Programme: "Moving forward together: A Bolder, Simpler, Faster Union". If this is the order of ideas, the words spoken by who defended and made official[14] the Commission's decision to scrap the AILD might be less drastic than they seem. Before diving into the foreseeable consequences deriving from a bold move, which may equally end up being the closure of the effort of an overall EU regulation on AI or the first brick of a luminous renaissance, an analysis of the features of the AILD and of the critiques raised against the same is in order. The reason for this choice is not connected to a simple theoretical analysis of the provisions, but rather to an examination of the wording of the text as a mean to convey the intentions of the authors. While the performance of literal interpretation of the legal texts has left space throughout the decades, shifting especially to courts the burden of filling the voids left by the legislators, only comparing the different versions of the proposals laid down on the path to a normative body it is possible to notice the changes in both the content itself and in the direction of action. Moreover, it is essential to test whether the provisions actually undergo significant amendments or simply shapeshift on the surface without deep changes.

## II. AILD: FROM A STRONG IDEA TO A MESSY REALITY

### II.1 *The 2022 Proposal and the landscape leading to it*

The Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)[15] was advanced on September 28, 2022. The reason calling for the enactment of a new piece of legislation has to be located exactly within the market.

The Commission made abundantly clear already in the first line of the Explanatory Memorandum that the need for new rules with respect to liability, which is one of the most longstanding and, yet, most discussed, fields of law, originated directly from the stakeholders. It mentions, in fact, the results of a survey conducted two years prior among the companies willing to engage in their business in the EU[16]: liability was listed in the top three places regarding the barriers that such companies encountered in their path adjusting

[14] S. Brachmann, *EU Commission Confirms that SEP Regulation, AI Liability Directive are Officially Scrapped*, August 6, 2025, available at https://ipwatchdog.com/2025/08/03/eu-commission-confirms-sep-regulation-ai-liability-directive-officially-scrapped/id=190857/ (last visited Aug. 12, 2025).

[15] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0496 (last visited Aug. 13, 2025).

[16] European Commission: Directorate-General for Communications Networks, Content and Technology, iCite and IPSOS, *European enterprise survey on the use of technologies based on artificial intelligence – Final report*, Publications Office, 2020, available at https://data.europa.eu/doi/10.2759/759368 (last visited Aug. 13, 2025).

to the use of AI. According to 43% of the responders, it was even the most relevant external obstacle for companies that were planning to adopt AI, but had not done it yet. The legal framework on liability has been and still is mostly subject to the national rules of each single legal system of the twenty-seven Member States. The fact that a heavy burden of proof is placed on the plaintiff regarding the consequentiality between, on one side, the act or omission and, on the other side, the damage occurred, leads to a potential deterrence in even just initiating the legal proceedings. According to the Commission's perspective, the specific and unique features of AI led and lead to the rise of new and unforeseeable up-front costs, along with a relevant augmentation of the time needed to reach a decision.

The situation painted by the Commission was rather dark. Nevertheless, it had not even specifically addressed the issues that each single State was, and still are, facing dealing with the most traditional proceedings. Moreover, the features of AI interfering with the longstanding approach on liability, identified especially in complexity, autonomy and opacity, are even more serious in the current moment. The Commission was almost optimistic when it claimed that the situation would lead to legal uncertainty only in the future, while the legal practitioners, the scholars and even the private citizens are painfully aware that the legal uncertainty is a situation we were living in in 2022 and are sadly still experiencing today.

In October 2020, the EU Parliament issued a resolution on a civil liability regime for artificial intelligence[17] with a plan that was defined as both ambitious and radical. It proposed a high degree of harmonization at EU level for an AI-specific liability regime, thanks to the adoption of regulation based on two layers: on one side, strict liability for high-risk AI systems and, on the other side, fault-based liability for systems other than the high-risk ones[18]. Instead, the solution prospected by the Commission was centered around a multi-faceted approach, starting with the ex-ante assessment that lately found its core in the AI Act and ending with the ex-post evaluation of the damages not possible to prevent at an earlier stage. Following this road, the Commission felt the need, on the one side, to update the 2001 General Product Safety Directive[19] and, on the other side, to address the topic of liability though different actions. Such actions were supposed to be performed both on the existing directive on product liability (the so-called "PLD")[20] and through a

[17] Civil liability regime for artificial intelligence European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020IP0276 (last visited Aug. 13, 2025).

[18] T. Rodríguez de las Heras Ballell, *The revision of the product liability directive: a key piece in the artificial intelligence liability puzzle*, in *ERA Forum*, 249 (2023), available at https://doi.org/10.1007/s12027-023-00751-y (last visited Aug. 13, 2025).

[19] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0095 (last visited Aug. 13, 2025).

[20] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374 (last visited Aug. 13, 2025).

new legislative text able to address the specific features of AI and the equally specific risks deriving by the same.

The legal instrument chosen for updating the rules of general safety for products shifted from directive to a regulation and, thus, the first goal set out above was reached in December 2024, with the entry into force of the General Product Safety Regulation[21] of May 2023. Instead, the direction of action regarding liability and, especially, AI liability, was the opposite: the Commission conceived a directive rather than a regulation. First, the Commission took into consideration the preliminary results of a public consultation run from October 2021 to January 2022[22]. Secondly, it addressed the cited high degree of interaction between national regimes of tort law, which differ greatly, reaching the conclusion that the only way to formulate a regulation able to derogate all of them only for the hyper-narrow field of harm caused by AI could lead to an unacceptable level of friction and inconsistency across the EU[23].

### II.2 *The pillars of the Proposal*

The focus of the new piece of legislation was already very clear from article 1. It explicitly declares that the directive will lay down common rules dealing with two topics. On the one side, the disclosure of evidence on high-risk AI systems, in order to enable the claimant to substantiate a non-contractual fault-based civil law claim for damages. On the other side, the burden of proof, in case of non-contractual fault-based civil law claims brought before national courts for damages caused by an AI system. Moreover, it expressly excludes criminal liability, thus, clearly delimiting the borders of the theme to be addressed. Nevertheless, some elements in need of flexibility are already introduced through article 2, where all the definitions are linked to the ones provided in the AI Act. Such circumstance renders immediately clear that the AILD could not ever survive without the approval and entering into force of the AI Act itself and the close connection has confirmed from the beginning the fears that a long path for the AI Act also meant prolonging the timeframe needed for the introduction of the new instruments on AI liability. In fact, it comes with no surprise that all the works and discussions on the text of the AILD have been frozen until around July 2024. In the same way, it is not surprising at

[21] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R0988 (last visited Aug. 13, 2025).

[22] European Commission. *Civil liability – adapting liability rules to the digital age and artificial intelligence*, 2021, available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital%20age-and-artificial-intelligence_en (last visited Aug. 13, 2025).

[23] C. Wendehorst, *AI liability in Europe: anticipating the EU AI Liability Directive*, 4 (2022), available at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/09/Ada-Lovelace-Institute-Expert-Explainer-AI-liability-in-Europe.pdf (last visited Aug. 13, 2025).

all that the Commission was ready to reopen such chapter, or, rather, bury it, only in its Work Programme for the year 2025.

Article 3 and article 4 make even more evident that the whole impact envisioned for the AILD has roots strongly held in procedural law. In fact, it establishes two relevant presumptions, albeit rebuttable. First, the presumption of non-compliance when, after the plaintiff has presented facts and evidence sufficient to support the plausibility of the claim for damages, the defendant does not disclose the relevant evidence at its disposal about the specific high-risk AI system that is suspected of having caused such damage. Secondly, the presumption of a causal link in the case of fault when the three following conditions exist at the same time: i) either demonstration by the plaintiff or presumption by the court, on the basis of the previous article, that the fault of the defendant, or of a person for whose behavior the defendant is responsible, consists in the non-compliance with a duty of care directly intended to protect against the damage occurred; ii) reasonably likely consideration, based on the circumstances of the case, that the fault has influenced the output produced by the AI system (or the failure of the AI system to produce an output); iii) demonstration by the plaintiff that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage.

The requirements needed to verify the existence of the first condition are provided in a more detailed manner for the high-risk AI systems. Thus, such condition is deemed reached when the plaintiff has demonstrated that either the provider or the person subject to the provider's obligations failed to design and develop the AI system in compliance with the following requirements, laid down in the AI Act: i) quality criteria for training, validation and testing data sets; ii) transparency; iii) effective oversight by natural persons during the use of the system; iv) appropriate level of accuracy, robustness and cybersecurity; v) not immediate application of the necessary corrective actions to either bring the AI system in conformity with the obligations, to withdraw or to recall the system.

As stated by the commentators, both the initial aim and the expected effect of the AILD are modest, pragmatic and realistic from a lawmaking perspective[24].The Commission was clearly aware that, at the time of the issue of the proposal, the regimes available to the plaintiffs to claim compensation for damages, due to both overlapping and juxtaposition between the single national laws and the PLD, were, essentially, three: i) fault-based liability claim, requiring the proof of damage, fault and causality; ii) strict liability claim, independent from fault; and iii) claim against the producer of a defective product, requiring both the proof that the product was defective and the causal link between that defect and the damage[25]. Through the revised PLD directive[26] adopted in October 2024,

[24] T. Rodríguez de las Heras Ballell, *The revision of the product liability directive: a key piece in the artificial intelligence liability puzzle*, cit., 250.

[25] T. Madiega, *Briefing. EU Legislation in progress. Artificial Intelligence Liability Directive*, 2022, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf (last visited Aug. 13, 2025).

[26] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402853 (last visited Aug. 13, 2025).

the Commission achieved its scope to adapt the producers' strict liability regime for defective products to allow for compensation for damages without the need to prove a fault. Instead, the whole point of the AILD has always been another one: taking into account the impossibility to reform the substantial provisions belonging to fault-based liability regimes due to their nature of national legislation, the aim has been to harmonize specific procedural aspects of the regime applicable to claims for fault influencing the AI system that caused the damage, in order to alleviate the burden of proof weighty on the plaintiffs' shoulder, being them either natural or legal persons.

The proposed horizon of action refers to two gaps correctly identified in the current landscape of the EU legal framework on liability. The first one, just addressed in the previous paragraph, refers to the so-called liability gap: in the present moment, it is not simple to ascribe responsibility for the harms caused by the AI system and, in particular, to allocate such responsibility among the different persons concurring in the development and in the deployment of the same, i.e. designers, developers, deployers and users. The second one, instead, regards the so-called information gap: the persons damaged by the use of the AI system, or of a system incorporating AI features, may not be aware that such use exists and affects their own rights[27]. While it seems that the provisions of the AILD, as it is in its latest form, cooperate in the first of the two directions of action, it is more disputed whether the same are suitable to face the challenges posed by the second.

### II.3 *The rejection of the harmonization horizon*

Despite the best efforts of its authors and of the people working on the same, the most invasive wound in the AILD is laid down explicitly in the contrast among the texts included in the recitals. In recital number 26, the AILD confirms that a full harmonization of the requirements for AI systems and, especially, the specific requirements for high-risk AI systems, is a task reserved for the AI Act. In the same sense, recital number 12 refers to the fact that the Digital Services Act fully harmonizes the rules applicable to providers of intermediary services in the internal market, thus covering the societal risks stemming from the services offered by those providers, including the AI systems they use.

The provisions of the AILD are not designed to touch either of the regulations just cited. What the Commission itself designs as a holistic approach is further enhanced by the text keen in making the borders of the effort towards harmonization crystal clear and, not, instead, underlining what the directive is trying to harmonize. This is evident under recitals number 7 and number 9, specifically referring to the need to harmonize certain national non-contractual fault-based liability rules and to pinpoint in a targeted manner specific aspects of such fault-based liability rules. Recital 10 manifests the limits that the text imposes on itself: in order to ensure proportionality, it is appropriate to harmonize in the cited targeted way only those fault-based liability rules that govern the burden of proof for

[27] M. Ziosi, J. Mökander, C. Novelli, F. Casolari, M. Taddeo, L. Floridi, *The EU AI Liability Directive (AILD): Bridging Information Gaps*, in *European Journal for Law and Technology*, 3 (14, 2023).

persons claiming compensation for damage caused by AI systems. It is highlighted with different wordings and in various sentences that the AILD should not harmonize general aspects of civil liability. These aspects are exemplified in the definition of fault or causality, the different types of damage that give rise to claims for compensation, the distribution of liability over multiple tortfeasors, the contributory conduct, the calculation of damages, the limitation periods. Each of them is regulated in a different way by national civil liability rules. Not only this should not change, but it also cannot change, according to the perspective adopted at the time by the Commission.

Tort Law and Contract Law are the domains that, notwithstanding the general trends in integration of legal systems and globalization as a whole, still resist within the limits of the States. The systems of extra-contractual liability of the single EU Member States share a common background on the classical human interests in life, bodily integrity, health and property, listing them as the core of the protective scope of causes of action based on tort, but diversity is behind the corner, especially dividing the road after having dealt with the same fundamental principles. One area where the European systems of tort or delict diverge concerns the status of statutory norms regulating behaviors through prescriptions or prohibitions[28]. Choosing not to address the juridical concepts underlying the features of the single regime and not even trying to establish principles relating to the substantial topics is certainly an interesting approach, especially since it has not been explained in detail by the Commission which ones have been the core reasons in leading it to believe that such approach to the topic could actually work. It is fascinating to consider that a very specific part of the civil liability regime, i.e. the procedural rules regarding the disclosure of information and the exact proportion of the burden of proof on the parties, could function without the building blocks of the domain defined in a harmonized way.

### II.4 *The longstanding issue of definition*

As already briefly anticipated under paragraph 1, it is safe to say that the defining problem has proved, time and time again, to be the main obstacle in, at least, the latest decade of legislation efforts around technology at the national level as well as in the EU. This is due to the fact that, once again, the subjects operating in the legal field have not reached yet an adequate level of confidence towards the key concepts for the technological tools. Such feature is absolutely needed to draft consistent and coherent sets of rules in order to deal with the same. Notwithstanding the above, this is not even the major reason for the stalling situation that the lawmakers are dealing with right now. Indeed, liability comes way before technology. It comes from the ancient times, from the rules of eye for eye and of the vengeance. It comes from the system of dueling to reach a solution around compensation and from the ancient belief that it would be up to the gods to decide where liability laid and what was the exact amount of compensation to be granted to the victim. Even nowadays, different treatments, different lengths of proceedings and even different

[28] G. Wagner, *Liability Rules for the Digital Age*, in *Journal of European Tort Law*, 232 (13, 3, 2023).

outcomes are still expected by victims in the same use case, depending on the legal system they initiate their disputes. This is, with all due probability, the defining obstacle not only of this century, but probably of the whole history of law.

Nevertheless, the only way to achieve legal certainty is the adoption of common rules. It was rather difficult in the past, but it has become unconceivable in the present to still have to manage the different treatments provided for the same circumstances under different national laws. This is why the choice of law and the choice of jurisdiction are still one of the most discussed themes not only among scholars, but within the drafting phase of a contract. This is because both parties do not wish to be put into an uncomfortable position if and when any obligation may be left incomplete or not fully performed. The legal uncertainty in the present globalized word is not bearable, especially taken into consideration the wide transnational implications of technology.

At the beginning of the newest era of the shared journey between technology and law, the latest has been subject to the longstanding Collingridge dilemma, torn between the option of regulating fast and in an insufficient way with regard to the actual outreach of the norms and the option of regulating after building a strong awareness, confidence and coherence, but with the unavoidable consequence of being too late. For a certain timeframe, soft law instruments have been deemed as the first line of action to try to bridge the gap between the fast pace of the changing reality and the inherent slowness of the lawmakers. Instruments of soft law have risen already in the years prior to the adoption of the EU White Paper, between 2018 and 2019: education and institutional entities, but also expert groups set up in the committees of the UN agencies and groups collecting categories of professionals with the same background have proposed decalogues of principles that present many features in common. However, it does not seem that in the current situation of clash between legal orders that have become very polarized thinking only in a soft law perspective is a viable solution. Soft law might be a lifeline to lead the way, but proper enforceable regulation is needed.

### II.5 *A divided field*

Notwithstanding the above, the concerns of the same Commissioners defending the choice to scrap the AILD with the features described are, at least, shareable. Indeed, the same Commissioner for Tech Sovereignty, Security and Democracy Henna Virkkunen has not subtly hinted at the fact that what has been seen as a (negatively) groundbreaking decision may not be full of such dreadful consequences in the long-term period. Virkkunen declared that the main reason for the withdrawal of the AILD was that the legal instrument of the directive enables the Member States to implement the rules in different ways, while the new approach to the topic might be more towards more regulations, with the aim of reaching the goal of one single market[29].

[29] C. Kroet, *EU Tech Commissioner defends scrapping of AI Liability rules*, available at https://www.euronews.com/next/2025/04/09/eu-tech-commissioner-defends-scrapping-of-ai-liability-rules (last visited Aug. 14, 2025).

In its Draft Opinion[30] of January 2025, the Committee on the Internal Market and Consumer Protection (IMCO) stated loud and clear that the adoption of an AILD at this stage is "premature and unnecessary". The reasons behind this strong message reside in both a physiological and a pathological condition of the EU legal landscape. The first one is that much time actually passes between the adoption of a legal act and its effective entry into force. The opinion recalls that, while the AI Act officially entered into force in August 2024, the different rules dealing with low-risk or high-risk AI will be applicable, partly in August 2026 and partly in August 2027. Besides, even the revised PLD will need to be transposed only within the timeframe closing at the end of 2026. It has to be remembered, in the same sense, that the AI Act itself was aware of the issue and, thus, tried to provide a mechanism including the automatic need for revision six months prior to the effectiveness of each set of provisions included in the same. Notwithstanding the above, it is clear that such circumstance, already present for any new body of law, has exacerbated consequences in the field of AI. Thus, the cautionary approach taken in the Draft Opinion about the content of the AILD, especially due to the tight connection with the AI Act already subject to analysis in the present paper, is, once again, completely shareable.

While the opinion on the prematureness can be easily understandable and even agreed upon, the part about the unnecessariness might be faulted. Indeed, the Draft Opinion cites reports and data relating to cost-benefit analysis, informing that the EU's run on AI is significantly slower than forecasted and also declaring that the impact assessment provided by the Commission in 2022 with reference to the AILD proposal relied on hypothetical scenarios rather than concrete data. The input is that an excessive liability or rather procedural law framework risks to deter innovation and increase compliance burdens, particularly for SMEs (that are, indeed, a major part of the market for many EU Member States, Italy included). Moreover, according to the rapporteur, the fact that the AILD proposal envisions changes in the procedural rules could disrupt national civil law systems, which have functioned effectively for decades, including in the digital era. The opinion also mentions the claim that the Commission's perspective in proposing the AILD has more theoretical and academic roots, rather than being based on a balanced assessment grounded in the reality and backed by a comprehensive consideration of relevant data. Despite not assessing in deep whether such conclusions may be regarded as wrong or, at least, sleeting on a fragile ground, it is rather interesting that such perspective is backed by inputs, the content of which is undisclosed, from a variety of entities, including Apple Inc. and OpenAI OpCo, LLC.

Both are closely monitored from a variety of viewpoints relating to the EU regulation of different aspects of digital technologies. Besides, especially the latter is now famously involved in a variety of proceedings relating, in particular, to the training of its systems on

[30] Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Legal Affairs on the proposal for a directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM(2022)0496 – C9-0320/2022 – 2022/0303(COD)), January 19, 2025, available at https://www.europarl.europa.eu/doceo/document/IMCO-PA-768056_EN.pdf (last visited Aug. 14, 2025).

copyrighted works. While all of them are currently ongoing and the majority of which has been filed before courts in the US, something is moving also on the European side of the Atlantic[31], showing that the level of attention is raising in the EU Member States as well. Morevoer, one of the first judgements dealing with the same claims[32], despite recognizing fair use of the copyrighted works by the defendant, has been referred to as "salomonic", since it leaves the door open for a jury trial on the theme of piracy that involves more than billions of dollars in damages. Thus, it is rather interesting to see how the internal interest of the mentioned companies not to be ordered to pay damages on the grounds of their past behavior developing AI systems is linked to voicing their concerns about the disruption of a fragmented system around liability, in contrast with an effort towards an all-encompassing solution, at least partially on the substantial contents. This is not, of course, to say that they may have had any undue interference on the reasoning path of the IMCO, but rather that the current circumstances call, as never before, for the approach suggested by Commissioner Virkkunen. Indeed, the rapporteur of the AILD proposal, MEP Axel Voss, has declared that liability rules are a need in the horizon of creation of a single market, even within a simplification trend. The shared feeling, among both the MEPs supporting the Commission's decision on the withdrawal of the AILD proposal and the MEPs opposing the same, is that the AILD must undergo substantial changes, whether in its form or in its content, but that its own existence cannot be put at stake.

## III. THINGS WE LOST IN THE FIRE AND WHAT CAN BE SAVED

### III.1 *The need for a new beginning*

Multiple concerns have arisen with reference to various features of the AILD and it is needed to address some of them in order to understand the grounds underlying the present text about what can be learned from a failed proposal and where to go after the striking of the same without abandoning the principles that guided its birth.

With purposes of order and clarity, the first one to be addressed will be the one concerning the piece of legislation as a whole and, especially, the compliance of the same with the goal that its authors had in mind when drafting the proposal: the need for harmonization. Such circumstance corresponds to sort of a close road that has posed and will continue to create deep issues. Both the conditions for disclosure of evidence for high-risk AI systems and the ones relating to the presumption of a causal link in fault-based cases are not based on harmonized concepts. Thus, they will leave an unbearable amount of space not only to the national legislators, as in the intentions of the AILD itself, but also to the courts called to implement such provisions.

---

31 M. Tsimitakis, *OpenAI faces landmark copyright lawsuit from GEMA*, available at https://creativesunite.eu/article/openai-faces-landmark-copyright-lawsuit-from-gema (last visited Aug. 14, 2025).

32 Available at https://admin.bakerlaw.com/wp-content/uploads/2025/07/ECF-231-Order-on-Fair-Use.pdf (last visited Aug. 14, 2025).

EU Law relies deeply on the decisions of the Court of Justice in order to be properly addressed, interpreted and updated, especially dealing with bodies of legislation adopted decades ago. It creates almost a unicum in the legal order of Europe, made mostly by codified law systems. However, it is not acceptable to enact new legislation with already such a deep wound in itself, even before being implemented by the national Parliaments. With reference, in particular, to the request to disclosure of evidence, the conditions differ in case the plaintiff advances such request to the defendant or to third parties and, in both these scenarios, first, a great deal of discretion will be undoubtedly provided to the national courts called to evaluate the requests and, even before that, it will be the turn of the Court of Justice to clarify the requirements, namely in relation to the concepts of necessity, proportionality and the balancing of the interests of the parties[33].

It is very much understandable the reason why the EU institutions have reached the choice of a laxer approach to regulation. The nomination of a specific Commissioner for Implementation and Simplification in September 2024, in order to ensure that EU rules and policies in place to support business and protect people are issued in the simplest, fastest and most practical way[34], was only the formalization of an effort pursued since the 1990s under the umbrella goal of "better regulation". It is rather surprising that the international organization that has mostly been accused of its over-regulatory approach is, indeed, the one that has been striving for almost thirty years to strike a balance between the needs for protection of the individual's fundamental rights and of competitiveness of the companies based in its territory. In this sense, the attention has to be drawn back to the roots of the EU system: in the absence of a common political vision (and of any chance to reach the same), the first seed of a uniting effort had to be located in an economic-centric approach and, only later, in the need to guarantee the respect of fundamental rights. It is not completely out of scope that the von der Leyen's Commission has recovered the first goal, despite not being completely aligned with the policy efforts of the previous Presidents of the Commission. The regulatory strategy now centers around the building blocks of competitiveness and cost-reduction for businesses, with an eye specifically on SMEs, while it has been witnessed a rather slow, but steady, shift of the attention away from societal benefits and, especially, from the analysis of the cost of inaction[35]. In this sense, it is interesting to note that the same push towards a double path for liability, through the revision of the PLD and a brand new AILD, might be considered as an exception in this strategy, since it poses the individual again at the center of the picture, with regard to harms caused by the AI-embedded products or services. Nevertheless, the

[33] S. Li, B. Schütte, *The Proposed EU Artificial Intelligence Liability Directive Does/Will Its Content Reflect Its Ambition?*, in *Technology and Regulation*, 147, (2024) available at https://doi.org/10.71265/82fwbw94 (last visited Aug. 23, 2025).

[34] Mission Letter of Ursula Von der Leyen to Valdis Dombrovskis, September 17, 2024, available at https://commission.europa.eu/document/download/71c3190f-0886-4202-846e-5750f188f116_en?filename=Mission%20letter%20-%20DOMBROVSKIS.pdf%22%20%EF%B7%9FHYPERLINK%20%22https://eur01.safelinks.protection.outlook.com/GetUrlReputation (last visited Aug. 23, 2025).

[35] B. Pircher, *Rebalancing EU Regulation: Progressive responses to the deregulation push*, 2025, available at https://library.fes.de/pdf-files/bueros/bruessel/22096-20250604.pdf (last visited Aug. 23, 2025).

approach has been defined as "half-hearted"[36] and this strikes as both the most complete and efficient way to provide a full picture. In order to fully comply with the scope of such piece of legislation, the form of regulation would be preferable, being it the only one able to provide full harmonization in view of the efforts made through the AI Act.

This would also be the road mostly aligned with the close link established between the AI Act and the AILD by the same authors of the latter text. Throughout the years of discussions, confrontations and, oftentimes, quarrels among the various streams of the various EU institutions, such link allowed a prospective widening of the material application of the AILD, once approved and entered into force. As it was explicitly stated under the third recital of the General Prodcut Safety Regulation, "A regulation is the appropriate legal instrument as it imposes clear and detailed rules which leave no scope for divergent transposition by Member States. The choice of a regulation instead of a directive also allows for better delivery of the objective of ensuring coherence with the market surveillance legislative framework for products falling within the scope of Union harmonisation legislation, […]". Also building on the road full of obstacles that the AI Act encountered in the portion of its path preceding the publication of the AILD proposal, between April 2021 and October 2022, it has been clear from the very beginning that the ambitious formal vest of a regulation was a complex horizon to consider for the normative effort around liability. Indeed, bearing in mind the simplification goal and the better regulation framework, it seems that, instead, the AI Act became the unique exception. An unavoidable exception, as it was, before, the GDPR. It is questionable, however, how proposing directives which are actually devoid of any significance without the supporting regulation is the correct direction of action when facing pressing issues such as the regulation of AI.

The more and more evident "directivization" direction of the EU legislative approach is understandable. It follows an enlargement that, on one side, cannot be deemed as completed and, on the other side, led the whole structure to undergo a growing level of fragmentation. The opt-out clauses in the legislative acts have been the key to obtain the consent of some States to become and to keep being part of the Union, while the free circulation of people under Schengen and the Euro-Area is only the most prominent example of the model of differentiated integration. The directivization trend is only the last consequence of it. That reflects, of course, on the true impact that the EU can have on each of the legal systems belonging to the areas of the world outside of it, when it cannot even provide the same level of protection for the rights of its citizens and of the companies based in the Member States.

[36] P. Hacker, *The European AI liability directives – Critique of a half-hearted approach and lessons for the future*, in *Computer Law & Security Review*, 40 (51, 2023), available at https://www.sciencedirect.com/science/article/pii/S026736492300081X (last visited Aug. 23, 2025).

III.2 *Beyond the directivization trend*

The directivization of the normative framework might also be deemed as the most prominent obstacle to harmonization, but the issue goes beyond that. First, the Parliaments of the Member States are called to implement the legislative acts of the Union, with, in some cases, significant delays with respect to the timeframe provided. Moreover, the Member States have the right to challenge the content of the directives before the Court of Justice, meaning that the same is called to provide its guidance on the concepts at the core of the norms being adopted. Despite the concerns about delays and the deep issue posed by such mechanism, again, for the compatibility between the solutions proposed and the high-speed of the changes in the reality, it may be argued that such road is actually the safest choice, since there is a unitary interpretation, provided centrally by the Court of Justice, which both the Parliaments and the national courts have to comply with and, eventually, build upon. Instead, the major concerns arise when the implementation through national bodies of law runs smoothly and the citizens to whom such provisions have to be applied in judiciary proceedings have no other option that hope that the judge activates the process of preliminary ruling according to article 267 TFEU.
The need to strike a balance between the legislative power of the Member States and that of the EU itself has been at the core of the same existence of the EU, with the specific definition (and limitation) of competences, along with the principle of proportionality remaining throughout the decades probably the most sacred provision. Especially in the tumultuous years after the withdrawal of the United Kingdom from the EU, Member States have asked for and have been awarded more and more shreds of sovereignty.
The simplification at the core of the von der Leyen Commission's efforts shall not be translated into less regulation and more self-regulation through codes of conduct developed and applied internally by the various category of stakeholders. Rather, it should lead to a complete re-thinking of the instrument of regulation. The most viable effort could be the production of regulations that do not share the all-encompassing features of the GDPR or of the AI Act, but rather follow the steps already laid out, as a way of example, by the Digital Services Package, with the Digital Services Act and the Digital Markets Act, or by the Data Package, with Data Act and Data Governance Act. The AILD shall, hence, be effectively transformed into an AILR, with the specific changes to its features that will be further highlighted, building on the critiques and suggestions of the experts and of the scholars. The choice of framing such piece of legislation as directive was understandable four years ago, but it can and has to be challenged now. By redefining its premises, it may be possible to envision an instrument able to go not only beyond the obstacles posed by its inner structure, but also beyond its original scope.
The specific content of the proposal also needs to molt in order for the AILR to be a resourceful source of law, able not only to bring the EU into the technological revolution 4.0, but also to provide both the EU enterprises and the EU citizens with the most suitable tools to face the challenges of the reality (which, it will never be stressed enough, is) constantly changing at high-speed pace. The idea of a double system regarding liability is, in substance, correct. The sole revision of the PLD is not currently and will not be able,

in the future, to address the specific concerns deriving not only from AI systems, but especially from the implementation of AI components into the products offered on the market. While, in theory, it is clear that the system will have a manufacturing defect if it is trained with a learning algorithm or with training data that deviate from the manufacturer's intended specifications, the design defects are even more difficult to be identified for a variety of reasons, among which the impossibility for humans to retrace the learning process followed by the system[37]. On one side, such landscape poses to the courts the same issues already highlighted in the context of the AILD, that also the PLD tries, in parallel, to overcome through procedural rules regarding the burden of proof. Despite this perspective not being a complete failure in itself, imagining to see in place only the PLD and, thus, the inclusion of the AI-driven or AI-powered systems under the sole PLD is far from providing the legal subjects with at least a minimum level of protection for their rights. The ex-ante assessment around safety requirements for the AI system and the discussion about the features of liability of the same and of the individuals involved in its development and deployment cannot and should not overlap. In fact, the goal is to consider the different nature of the two approaches, from both a technical and a legal point of view, with the aim of allowing them to converge to create a system suitable both for the enhancement of the market value of the systems itself and for the protection of the fundamental rights of the people.

On the other side, the theme of human oversight (which is the title of article 14 of the AI Act), or lack thereof, with reference to both the process and the outcome of the path of AI system is a further issue in itself. With reference to the current content of the AILD proposal, paradoxically, in the case of technically opaque or complex systems, victims seeking to prove fault may find such task easier when the system is high-risk. Instead, revising the whole framework, courts should be empowered to order the defendant to disclose relevant evidence at its disposal in any case, upon request of an injured person claiming compensation and when the claimant has presented facts and evidence sufficient to support the plausibility of the claim[38].

Besides, with reference to the claim that the AILD is superfluous in the framework of liability established by the PLD, it necessary to remember that, in case no further piece of legislation dealing with the theme of liability in the landscape of AI is enacted, all of the following causes of damage will not be covered, with catastrophic results for the protection of the fundamental rights: discrimination, when AI systems lead to outcomes impacting individuals or groups unfairly; personality rights, among which privacy, dignity and potentially family-related rights, violated as a way of example by the share of toxic, non-consensual intimate or harmful content; intellectual property rights; pure economic

[37] A.-K. Mayrhofer, *Product liability in the age of AI — Proposal for a "two track" solution*, in *Revista Electronica de Direito*, 112 (2024), available at https://cij.up.pt/en/red/previous-editions/2024-no-1/product-liability-in-the-age-of-ai-mdash-proposal-for-a-ldquotwo-trackrdquo-solution/ (last visited Aug. 26, 2025).

[38] B. Botero Arcila, *AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight?*, in *Computer Law & Security Review*, 10 (54, 2024), available at https://www.sciencedirect.com/science/article/pii/S0267364924000797 (last visited Aug. 26, 2025).

loss from damages not associated with physical harm or property damage, but with direct financial losses; sustainability, in relation to the environmental and climate impact of AI systems[39]. In particular, it has become obvious that the fight around IP rights and, specifically, to the fairness of the use of copyrighted works in the training of systems might be the most prominent issue actually involving AI in the everyday life of people in the current age. This happens because, of course, no specific legislation is currently in force in order to regulate such impending matter. Instead, in an unprecedented expression of unity of intents, creatives have joined to make a common front against the unfair exploitation of their works by the developers of AI systems.

As previously mentioned, the US courts in particular have been flooded by complaints submitted by creatives belonging to a variety of fields, from journalist to screenwriters, from narrators to actors. Such issues may seem trivial in the big scheme of things, with the specter of General Purpose AI at the horizon, but, instead, they cannot pass under silence. Such matters are important for the protection not only of the rights of economic exploitation of the copyrighted works, but also for the protection of the fundamental rights of the authors, especially as they have been considered as untransferable in the systems leaning on codified law. But even more, they present a perfect test bench for the topic of liability and for the push towards a regulation of the same that is not only acceptable, but also satisfactory. If AI-generated outputs that reproduce third-party copyrighted works and/or protected subject-matter are deemed to be infringing, the next step to be considered is the allocation of liability resulting from the same. Specifically in the context of generative AI, the traditional bridge between primary/direct and secondary/indirect liability inevitably shatters, leaving ground necessarily open with reference to the need for a rewriting of the terms of service issued by the providers of AI models[40].

## IV. FINAL THOUGHTS

Since many of the most ferocious critiques, as recalled above, have been addressed to the features of the impact assessments produced by the relevant EU institutions with reference to the AILD, it is worth to mention the lines drawn by the same EU Parliament in the latest Complementary Impact Assessment, dated September 2024. It has, first, to be borne in mind that such publication was issued some months ahead of the decision of the Commission to scrap the AILD and it already provides answers to many of the concerns that led to the very much discussed outcome. From such text, it is clear that two

[39] S. Wachter, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, in *Yale Journal of Law and Technology*, 671, (26, 2024), available at https://yjolt.org/sites/default/files/wachter_26yalejltech671.pdf (last visited Aug. 28, 2025).

[40] E. Rosati, *Infringing AI: Liability for AI-Generated Outputs under International, EU, and UK Copyright Law*, in *European Journal of Risk Regulation*, 619 (16, 2025) available at https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/infringing-ai-liability-for-aigenerated-outputs-under-international-eu-and-uk-copyright-law/C568C6B717E9CFC45FB52E58E54B6BEC (last visited Aug. 29, 2025).

main tendencies are, right now, confronting one another in the same EU scenario. On the one side, the cautious willingness of the Commission to defend the steps reached until now, derived from the awareness that the approval of the AI Act is not the last word on the topic, but the start of a new season of discussion and, in many cases, fights on the application and implementation of the same by the national legislators and by the relevant stakeholders. On the other side, the drive of the EU Parliament not to close the door of the topic, but to push the need for regulation forward. The desire (and the plan) of the Parliament is that the AILD is expanded into a more encompassing software liability instrument, able to cover not only AI, but also all other types of software, to ensure that the evidence disclosure mechanisms and the principles of rebuttable presumptions apply universally to all software applications[41]. As highlighted throughout this whole opinion, the different political seasons will have on the subject a heavy weight, due to the fact that the topic concerned is closely tied to any aspect of the everyday life of individuals.

At the present moment, it seems that the attention of the EU legislator is pointed more on looking for a coherence in the different bodies regulating the AI-adjacent fields then on addressing the still existent gaps in the regulatory framework. Such trend seems to be confirmed by the latest normative proposal, the so-called "Digital Omnibus" Regulation[42], issued in November 2025. It is interesting to see how not once the theme of liability is included in the one hundred and fifty-five pages of the document shared by the Commission. Nevertheless, from a lawmaking perspective, it is relevant to note that the nature of the instrument chosen is the Regulation, whose features and impact have been addressed before in the present text.

Lines of thought have been suggested and inputs for discussion have been provided, showing that the only walkable road is in the direction of changing what is already in place to find the most reasonable, yet efficient, mean for regulating a topic that desperately need to be addressed from a realistic point of view. The route is the furthest away possible from being clear, but the only way forward is through the uncertainty, certainly not avoiding it.

[41] P. Hacker, *Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence. Complementary impact assessment*, 25 (2024), available at https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU(2024)762861_EN.pdf (last visited Aug. 28, 2025).

[42] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), available at https://eur-lex.europa.eu/resource.html?uri=cellar:ebf17714-c56e-11f0-8da2-01aa75ed71a1.0001.02/DOC_1&format=PDF (last visited Jan. 12, 2025).

# TOKENISING PROPERTY

*Edoardo D. Martino – Veronica Zerba**

TABLE OF CONTENTS



*This article examines how the blockchain technology reshapes the traditional contract-property divide in private law, leveraging on the peculiar features of non-fungible tokens (NFTs) and real-world asset (RWA) tokenisation. Building on foundational doctrines—*in rem *rights, the* numerus clausus *principle, and third-party notice—we show that blockchain enables the creation of* de facto *property entitlements, including exclusivity and enforceability against subsequent transferees, without State involvement or adherence to traditional publicity requirements. We label this phenomenon "tokenising property." Through illustrative examples, such as NFT royalties, we show how on-chain entitlements may override or bypass the allocation of rights under existing property regimes, raising coordination and enforcement challenges. Using a transaction cost framework, we assess the conditions under which tokenizing property can deliver efficiency gains and when it generates new frictions.*

*Finally, we argue that blockchain regulation rather than private law reforms can reassert control over this new form of property by intervening directly in the technical layer of blockchain systems. This may help in ensuring consistency between tokenised entitlements and the broader legal order, as illustrated by the EU Data Act and the Liechtenstein Blockchain Act.*

**Keywords:** property rights; incompatible contracts; tokenization; NFT

## I. INTRODUCTION

In the past years, blockchain applications experienced an extraordinary development. Indeed, the operations that can be run on blockchain are not anymore limited to the issuance and exchange of virtual currencies. There is a whole new set of heterogeneous activities running on chain which were hardly imaginable when the Bitcoin white paper

* Edoardo D. Martino is Associate Professor of Law at the University of Amsterdam (UvA). Veronica Zerba is PhD Candidate at the University of Trento. This article is the product of shared reflections and thought between the authors. However, for the relevant institutional purposes, paragraphs 1, 2 and 3 can be attributed to Edoardo D. Martino; paragraphs 4, 5, 6 can be attributed to Veronica Zerba.

The authors would like to thank Ugo Malvagna, Filippo Sartori and Massimiliano Vatiero, Maddalena Rabitti. A previous version was presented at the 19th Italian Law & Economics Conference in Brescia, the comments of participants are gratefully acknowledged. All remaining errors are our own.

was first published,[1] such as smart contracts and decentralised autonomous organizations.[2] All these new applications came with the second generation of DLTs, starting with the Ethereum blockchain.[3] The key innovation of these new ledgers was to enable users to build their 'layer two' applications on the naked blockchain.[4]

This article specifically focuses on one of these innovations: non-fungible tokens (NFT). The key technological innovation enabling NFT is the possibility to encode tokens holding unique characteristics leveraging on different blockchain standards.[5] Traditional cryptocurrencies are fully fungible and, accordingly, each unit of Bitcoin or Ether is identical and replaceable with another unit of the same cryptocurrency. In contrast, NFTs are, as the name itself suggests, non-fungible so that each token is unique and distinct from all others.[6] Crucially, these tokens can uniquely represent either a digital asset, such as digital art, or a real-world asset (RWA), such as a piece of real estate or a commodity. The combination of NFTs and RWAs tokenization is still in its technological and business infancy but it holds an immense potential to reshape many industry segments and to challenge traditional institutions–chiefly, the institution of property.

In such landscape, we want to understand what criteria should drive a regulatory intervention on this technological innovation.

To do so, we show that the ability to encode non-fungible assets into tokens and to transfer these via smart contracts change the conditions in which the traditional contract-property divide operates–one of the basic tenets of private law. In fact, parties can privately design and encode rights into tokens and, thanks to the characteristics of the blockchain, these rights are automatically enforced upon the transfer of the token or other pre-specified contingencies. The strength of the automatic enforcement of encoded promises led many crypto enthusiasts equals code to law, following the famous *motto* 'the code is law' proposed by Lessing.[7] While we do not ascribe to such a draconian view, we want to investigate the intricate relationships between code and law.

Specifically, the phenomenon we are describing allows private parties to create new *de facto* property rights. We label this as 'tokenising property'. To steer clear of misunderstandings, this article does not aim to answer the question of whether and to what extent crypto assets can be object of property and the necessary legal amendments to embed crypto assets into the legal system.[8] Rather, we investigate the more structural impact of the,

[1] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, available at <https://bitcoin.org/en/bitcoin-paper> (2008), last visited 24 July 2025.

[2] See, respectively, M. Vatiero, *Smart contracts vs incomplete contracts: A transaction cost economics viewpoint*, Computer Law & Security Review 1 (2022) and O. Borgogno, E. D. Martino. *Decentralised autonomous organisations: targeting the potential beyond the hype*, Law, Innovation and Technology, 19, (II, 2024), 392.

[3] V. Buterin, *Ethereum Whitepaper. Ethereum Whitepaper A Next-Generation Smart Contract and Decentralized Application Platform*, available at https://ethereum.org/en/whitepaper/ (last visited 24 July 2025).

[4] *Ibid*, 34.

[5] M. Kumar, B. Mondal, *Secure Non-fungible Token Marketplaces Using ERC-721*, In *International Conference on Computational Intelligence in Communications and Business Analytics*, Cham: Springer Nature Switzerland, 189 (2024).

[6] J. Fairfield, *Tokenized: The law of non-fungible tokens and unique digital property,* Indiana Law Journal, 97 (2022), 1261

[7] L. Lessig, *Code Is Law. On Liberty in Cyberspace*, Harvard Magazine, 1 (2000).

[8] See, for instance, UK Law Commission, *Digital Assets: Final Report*, available at https://lawcom.gov.uk/project/digital-assets/ (last visited 24 July 2025). For an academic perspective, see R. Sarel, *Property rights in cryptocurrencies: a law and economics perspective*, in North Carolina Journal of Law & Tech., 22 (2021), 389.

currently, most far reaching application of the blockchain technology on the institution of property.[9]

The article demonstrates the disruptive potential of 'tokenising property' and assesses its impact both on the legal system and on societal welfare. In so doing, we build on foundational function frameworks for the analysis of property rights, grounding the economic rationale for the contract property divide.[10]

Relevantly, similar issues arouse from the implementation of Digital Rights Management technology, which was used to protect the right holders in copyright law. DRM prevented the malevolent user to access protected content, allowing only the licensee. However, at the end it had the effect to widen the protection of the right holders beyond the scope of copyright law, as limited by general clauses such as fairness.

In this context the consistency between the digital and legal layer was often difficultly and insufficiently granted. This depended firstly on the lack of a clear-cut distinction between contract and property rights in the field, which often prevented an *ex ante* regulation of the technological layer. Secondly, the legislator was often unable to provide legal and factual access to the beneficiaries of the copyright exception[11].

The peculiarities of blockchain show the importance of our study. From the one hand, the *de facto* effects of tokenizing property potentially involve all rights traded on chain. Tokenising property may, in some instances, bring about efficiency gains, especially in downscaling transaction costs. However, the lost coercive power of the State in the creation and enforcement of property rights may allow for systematic externalization of costs and losses, decreasing the overall welfare and atomizing property entitlements[12]. From the other hand, the blockchain allows to simplify the problem in two respects. Firstly, as all rights traded are involved, it allows to consider situations where the limitations to the property rights are clearly set. Secondly, the DLT is highly programmable, immutable and traceable; this fosters a regulatory response that could help to reconcile the gap between digital and legal layer.

This exercise provides a strong analytical framework to assess the impact of property tokenisation especially on one key dimension–the extent to which the law can still shape property (i.e., '*erga omnes*') entitlements. We show that regulatory provisions on blockchain and smart contracts are the simpler way for the State to still exert control over property creation. In contrast, traditional property law will likely lose its grip given the limited scope of ex-post judicial enforcement, especially when it comes to the breadth of available remedies. The findings of this article are necessarily non-conclusive, given the partly anecdotal nature of the analysis and the impossibility of foresee the evolution of the technology in the future. Nevertheless, we provide a rigorous analytical framework to analyse the impact of tokenising property on traditional legal systems. This can be applied, *mutatis mutandis*, to new applications and upgraded technologies.

The rest of the article unfolds as follows. Section 2 sets the framework, discussing the traditional contract-property divide and mapping the economic justifications of the *numerus clausus* principle. Section 3 provides a brief explanation of the key technological

[9] D. North, *Institutions, institutional change and economic performance,* Cambridge University Press, Cambridge, 1990.

[10] H. Hansmann, R. Kraakman, *Property, contract, and verification: The numerus clausus problem and the divisibility of rights*, The Journal of Legal Studie, 2002, 31, S373 and T. Merrill, H. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, Yale Law Journal, 2000, 110(1), 1.

[11] S. Bechtold, Digital rights managements in the United States and in Europe, American Journal of comparative law, vol. 52, 2004, 323 ff.

[12] M. Heller, *The tragedy of the anticommons: property in the transition from Marx to markets,* Harvard Law Review, 11, 621 (1998). See also F. Parisi, *Entropy in property*, American Journal of Comparative Law, 50, 595 (2002).

components for tokenising property, focusing on the automatic execution to the terms that define the relationship between the parties. Section 4 specifically explains the mechanisms for tokenising property, providing anecdotal examples of its growing importance in market practices. Section 5 analyses the remaining public grip in controlling the creation of property entitlements, focusing on how regulatory law has the potential to shape this new form of *de facto* property.

## II. THE CONTRACT-PROPERTY DIVIDE

Modern Western legal traditions, with different paths and nuances, are rooted in Roman Law at least with regards to private law institutions. Therefore, to investigate the impact of technological disruptions on the institution of property, it is pivotal to introduce an analytical framework that captures the key design features shaping such an institution. In so doing, this section discusses the key 'design features' of property rights as opposed to contractual rights. This allows to appreciate how impactful tokenising property can be, vis-à-vis an institutional equilibrium built in centuries of business experiences. Notably, the contract-property divide is crucial in both civil and common law traditions, despite diverging details linked to the different ways in which these legal systems developed.[13] This latter remark makes the disruptions brought by tokenising property even more momentous.

We focus on three key design features: first, the *in rem* nature of property rights as opposed to the *in personam* nature of contractual ones (Section II.1); second, the *numerus clausus* system of property rights and the control of the State therein (Section II.2); third, the importance of notice towards third parties (Section II.3). Eventually, we discuss the economic justifications for the contract-property divide so to better position the analysis of the impact brought by tokenising property (Section II.4).

### II.1 *In personam & in rem*

The key question for private law institutions tradition is the ways in which individuals exerts control on resources and the extent to which such control is limited. From this standpoint, the contractual or proprietary nature of individual rights over assets shapers the ways in which control can be exerted.

Property rights represent the strongest form of control over assets, ensuring that the owner can benefit from the asset as desired and excluding others from doing the same; in this case, the right insists on the asset itself–the right is *in rem*.[14] This results in the overlap between the thing object of the right and the right itself. This relational view links the right of the owner with a corresponding duty that compels an undetermined number of people–to the limit, the whole society members–not to interfere with the use of the good–the right is *erga omnes*.[15] Such a broad control over the asset is dense of further legal consequences. Chiefly, with regards to the remedies deviced by the State for protecting the property entitlement against breachers, they focus on injunctions and specific performance–

[13] H. Hansmann, R. Kraakman, cit., S402. For an introduction to the role of legal culture in comparative regulatory analysis, see E. D. Martino et al, *An analytical framework*, A. M. Pacces, E.D. Martino, H, Nabilou (eds.) *Comparative Financial Regulation*, Edward Elgar Publishing, Cheltenham, 8. (2025)

[14] R. Epstein, *Takings : Private Property and the Power of Eminent Domain*, Harvard University Press, Harward, 1985, 57 and ff.

[15] W. N. Hohfeld, *Fundamental legal conceptions as applied in judicial reasoning.* The Yale Law Journal, 26, (VIII, 1917)

proprietary remedies–and reflects the prevailing position recognized to the owner.[16] In contrast, contractual rights reflect a legally relevant relationship with a specified person or group of people that are bound by a specific agreement. Such a relationship usually materializes in an obligation that the grantor is required to discharge and that can be enforced against him in case of default. Accordingly, contracts usually bear no third-party effects, i.e., no other member of society is bound by the agreement between the private parties–the right is *in personam*. In this case, the remedies protecting the entitlement of the contractual parties are, by and large, based on the compensation of the damages caused by the default; injunctions and specific performance have a much more limited scope.[17]

Things become more entangled when adding two more variables: the possibility of devising partial rights on assets and the possibility to transfer such asset to a third party. Here the distinction between proprietary and contractual rights becomes extremely consequential. On the one hand, property rights have long been described through the metaphor of the 'bundle of sticks', whereby the full property of an assets can be divided into several specific rights, all supported by the *in rem* nature of property rights–such as the right to use; to manage; to exclude, to possess, to pass, and so forth.[18] Accordingly, the owner can dispose of its right as a whole or partially, by transferring one of the 'sticks' to someone else, with each stick maintaining the proprietary features of the right, including the possibility to enforce such (partial) rights against the whole world.[19] In contrast, if an asset burdened by a contractual right is transferred to a third party, that is transferred free of any burden.[20]

A simple example clarifies this point. *Adam* owns a piece of land that is adjacent to that of *Bernie*. He only needs to access his land during summer months, as it is where *Bernie* spends holiday. To satisfy Bernie's need, the parties can either establish a (property) right of easement, allowing *Bernie* to pass through *Adam*'s land. Alternatively, they can enter into a more complex agreement establishing when and under which conditions *Bernie* can pass through *Adam*'s land. Both structures fully satisfy both *Adam* and *Bernie*'s needs and are considered as equivalent by the parties. However, a few years later, *Adam* transfers the land to *Chloe*. After the transfer, does *Bernie* still have the right to pass to *Chloe*'s land? As most of legal questions, especially when fictional, the answer is 'it depends'. Crucially, it depends on the nature of *Bernie*'s right of passage. In most jurisdictions, an easement is considered a property right: the right of passage for specific days or periods of the year are considered contractual rights. Therefore, upon the transfer, *Chloe* is burdened by the property rights attached to the land, not by the contractual relationship between the previous owner and a third party. The reason why some rights have a proprietary nature and other not is further discussed later on. At this point, it is important to underline that an extremely consequential implication of the *in rem* nature of property rights is that these run with the asset, which means that they "survive unaltered through all kinds of transactions and transformations dealing with other rights" on the same asset.[21] In contrast, contractual rights only bind contractual parties and not subsequent transferees.

[16] G. Calabresi, D. Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, Harvard Law Review, 85(6), 1089, 1092 (VI,1972).
[17] H. Hansmann, R. Kraakman, cit., S413.
[18] H. Demsetz, K. Lehn, *The structure of corporate ownership: Causes and consequences*, Journal of Political Economy, 93, 1155, (VI, 1985); see also A. Dorfman*, Property and collective undertaking: the principle of "numerus clausus*, The University of Toronto Law Journal, 61, 467 (III, 2011).
[19] R. Epstein, cit., 57 and ff.
[20] B. Arruñada, *Property Enforcement as Organized Consent*, Journal of Law, Economics, & Organization 19, 401, 408. (II, 2003)
[21] Ibid, 404.

As we shall see later in this article, tokenising property relaxes this constraint, posing a first significant challenge to the traditional institution of property. To understand why this is so relevant, we need to go back to the earlier unanswered question: why only some rights can be '*in rem*'?

II.2 *The 'numerus clausus' principles*

Why is a general easement of passage on land considered a property rights while a more specific contract allowing a party to pass through a piece of land on specified days or period of the year is commonly considered a contractual right? The answer to this question, however unsatisfactory this may appear, is tautological: because only the specific rights recognized by the legal system as property rights are *in rem* and *erga omnes*. This is known as the *numerus clausus* principle. In all modern jurisditions, including common law ones, "property rights are limited in number (…) and in content" so that "private parties must choose from a predefined set of property rights of which the content is already pre-established, to a considerable degree".[22] In contrast, parties enjoy wide freedom in the design of contractual obligations, with the external limits of not infringing recognized property rights and–especially in the past decades–complying with regulatory provisions.
In modern western legal systems, the *numerus clausus* principle emerges as a push back to the feudal system which was based on the power of the lord to allocate specific powers to specific people, realizing an excessive parcelization on the control of resources. This development is connected to the raise of the middle class of merchants and entrepreneurs in ladder.[23] Therefore, it can be considered one of the basic tenets of modern societies. In this context, the possibility to establish partial property rights was limited as it imposes long-lasting burden on assets[24]. Accordingly, partial property rights were always associated with some central power, granted to the executive or the judicial branch, to unify property rights ex post: think for instance of eminent domain or the judicial dissolution of co-ownership[25].
The *numerus clausus* principle marks the control of the State over the creation of property rights – i.e., of rights that can be coercively enforced against all members of the society. This is consistent with the premises of the Westphalian State as well as with the constitutional approach to private property in the post WWII constitutional democracies. Unsurprisingly, tokenising property holds challenges for the public control over the creation of property-like entitlements, therefore challenging the *numerus clausus* principle. Section 2.4 discusses the economic rationale for the current contract-property divide and further details the dense implications of the existence of the *numerus clausus* principle. Before doing so, it is necessary to look at the information dynamics linked to the contract-property divide and, specifically, to the dissemination of information required to rightfully establish property rights on an asset.

[22] B. Akkermans, The Numerus Clausus of Property Rights, M. Graziadei, L. Smith (eds.), *Comparative Property Law: Global Perspectives*, Edward Elgar Publishing, Cheltenham, 100 (2017). For common law specifications, see H. Hansmann, R. Kraakman, cit., S404.
[23] S. van Erp, Sjef, *Contract and property law: distinct but not separate*, European Property Law Journal, 2, 240 (III, 2013).
[24] H. Hansmann, R. Kraakman, cit., S375.
[25] *Ibid*, S418.

II.3 *Third-party notice*

If a right is enforceable *erga omnes* and runs with the asset in case of subsequent transfer, then all members of society must be put in the condition of knowing who holds property entitlements over such asset. This is the necessary condition for rights to bind third party.[26] Therefore, each property right recognised by the State as such is accompanied by a specific notice mechanism. In contrast, the privity of contract justifies simpler and less formal ways to keep track of parties' reciprocal rights and obligations.[27]
Crucially, parties do not have the freedom to choose the notice system they deem fit, but to validly establish property rights they need to abide by the specific notice mechanisms elected by the political power. The *in rem* nature of the rights directly derives from the observation of the formalities required by the legal system in disseminating the information about the establishment of the right itself.[28] This introduces a ritual element in the establishment of property entitlements in a way that is not dissimilar from ancient Roman forms to transfer property, such as the *mancipatio*.[29]
Therefore, the *numerus clausus* system of property rights goes hand in hand with codified formalities to disseminate information about the establishment of property entitlements. The examples are countless: for the property on movables, good faith possession is usually considered a sufficient notice to third parties, for real estate property the rightful transcription in public registries of the deed of transfer is constitutive of the right to property. In a similar vein, the contract establishing a business organization is granted proprietary features, such as limited liability, only if correctly listed in the business register according to the procedure prescribed by the legal system.[30] The constitutive nature of these formalities allows to govern potentially incompatible contracts granting, for instance, the same property entitlements to different individuals. Only the right established following the prescribed formalities is protected *erga omnes*, including those who acquired the right without following such formalities.[31] Therefore, the *numerus clausus* principle and the notice requirements can be understood as a way to govern incompatible contracts.[32]

II.4 *The contract-property divide: economic justifications*

We have sketched the defining features of the contract-property divide, highlighting how it is the result of centuries of legal evolution. Assessing the economic rationale of this equilibrium is crucial to, eventually, analyse the impact of tokenising property on welfare. A complete analysis of all welfare implications of the property system is clearly out of the scope of this contribution. However, the key elements at play can be easily derived from the seminal and Nobel Prize winning contribution by Ronald Coase. In his work, Coase demonstrates that transacting property rights over assets leads not only to mutually beneficial outcomes for the transacting parties, but also to social welfare maximisation,

[26] C. Rose, *What government can do for property (and vice versa)*, N. Mercuro, W. Samuels (eds), *The fundamental interrelationship between government and property*, Routledge, London, 213 (1999).
[27] H. Hansmann, R. Kraakman, cit., S383.
[28] B. Arruñada, *Property Enforcement,* cit., 411.
[29] B. Arruñada, *The Institutions of Roman Markets*, G. Dari-Mattiacci, D. Kehoe (eds.), *Roman Law and Economics*, Oxford University Press, Oxford, 247, 255.
[30] J. Armour, John, M. J. Whincop, *The proprietary foundations of corporate law*, Oxford Journal of Legal Studies, 27, 429, 450 (III, 2007).
[31] B. Arruñada, *Property Titling and Conveyancing*, K. Ayotte, H. Smith (eds.), *Research Handbook on the Economics of Property Law*, Edward Elgar Publishing, Cheltenham, 237 (2011)
[32] G. Dari-Mattiacci, *The theory of business organizations*, A. Badawi (ed.), *Encyclopedia of Law & Economics*, Edward Elgar Publishing, Cheltenham, 8, 14 (2023).

handling the 'problem of social cost'–i.e., externalities.[33] This is in line with the new institutional economic analysis that approaching institutions – such as property – as a set of formal or informal rules that giving structure economic cooperations in modern societies.[34]

Transacting around property rights can maximise social welfare only under two specific assumptions: first, the costs of transacting must be negligible; second, the allocation of property entitlements before the transaction takes place must be clear.[35] The extent to which these two assumptions are satisfied defines the social efficiency of private bargaining.

Looking at the contract-property divide and the *numerus clausus* principle, the literature has proposed two main interpretations. On the one hand, a closed system of property, centred around the *numerus clausus* principle, generates a remarkable level of standardization that, in turn, reduces transaction costs. Standardized property rights limit the additional information that third parties would need to acquire to ascertain the nature and the value of the asset and, consequently to transact on the asset and allocate it to whom valuer it the most.[36] In this perspective, the State must trade off the benefit of standardization with the costs of the inflexibility of the *numerus clausus* system, adapting the menu of rights with *in rem* effects accordingly.

On the other hand, many see that the standardization of rights and entitlements is more a myth than a reality and, in any case, not the decisive variable to justify a closed system of property rights.[37] In contrast, the *numerus clausus* principle as complemented by third-party notice mechanisms allows all members of society potentially interested in transaction on the assets to clearly ascertain the allocation of property rights over such asset.[38] Such mechanisms work as rules that parties and courts can use to solve both the problems of coordination and enforcement. The first refers to the correct understanding of the allocation of rights on an asset, the second refers to the enforcement of the right against opportunistic behaviour. This literature has identified relevant trade-offs between the third-party notice mechanism (and the information they are able to convey) and the costs connected with their establishment and use[39]. In this perspective, the *numerus clausus* principle is crucial to ensure that property rights are clearly defined *ex ante* and enforceable *ex post*, and, thence, negotiable. Against this background, we analyse the impact of tokenising property and the challenges it brings to the traditional system of property described in this section. Before moving to this analysis, Section 3 introduces in a brief and functional manner the key technological features surrounding tokenising property.

[33] R. H. Coase, *The Problem of Social Cost*, in The Journal of Law & Economics, 3, 1 (1960).
[34] D. North, cit., 61 and ff.
[35] F. Parisi, *Coase Theorem*, in *New Palgrave Dictionary of Economics*, S. N. Durlauf, L. E. Blume (eds), Palgrave Macmillan, London, 859, 863 (2008).
[36] T. Merrill, H. Smith, cit., 24.
[37] H. Hansmann, R. Kraakman, cit., S401.
[38] *Ibid*, cit., S382.
[39] *Ibid*, cit., S382

## III: THE BLOCKCHAIN TECHNOLOGY AND THE INSTITUTION OF PROPERTY

### III.1 *The technological building blocks*

Tokenising property, i.e., the technical possibility for private individuals to design and customise *de facto* property rights over (digital) assets, requires a wealth of technological capability. This section briefly introduces the building blocks necessary to this end.
First, blockchain technology is a necessary pre-requisite for tokenising property. To appreciate the importance of this technological advancement, it suffices to recall that the idea of 'smart property' is not completely new but was already theorized at the end of the 90s as the possibility of controlling real world resources through a protocol.[40] However, doing so would require technological capabilities unknown at the time. Specifically, the blockchain technology features two key characteristics that facilitates tokenising property. First, the distributed ledger, where data representing digital assets is recorded and stored. Second, the consensus protocol that allows the nodes of the network to amend the ledger, adding new blocks which are, in turn, stored and timestamped. The consensus protocol requires the node of the blockchain to invest resources, either computational or financial, to validate the transaction, making sure that the transaction is uniquely carried out, solving the 'double spending' problem.[41] In the context of the contract-property divide, the consensus mechanism can be understood as a device to govern incompatible transactions: only the transaction validated through the mechanism is valid and implemented on the ledger.[42] Therefore, the blockchain is an inherently transactional technology, perfectly fit to allocate rights over (digital) assets and determining who has control over them.[43]
The initial blockchain, the Bitcoin one, only allows for transacting its native token–the Bitcoin. However, this would not be enough for tokenising property as it does not allow for the customization of rights and for the transfer of assets other than the native token. Therefore, smart contracts are the second necessary building block for tokenising property. Unsurprisingly, the theorisation of smart contract dates back to the pre-blockchain era and were first defined "a set of promises, specified in digital forms, including protocols within which the parties perform on these promises".[44] In other terms, smart contracts can be understood as promises encoded in machine readable scripts and formulated in 'if *X* then *Y*" form. These were first embedded in the Ethereum blockchain which allowed to set the terms for the computational execution of a relationship between two or more users through complex operations, and is deployed and executed as an on-chain transaction.[45] Once again, to steer clear of misunderstanding, the discussion about the legal classification of smart contracts is not within our scope.[46] What is relevant for tokenising property is the technical possibility for parties to devise promises that are self-enforceable on-chain when the encoded condition materialize and when the resulting amendment of the ledger is validated through the consensus protocol.

---

[40] N. Szabo, *Formalizing and securing relationships on public networks*, First Monday, 2 (IX, 1997).
[41] M. Xie et al., *A survey on blockchain consensus mechanism: research overview, current advances and future directions*, in International Journal of Intelligent Computing and Cybernetics, 16, 314 (II, 2023).
[42] A. Wright, P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographai,* 7, (2015) available at https://ssrn.com/abstract=2580664 (last visited 24 July 2025).
[43] E. D. Martino, W. G Ringe, *The Social Cost of Blockchain: Externalities, Allocation of Property Rights, and the Role of the Law*, in European Journal of Risk Regulation, 1, 7 (2025).
[44] N. Szabo, cit.
[45] V. Buterin, cit., 11.
[46] For that see, among other, R. De Caria, *The Legal Meaning of Smart Contracts*, European Review of Private Law, 2019, 26 (6), 731.

One additional building block for tokenising property is the ability to transfer the control over assets. Leveraging only on the blockchain and smart contracts parties would be able to transact only on cryptocurrencies and utility tokens. While this is already noteworthy, it lacks the breadth and depth to challenge the institution of property itself. Therefore, the possibility for tokens to uniquely represent either digital or real assets is crucial. This is why the advent of non-fungible tokens (NFTs) holds more disruptive potential than one would think only looking at the rise and fall of the art NFT industry between 2021 and 2023.[47] The possibility of transacting over tokenised non-fungible goods is a fully technical problem that has, indeed, been solved technically through the development of new blockchain protocols, specifically the ERC-721 protocol. The use of this protocol allows for attaching a unique identifier to each token.[48] This technical functionality makes NFTs suitable for encoding singular entitlements and mimicking the exclusivity of traditional proprietary rights and, consequently, opening the door to tokenising property.
Finally, one last necessary building block is the possibility to transact a wide variety of assets on chain, including real world assets. The development of real-world asset (RWA) tokenisation is the most ambitious and the most early-stage element of the construction we are analysing.[49] RWA tokenization requires to represent off-chain assets—ranging from commodities or securities to real estate—through on-chain tokens. Both fungible and non-fungible digital tokens can be used for this purpose, depending on whether the underlying asset is homogeneous or uniquely identifiable. The development of RWA tokenisation has both a technical and legal component. On the technical side, of course, it requires reliable mechanisms for linking the digital token to its off-chain counterpart, ensuring that the token exactly identifies the specific asset it represents. On the legal side, the link between the token and the specific asset must be valid, guaranteeing that on-chain transfers correspond to changes in ownership off-chain.

### III.2 *Freedom of code, automatic enforcement & de facto property*

How can the technological building blocks for tokenising property allows to reproduce on-chain the key features traditionally associated with property rights thereby enabling the creation of *de facto in rem* entitlements? This section tries to connect all the elements introduced so far and, in so doing, offering a grounded analytical bedrock for the proceeding of the article.
Programmable smart contracts allow parties to encode their promises through "if *X* then *Y*" statements. This allows to an extremely high level of sophistication and customizability of these promises keeping transaction costs fairly low. The automatic enforcement guaranteed by the consensus mechanism is the key game changer, eliminating the need for an external coercive apparatus at the point of performance.[50] In fact, standard contractual obligations are guaranteed by *ex post* enforcement through courts; encoded promises are self-executing: the obligation is automatically performed when the encoded conditions are met. This is possible thanks to the consensus mechanisms of the blockchain: once a transaction is validated and recorded on the distributed ledger, it becomes effectively

[47] J. Fairfield, cit., 1268.
[48] X. Tan et al., *Bubble or not: an analysis of ethereum erc721 and erc1155 non-fungible token ecosystem*, International Symposium on Circuits and Systems (ISCAS), IEEE, 2024, 1.
[49] H. S. Shin, *Tokenisation for the real world*, OCC Symposium on the "Tokenization of Real-World Assets and Liabilities", Washington DC, 2024, available at https://www.bis.org/speeches/sp240209.htm (last visited 24 July 2025).
[50] M. Vatiero, cit., 3.

immutable and enforceable within the network.[51] Notably, the ability to hard-code (partial) entitlements within the asset itself effectively mimic the "bundle of sticks" in a digital token. In this setting, the rights and duties encoded in the token runs with it and are enforced at any subsequent transfer.

Compared to the off-chain system, the power of the State in enforcing property rights is by and large substituted by cryptographic and computational consensus. The blockchain can provide a degree of reliability in executing entitlements that rivals, and in time may even surpass, traditional property enforcement. Finally, on-chain transactions are recorded, immutably, on the ledger effectively providing notice of the transfer of (partial) ownership over an asset. The information is technically accessible to all network participants, reducing the risk of hidden encumbrances and strengthening the expectation that entitlements are respected, as long as the blockchain is permissionless.

To appreciate the remarkable paradigm shift of tokenising property, it is useful to reframe the example of Section 2.1. In a (not so) dystopian future, *Adam* has tokenised his piece of land. *Adam* and *Bernie* encode in a smart contract *Bernie*'s right to pass through the land during summer months and attaches this promise to a "tokenised land" asset. When *Adam* transfers the tokenised land to *Chloe*, the token is burdened by the partial encoded right of *Bernie*; hence, it automatically binds *Chloe*. In this example, the right of Bernie to pass through a specific piece of land only during summer months runs with the tokenised asset and is, thereby, enforced *erga omnes*, a result that is not possible under the traditional contract-property divide, unless the *Bernie*'s right is part of the limited menu of rights to which the State assigns proprietary nature Nonetheless, challenges remain. Tokenisation cannot, by itself, prevent the coexistence of conflicting on-chain and off-chain rights. While code can govern entitlements within the network, it cannot unilaterally resolve conflicts with rights recognised–or created–outside it. These frictions underscore the hybrid nature of tokenised property: it emulates the core attributes of *in rem* rights yet lacks the full coherence and integrative power of State-sanctioned property law, at least under the current legal systems.[52]

## IV: A NEW CONTRACTUAL ENVIRONMENT

### IV.1 *Contractual rights running with the asset*

The blockchain environment applied to contracts yields a whole new landscape for the generation and transmission of rights through (smart) contracts.[53] The key features of this environment are transparency, immutability and – most importantly for this contribution – automatic enforcement of the encoded promises.

For a more concrete understanding of such a disruptive contractual environment, a real-life example of tokenising property helps. Consider the case of the art market, both the off-chain version through traditional sales of pieces of arts, and the on-chain one through the sales of NFTs representing pieces of digital art. In the US the monetary rights (i.e.: royalties) of the artist on its art are contractual.[54] This means that artists are weakly protected upon resales, as they have no recourse against the second buyer and can only

[51] A. Wright, P. De Filippi, cit., 11.

[52] S Bechtold et al., *Property Without Law. Personalized Property Rights Through Smart Contracts on the Blockchain*, Yale Journal on Regulation (forthcoming).

[53] E.D. Martino, W.G. Ringe, *cit.,* 13. See also S. Davidson, P. De Filippi, J. Potts, *Blockchains and the economic institutions of capitalism*, Journal of Institutional Economics, 14, 655 (2018).

[54] H. Hansmann & M. Santilli, *Royalties for Artists versus Royalties for Authors and Composers*, in Journal of Cultural Economics, 25 (2001), 261.

sue the original buyer for damages. In contrast, in the EU, royalties are recognized as property right according to the Resale Rights Directive.[55]

In the on-chain market for art, the NFT exchanges for digital art attempted to solve this problem, tokenising the entitlement to receiving royalties upon resale and making it a *de facto* property right. These exchanges were first established in dedicated marketplaces, such as Opensea and Rarible, where artists could opt for a fee, determined as percentage of the price, in the piece of digital art and bind the subsequent purchaser[56]. This option allowed to tokenise the (property) right to royalties but was fairly easy to arbitrage, as the NFT could be wrapped in another token without the royalty option, or moved to a competitor that did not enforce royalties. Therefore, the marketplaces decided not to implement this option anymore. In response to this, the blockchain community created a specific standard for art tokens, the ERC721C – where C stands for Creator – designed to encode the royalties immediately in the smart contract regulating the NFT transactions. These functions close the arbitrage opportunity and allow the original creator to receive a percentage of the sale prize whenever the NFT is transferred, as the fee provision in the smart contract regulates the relationship with subsequent transferees and gives automated enforcement to the creator's claim, making the tokenization of the right to receive royalties upon resale effective.[57] In fact, the effects of the transfer of an NFT are comparable with *in rem* entitlement and this derives directly from the NFT's technical features.

Comparing the outcome of the on-chain tokenization of the right to royalties US law, the disruptive potential of tokenizing property becomes clear: even in the absence of legally sanctioned property rights, artists can have *de facto* property protection. It is important to notice that the royalties embedded in the smart contract is only the last attempt to reach the same result. In the 1970s, the «Projansky contract»[58] (also known as the «Artist's contract»)[59] was conceived for the same purpose[60]. It provided a template contract where a clause provides that in case of resale of the work of art, the original buyer is bound not only to pay to the artist a royalty of a certain amount, but also to use the same contract form in any future sale, so that the subsequent buyer will be bound to the same terms (royalties included).

Looking at the differences between off-chain and on-chain contractual solution helps to further highlight the disruptive potential of tokenizing property. Firstly, while the Artist's contract was seldomly used, this function is widespread in the community. Secondly, the Artist's contract was difficult to enforce in courts, because the courts themselves were suspicious of such a stretch of typical contractual rights effects[61]. In contrast, in the blockchain the automatic execution provided by the code prevents the breach of the provision and ensures the protection of the artist. Given the characteristics of the DLT, an opposite transaction would be required to grant an absolute control to the subsequent

[55] See Art. 1(1) of the EU Resale Rights Directive (Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the Resale Right for the Benefit of the Author of an Original Work of Art, 2001 OJ (L 272) 32.

[56] Opensea, For developers, Setting fees on secondary sale, https://docs.opensea.io/docs/10-setting-fees-on-secondary-sales updated 03/2023.

[57] A. Kutsenko, *ERC721C, a new approach to royalty payments*, at https://metalamp.io/magazine/article/erc721c-a-new-approach-to-royalty-payments-2, 3.06.2025, last visited 21.07.2025

[58] E. Harris, *Mint, sell, repeat: Non-fungible tokens and resale oyalties for Indigenous artists*, in Alternative Law Journal, 48, 11 ff. (I, 203); L. Van Haaften-Schick, A. Whitaker, *From the Artist's Contract to the blockchain ledger: new forms of artists' funding using equity and resale royalties*, in Journal of Cultural Economics, 46, 287. (II, 2022).

[59] The contract can be found at https://primaryinformation.org/product/siegelaub-the-artists-reserved-rights-transfer-and-sale-agreement/.

[60] B.L Frye, *Equitable Resale Royalties* in Journal of Intellectual Property Law, 24 237 ff. (II, 2017).

[61] B.L Frye, *Equitable Resale Royalties,* 246 ff.

transferee, as such requiring the consent of the beneficiary. In this scenario, contractually created rights effectively run with the asset, a characteristic that only state sanctioned property rights can have off chain.

The on-chain tokenization of property rights may collide with off chain legal property. We can think at least of two examples. First, the content of the on-chain claim may not be compatible with a property right as established by law off chain; second, the legal publicity requirements to create property rights off chain are not satisfied. In this latter case, a transfer on chain alone could not immediately confer a legal property to the recipient but require the fulfilment of the applicable publicity rule and, when necessary, the collection of the consent of every property right owner.[62] In the former case, the tokenisation of real-world asset further complicate the matter: off-chain transactions are not constrained by the consensus mechanism so that it is in principle possible that incompatible rights are granted on chain and off chain. Due to the control exerted on the asset through DLT technology, the smart contract will always grant a substantial advantage, regardless of the classification of the claim as a property or contractual right. In this context, DLT technical features will hinder the enforcement of legal provision, even after judicial proceedings, leaving only damages remedies and making injunctions unavailable.[63] Blockchain offers a powerful tool to grant to others a substantial control on (tokenized) physical and digital resources, publicly recorded on a DLT ledger and automatically executed, altering the traditional economic justification of the *numerus clausus* principle: namely, the necessity to give a solution to the coordination and enforcement problem, and the deriving transaction costs.

IV.2 *A transaction cost analysis*

Transaction costs are determined by the interaction of legal and informal constraint and how contracts are enforced[64]. Relevantly, they can derive from discrepancies between the technology functioning and legal rules. When DLT is concerned this is recurrent, due to the difficulty (or impossibility) to effectively replicate legal rules (national-bound) through technical layers (internet based)[65].

When the technology clashes with legal institutions and hinder their functioning, it can also alter the equilibrium of the market for the allocation of entitlements, resulting in deadweight losses and inefficient allocation as a direct consequence of the automatic enforcement guaranteed by smart contracts.[66]. On the other hand, smart contracts can also provide a solution to the coordination and enforcement problems, going beyond the *numerus clausus* principle. In fact, smart contracts also provide publicity, automatic

[62] B. Arruñada, *Blockchain's Struggle to Deliver Impersonal Exchange* in Minnesota Journal of law, Science and Technology 19, 55 ff. (I, 2018); R.M. Garcia-Teruel, H. Simón-Moreno, *The digital tokenization of property rights. A comparative perspective* in Computer Law & Security Review, 41 (2021); O. Borgogno, E. D. Martino, *cit.*

[63] This rewrites some of the most foundational analysis about property and liability rules. See G. Calabresi, D. Melamed, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, Harvard Law Review, 85 (1972).

[64] D.C. North*, cit.*

[65] E. Tjong Tjin Tai, *Smart Contracts As Execution Instead of Expression* J.G. Allen & P. Hunn (eds.), Smart Legal Contracts, Oxford University Press, Oxford 2022, 222. The author actually suggests that is sterile to even attempt such an operation, given the advantages brought by smart contracts of "simply attaching factual consequences to the fulfilment of certain conditions".

[66] H. Eenmaaa-Dimitrieva, M.J. Schmidt-Kessen, *Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts*, Computer Law & Security Review: The International Journal of Technology Law and Practice, vol 35, 2019, 69-88. The author brings many examples – one for all, the impossibility to verify whether the consent of one of the parties is defective.

execution and are characterized by a necessary internal consistency. Therefore, understanding the net impact of DLT contracting on transaction costs is not straightforward,

On the one hand, the DLT technology provides an easy access to reliable information concerning the features of the token and its previous transactions on chain. The availability of browsers that search public ledgers levels the playing field between users and non-users. This substantially reduces search costs, minimizing adverse selection or the possibility to transact on assets burdened by competing claims, as long as they are recorded and traded on chain. In this instance, the blockchain reduces the need to build reputational capital and to rely on traditional intermediaries[67]. In the enforcement phase, the automatic execution relieves parties from the cost of monitoring the counterparties to detect defaults.[68]

On the other hand, the DLT technology can also increase transaction costs. Firstly, its immutability and automatic execution result in lack of flexibility. It must be noted that, while parties can take into account a great variety of contingencies, there will be always limitation determined by human failure. In other terms, smart contracts cannot be perfectly contingent: contracts remain incomplete and, unlike the off-chain environment, do not provide flexibility for adaptation.[69] Moreover, any efficient breach would be automatically prevented.[70] Finally, the phrasing of the smart contract as a code will also deprive the parties from the shades of the legal language, providing only for on/off solutions[71].

In addition to the transaction costs borne by the contracting parties, there can be significant externalities. The use of consensus mechanism leads to environmental concern, due do its consumption of energy and water[72]. Moreover, the necessity to check for tokenisation by non-users raise questions on digital literacy: as the population is averagely becoming older and older, it is impossible to imagine that the blockchain will be so widespread (and elder-friendly) that everybody could access easily such new technologies, at least at the moment.

From the existence of not negligible transaction costs that arise from tokenizing property, we can infer that the *numerus clausus* principle may still be economically justified. However,

---

[67] C. Catalini, J.S. Gans, *Some simple economics of the blockchain* in NBER Working Paper Series, Cambridge, (2016 revised 2019), available at http://www.nber.org/papers/w22952; J. McMurren, A. Young, S. Verhulst, *Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers* (2018) available at https://blockchan.ge/blockchange-land-registry.pdf (last visit: 1st February 2026).

[68] D. Tapscott, A. Tapscott, *How blockchain will change organizations* in MIT Sloan Management Review, 58 (II, 2017) available at https://sloanreview.mit.edu/article/how-blockchain-will-change-organizations/; S. Davidson, P. de Filippi, Primavera, J. Potts *Economics of Blockchain* in Public Choice Conference, May 2016, Fort Lauderdale, United States; C.G. Schmidt, S.M. Wagner, *Blockchain and supply chain relations: A transaction cost theory perspective,* in Journal of Purchasing and Supply Management, 25 (IV, 2019).

[69] M. Vatiero, *Smart contracts and transaction costs*, Discussion Papers del Dipartimento di Economia e Management – Università di Pisa, n. 238, 2018 http://www.ec.unipi.it/ricerca/discussionpapers.html; M. Vatiero, *Smart contracts vs incomplete contracts: A transaction cost economics viewpoint*, in Computer Law & Security Review, 46 (September, 2022) 1 ff.; J.M. Sklaroff, *Smart Contracts and the Cost of Inflexibility,* University of Pennsylvania Student Papers, Prize Winning Papers n. 9, 2018, https://scholarship.law.upenn.edu/prize_papers/9.

[70] E. Mik, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, 12 (2017), Available at SSRN: https://ssrn.com/abstract=3038406; H. Eenmaaa-Dimitrieva, M.J. Schmidt-Kessen, *cit.,* 40 ff.

[71] M. Vatiero, *Smart contracts and transaction costs*, cit.,11; J.M. Sklaroff, *cit.*, 282 ff.

[72] D. Ramirez-Escudero, *Bitcoin's water consumption is an environmental threat?,* https://cointelegraph.com/news/bitcoin-water-consumption-environment-adoption, last visited 28/07/2025.

finding the right balance between on chain property tokenization and off chain property guided by the *numerus clausus* principle is, again, a complex exercise.[73]
The potential differences between the legally provided allocation of rights and the technological allocation of resources are clearly a new source of transaction costs that should become part of any cost-benefit analysis when considering the desirability of State intervention. In fact, in case of competing on-chain and off-chain claims on the same asset the impossibility to edit the chain, would require the parties either to enter into an equal and opposite on chain transaction or to grant the owner the control of the blockchain account ex ante.[74] As a consequence, the absence of a *numerus clausus* on-chain leads to an extraordinary increase in the number of transactions and entropy in property, with the creation of too many tokenized rights enjoying property-like status.[75]

Furthermore, the enforcement of legal rights can become increasingly problematic. Since on chain promises are self-executing, courts may be extremely restrained in the type of remedies they can adjudicate outside of what has been encoded: all mandatory rules would be set by the parties and not by the law. It is technically possible to provide for some flexibility in the code, allowing judges to intervene, but this depends entirely on the parties' willingness.[76] Thereofre, the power of the judge would arise *if and only if* the parties agree to it ex ante, and *if and only if* they *allow* judicial authorities to take control of the tools. This looks much more like an arbitration clause that the standard powers of the judiciary.

### IV.3 *Possible private law solutions*

The use DLTs and smart contracts to allocate tokenised entitlements that enjoy property-like protection alter the dynamics between contract parties and affect transaction costs. This questions the *numerus clausus* principle, both when understood as a standardization tool and as a way to solve issues arising from incompatible contracting.

When facing this challenge, legal systems have two options to try and achieve optimal legal solutions through private law, so to ensure that entitlements are allocated to parties that value them the most. The first approach can be labelled as "do nothing approach", where a jurisdiction accepts this change while not addressing it directly. This first approach can be found in several legal systems. For instance, the UK Jurisdictional Task Force has adopted a Legal Statement in 2019 for transactions of native digital assets, recognizing that crypto-assets can be the object of property but, at the same time, considering DLT records as merely presumptive and unable to "be treated as a definitive record of legal rights".[77] Finally, a bill has been passed that introduces a third object of property beyond the traditional categories of things in action and things in possession in order to accomodate digital assets as the object of property.[78] Such principle is already judicially sanctioned[79] and the bill would simply provide it with statutory recognition without altering the essence

[73] E.D. Martino, W.G. Ringe, *cit.*
[74] J. Woxholth, D.A. Zetzsche, R.P. Buckley, D.W. Arner, *Competing Claims to Cryptoassets*, University of Hong Kong Faculty of Law Research Paper No. 2023/27, Available at SSRN: https://ssrn.com/abstract=4394952 or http://dx.doi.org/10.2139/ssrn.4394952.
[75] F. Parisi, *Entropy in Property*, American Journal of Comparative Law, 50 (2002).
[76] O. Meyer, *Stopping the Unstoppable - Termination and Unwinding of Smart Contracts, in* Journal of European Consumer and Market Law, 9, 17 ff. (2020).
[77] UKJT, *Legal statement on cryptoassets and smart contracts,* pt. 132 ff, 30. M. Lehmann, *National blockchain laws as a threat to market integration*, in Uniform Law Review, 26, 157, (2021).
[78] Property (digital asset) Act 2025, approved on 2nd December 2025; See: L. Palmieri, D. Pyper, Property (digital assets etc) Bill [HL], https://commonslibrary.parliament.uk/research-briefings/cbp-10305/
[79] AA v Person Unknow, [2019] EWHC 3556 at [55]; D'Aloia v Person Unknown [2024] EWHC 2342 (Ch)

of existing property laws, as its applicability depends ultimately from the traditional indicia[80].

This approach has the advantage that it does not preemptively bend the existing legal categories. However, it may result in increased inefficiencies when a) the entitlements transacted on chain and off chain are likely to be incompatible; *or* b) the content of the entitlement transferred on chain is compatible with an off-chain entitlement but the transfer on chain does not fulfil the publicity requirements; *and* c) the benefits from using the blockchain are sizeable, so that parties mainly use on chain transactions An alternative, second approach could be to statutorily alter the divide between property and contractual right, for instance recognizing the control exerted through smart contract as a mechanism to establish (existing) property rights. In a more daring version, this could mean to expand the number and features of existing property rights. An early example of this approach can be found in in the Italian legal system, in the case of trading of security-token. Under Italian law, the circulation of securities requires an annotation on the registries as a form of third-party notice. In contrast, with a legislative reform introduced by the Law 52/2023 (artt. 3 and 5), security-tokens can be issued and traded simply through the DLT platform, which also means that issuing and trading generates and transfer property rights also off-chain.[81]

The Unidroit Principles on Digital Assets represents another example of this sort.[82] The principles are applicable to the governance of property on digital assets by choice of the parties who encode them in the digital assets or in its recording system, or by reference of the State Law (pr. 5, par 1). The Unidroit Principles define "control" as an exclusive but shareable *de facto* relation with a digital asset, conferred by the asset itself, the system or the protocol, pertaining the possibility of exploiting the asset, excluding the others from doing so and transferring such powers. These conditions are satisfied in DLT technology whenever a private key controls a digital asset (comm. 2.24, 6.5). Despite its *de facto* nature, transferring control on a digital asset allow the creation of a security right effective against third parties, additionally to the methods provided by State law (pr. 15). With this principle, blockchain can effectively be used to create a property right on a digital asset, transferring it on chain, and with priority against the creditors who claim a security right on the same asset but created and made effective against third parties with other methods (pr. 16).

Both the 'do nothing approach' and the partial shift in the contractual and property divide can work as a tool to address the shift in transaction costs in the digital environment. The best solution obviously depends on the particular features of the market sector considered. Both of them foster a reflection on the current allocation of property rights, as a private law solution that leaves unaffected the traditional market mechanisms. Nonetheless, they cannot ultimately solve the enforcement issues and the creation of potential externalities. To the contrary, externalities may even increase. Therefore, in some legal systems additional regulatory provisions were implemented in order to close the gap between the digital and legal layer. In the next section, we investigate the regulatory potential to govern tokenising property.

[80] UK Law Commission, Digital assets as personal property: Supplemental report and draft Bill, 2024, many times in the report, eg. 49.

[81] S.M. Scalera, *Tokenizzazione di partecipazioni di società di capitali*, phd thesis dissertation (2024) available at https://ulb-dok.uibk.ac.at/ulbtirolhs/content/titleinfo/9627035 (last visit 2 february 2026)

[82] UNIDROIT, *Principles on Digital Assets and Private Law* adopted on 10-12 May 2023, and published on 4 October 2023 at https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/#1488897069871-af7a84cf-bd9a.

## V: REGULATING THE TECHNICAL LAYER

In recent year, several experimental solutions have been advanced to address the legal challenges of the blockchain technologies. Some of these also impact the allocation of entitlements complementing the application and enforcement of traditional legal categories. We can consider these as solution enabling to close the gap between the digital or real-world layer, ensuring consistency. Through these lenses, we briefly analyse the relevant provisions of the EU Data Act and the Lichtenstein "Blockchain Act".

### V.1 *EU Data Act*

The Act provides a legal framework for non-personal data produced by the "Internet of Things" and aims at a wider access to data, opposing the tendency of data manufacturers to lock in data through a technical layer not accessible for the users (Recital 20). Accordingly, the Act allocates specific rights to users such as a right to access, share with third parties, and switch provider. The access and use of data, when non statutorily mandated, are contractually regulated between the user and the data holder (art. 4 par. 13 and par. 14). Data must be shared between the data holder and the data recipient upon request of the user (art. 8). While strengthening the position of the user in exploiting data, the Act does not generally recognize new property rights,[83] nor does it establish protection for the data holders, allowing to ask for compensation to data recipient.[84]

What is interesting for our purpose, is that the Data Act envisions the use of smart contract to reduce transaction costs connected to data sharing (Recital 47)[85] as well as to prevent unauthorised access to data (art 11 par. 1). Within this framework, smart contracts are defined in art. 2, par. 1, n. 39 as "*a computer program used for automated execution using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological order*". This definition, though conceived in a technologically – neutral fashion (Recital 104), clearly includes the DLT smart contracts.

The Data Act establishes specific requirements for the use of these smart contracts, in the attempt to incentivize their use while curbing the risks arising from interoperability. Specifically, the vendor or the deployer of the smart contract shall include in the smart contract a mechanism for its "*safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions*". The provision aims to ensure the respect of the "mutual consent among parties" (Recital 106) and halts accidental executions. From the formulation, it remains doubtful who will push the button.

Given the spirit of the Act, it is maybe not too forward to interpret the provision in the sense that it prevents a *de facto* control, in favour of the data holders or of the data recipient, to grant the smooth circulation of data. This regulatory provision supports an on-chain transactional environment for data, clarifying the initial allocation of property rights and providing remedies against unwanted self-executions.

---

[83] H. Graux, *What is data ownership and does it still matter under Eu Data law?, https:*//data.europa.eu/.

[84] M. Eckardt, W. Kerber, *Designing the Bundle of Rights on IoT Data: The EU Data Act*, The Data Act: First Assessments, A. Sattler, H. Zech, (eds) Trier.3-22, Available at SSRN: https://ssrn.com/abstract=4879176 or http://dx.doi.org/10.2139/ssrn.4879176.

[85] F. Casolari, M. Taddeo, A. Turillazzi, L. Floridi, *How to Improve Smart Contracts in the European Union Data Act,* Digital Society, 2023, vol. 9, 8 ff.

V.2 *The "Blockchain Act" in Liechtenstein*

A second example of rules 'enabling' the efficient allocation of entitlements through tokenising property can be found in the "Blockchain Act" adopted in Liechtenstein in 2019.[86] The Act applies to "trustworthy technology", including (but not limited to) the blockchain and showcase innovative solutions in regulating the civil law effects of the token economy. The Act defines the token as a "container"[87] that can represent every right, property included. Consequently, there are two relevant features to considered: the digital assets, and the claim embedded in the token.

As for the digital asset itself, Liechtenstein civil law does not allow to establish ownership on immaterial objects. The Blockchain Act does not modify that but defines the legal entitlement towards the token as a "right of disposal", with features comparable to a property right[88]. Its acquisition is conditioned not only to the DLT transfer of the token but also to the agreement between parties and the legal entitlement of the transferor (art 4): the provision replicates the duality of title and *modus* for the transfer of property typical of German Law countries.[89] When these conditions are met, the disposal of the token determines also a legally valid transfer of the embedded right (art 7, par. 1)[90]. The disposal through DLT can be opposed against both the transferor and third parties in case of enforcement proceedings against the transferor (art 7 par 3). However, in case of further mandatory publicity requirements provided by law, these cannot be overlooked so that the mere transfer of the token does not effectively transfer property but only implies the legal obligation to do so (art 7 par 2 lett. a).[91]

The Liechtenstein Blockchain Act expands traditional property law. First, it creates a new legal object of rights that is functionally equivalent to a property right. Second, it tokenizes contractual claims, and opposes their transfer through DLT against third parties. However, for the valid transfer of property rights, existing legal requirements must be upheld: the handover of the possess of the asset, in case of movables; the registration, in case of immovables.

When it comes to incompatible contracts, Liechtenstein is conscious of the possibility of competing claims on the same asset and, accordingly, the Blockchain Act established various procedural safeguards. First, when the transferor has correctly disposed the token on the DLT but has still not fulfilled all the other necessary requirements for the transfer of property, he must make sure that no competing claims are established on the subject (art 7 par. 2).

---

[86] Also known as Token and Trusted Technology Service Provider Act (TVTG), entered into force on 1st January 2020.

[87] *Unofficial Translation of the Report and Application of the Government to the Parliament of the Principality of Liechtenstein concerning the Creation of a law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) (Blockchain Act),* n. 54/2019, 54 available at https://impuls-liechtenstein.li/wp-content/uploads/2021/02/Report-and-Application-TVTG-extract.pdf.

[88] A. Ferreira, P. Sandner, T. Dünser, *Cryptocurrencies, DLT and crypto assets – the road to regulatory recognition in Europe,* Handbook on Blockchain, M. Thai, D. A. Tran, B. Krishnamachari (eds), Springer 661 ff (2022).

[89] S. van Erp, *Land registration and "disruptive" (or "trustworthy"?) technologies: Tokenisation of immovable property*, in IMOLA II Project. The European Land Register Document (ELRD): A common Semantic Model for Land Registers Interconnection, A. Fraga, E. Ioriatti S. van Erp (eds.), 13, (2019) Available at SSRN: https://ssrn.com/abstract=3441938; M. Lehmann, *cit.,* 159.

[90] *Unofficial Translation of the Report and Application of the Government to the Parliament of the Principality of Liechtenstein concerning the Creation of a law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) (Blockchain Act),* cit. 57; literature: A. Ferreira, P. Sandner, T. Dünser, *Cryptocurrencies, DLT and crypto assets – the road to regulatory recognition in Europe*, cit.

[91] S. van Erp*, Land registration and "disruptive" (or "trustworthy"?) technologies: Tokenisation of immovable property,* cit., 14.

Further obligations rests with professional service providers, in particular, the tokenisation service provider and the physical validator. The first "*puts Tokens into circulation for clients and ensures the legal and technical requirements vis-à-vis third parties for effective representation and transfer of rights via Tokens*" (art 2 lett. m). She is required to ensure that the technical and legal features give consistency to the disposal of the token and the disposal of the embedded right against third parties. In particular, she must ensure the correct representation of the right, that its disposal is the immediate consequence of the disposal of the token, and that competing rights on the embedded right are technically and legally excluded (art 17 lett. b) [92]. When rights to physical assets are involved, a physical validator plays a complementary role in working off chain and in ensuring "*the enforcement of rights in accordance with the agreement, in terms of property law, represented in Tokens on TT systems*" (art 2 lett. p; art 17 lett e.). Practically, this involves also to ascertain the existence of the asset, the identification of parties, and that no incompatible claims are granted [93]. Both the tokenisation service provider and the physical validator are liable if they cause damages as a result of a breach of their obligations (art. 9a) and must award compensation.
Both the tokenization service provider and the physical validator are supervised entities: they must be registered and are under the supervision of the Financial Market Authority, which can cancel their registration if they systematically fail to abide to its legal obligations. The main purpose of these intermediaries is to ensure the consistency between the legal, factual and technological landscape. Operating in the tokenisation phase, the tokenisation service provider is able to provide consistency in an environment where smart contracts are able to shape property right in an asset. From the one hand he ensures the correct representation of the right; from the other, he grant the opposability of the transfer of a token against third parties. At the same time, the risk of incompatible contracts in token representing physical assets is minimized thanks to physical validators. In this perspective, the two professional figures support the legal allocation of entitlements. imposing constraint to limit the freedom of parties on chain.

V.3 *Regulatory provision shaping the transaction environment*

These two examples highlight the possibility to use the regulation of the technical layer to support the allocation of entitlements in the digital environment, ensuring the coordination with the legal system. It is still too early to say whether this will become a general trend.
In particular, in the case of the EU Data Act, the decision not to allocate a property right on data leaves with the need to ensure that the use of smart contract does not *de facto* nullify this provision. Consequently, the lawmaker intervenes directly on the technical layer, providing a mechanism to halt the smart contract.
In the case of Lichtenstein, a similar role is played by the intermediaries introduced by the policymaker and supervised by the administrative authority. The tokenisation of contractual claims has an effect similar to securitisation, with the consequence that its transfer is opposable to third parties, and consequently, that the debtor can discharge her obligation by paying directly to the holder. In this context, the Blockchain Act mandates the tokenisation service provider to ensure that the token has the digital and legal

[92] *Unofficial Translation of the Report and Application of the Government to the Parliament of the Principality of Liechtenstein concerning the Creation of a law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) (Blockchain Act),* cit. 60. while the text refers to the token generator, after the modification of art 17 of the Blockchain Act in 2024, some functions, previously exerted by the token generator, were conferred to the tokenisation service provider.
[93] *Unofficial Translation* … cit., 68.

characteristics to grant consistency with the legal system. As far as property claims on physical assets are concerned, the physical validator, who takes care that the assets exist, is owned by the transferor, and that no incompatible contracts are concluded.
The regulation of the technical layer is promising; however, key challenges still persist. One can for instance thinks of the high quantity of transactions on chain, the anonimity and the number of players constantly updating the chain.[94] The choice to impose the relevant requirements on the vendor and deployer on chain (EU Data Act) or on supervised intermediaries (Lichtenstein Blockchain Law) appears appropriate.

## VI. Concluding Remarks

This article analyses how blockchain technology and smart contract, particularly NFTs and real-world asset tokenisation, disrupts the traditional contract-property divide. By revisiting foundational private law doctrines—in rem rights, the *numerus clausus* principle, and third-party notice—we show that blockchain allows private parties to replicate many of the core features of property rights without State involvement. Through smart contracts, entitlements can be embedded directly into tokens, enforced automatically through consensus mechanisms, and made publicly visible on a distributed ledger. This combination effectively creates de facto property entitlements, allowing rights to "run with" tokenised assets and bind subsequent holders, even in the absence of formal recognition by the legal system.
This phenomenon challenges the institutional balance carefully built into private law. By bypassing the *numerus clausus* and publicity requirements, tokenising property risks proliferating uncoordinated, privately designed entitlements, potentially increasing transaction costs and generating negative externalities. At the same time, it can offer efficiency gains by lowering enforcement and information costs, expanding access to sophisticated transactional mechanisms, and enabling novel forms of asset management and monetisation.
Our analysis suggests that the State's traditional control over the creation and enforcement of property rights cannot simply be transposed into decentralised digital environments. Reforming private law may be feasible only for subset of tokenised assets, like securities. In contrast, public law should intervene at the technical layer to ensure alignment between tokenised entitlements and the broader legal order. Instruments such as the EU Data Act and Liechtenstein Blockchain Act illustrate how regulatory provisions—through interoperability requirements, supervisory oversight, and technical safeguards—can restore coherence to an otherwise fragmented property landscape.
Tokenising property ultimately forces legal systems to face a pivotal question: should the creation of property-like entitlements be left to code? The answer will shape not only the future of property law but also the institutional role of the State in digital markets.

[94] V. Lehdonvirta, R. Ali, *Governance and regulation,* UK Government Chief Scientific Adviser (ed.), Distributed Ledger Technology: Beyond Blockchain.