REVISTA DE DIREITOS HUMANOS
E DESENVOLVIMENTO SOCIAL

DOSSIÊ

Artificial intelligence, data protection, and human rights

Editors
Fernanda Carolina de Araújo Ifanger and Lucas Catib De Laurentiis

Conflict of interest
The author declare they have no conflict of interests.

Received
October 29, 2024

Approved
October 29, 2024

Why is European protection of personal data not a legal limit to the development of artificial intelligence? A critical analysis of the relationship between the General Data Protection Regulation and the proposal of a European regulation on artificial intelligence

Por que a proteção europeia dos dados pessoais não constitui um limite jurídico ao desenvolvimento da inteligência artificial? Uma análise crítica da relação entre o Regulamento Geral sobre a Proteção de Dados e a proposta de regulamento europeu sobre a inteligência artificial

Christina Koumpli[1]

[1] Associate professor of public law and will hold the Partnership Chair "Compliance & Innovation" at Avignon University. Avignon, France. E-mail: <christina.koumpli@univ-avignon.fr>.

How to cite this article: Koumpli, C. Why is European protection of personal data not a legal limit to the development of artificial intelligence? A critical analysis of the relationship between the General Data Protection Regulation and the proposal of a European regulation on artificial intelligence. *Revista de Direitos Humanos e Desenvolvimento Social*, v. 5, e249950, 2024. https://doi.org/10.24220/2675-9160v5a2024e9950

Abstract

The article puts forward the proposition that the function of European personal data protection as a legal limit and anthropocentric guarantee is increasingly called into question in the context of the development of artificial intelligence.

Keywords: Artificial intelligence. Data protection. European Regulation.

Resumo

O artigo propõe que a função da proteção europeia dos dados pessoais como limite jurídico e garantia antropocêntrica seja cada vez mais posta em causa no contexto do desenvolvimento da inteligência artificial.

***Palavras-chave**: Inteligência artificial. Proteção de dados. Regulamento Europeu.*

CC BY

Introduction

"Artificial Intelligence (AI) yes, but the European way", said the European Data Protection Supervisor (EDPS) in October 2023 (European Data Protection Supervisor, 2023a). Although these words may initially appear to be colonialist in nature, a few lines later, the text makes a number of universal declarations. The overarching aim of the EDPS is to "ensure that AI is integrated into everyday life in a human-centered and sustainable way, respecting the principles of privacy and personal data protection" (European Data Protection Supervisor, 2023a).

It can thus be posited that the European approach to AI is "human-centered AI". In order for this to occur, the "recipe" in Europe is AI systems that respect the principles of privacy and personal data protection. This can be defined as AI that respects the European Regulation on Data Protection (GDPR). Consequently, the European co-legislator (European Parliament and the Council) has determined that the EDPS will serve as the future controller of AI in EU institutions, while the personal data protection authorities will oversee AI in member states. This represents a clear indication that European personal data protection is a prerequisite for the development of human-centered AI.

The provided contribution aims to conduct a critical analysis precisely by questioning this premise. In other words, the question is whether and to what extent the protection of personal data constitutes a sufficiently effective framework for protecting individuals and society from the potential abuses of AI.

A review of the current discourse by European and national institutions following the proposal of a Regulation of AI (RAI) indicates a perceived need to limit the potential for adverse effects on fundamental rights, yet the specific rights and risks involved remain undetermined. This lack of clarity has resulted in concerns about the protection of personal data. The potential meaning of this "high risk to fundamental rights" is "absorbed" by the European data protection framework, which is constituted by the right to privacy and data protection (Arts. 7 and 8 of the European Charter of Fundamental Rights [ECFR]) and the GDPR's compliance procedures.

It can be argued that the use of an appeal to 'fundamental rights' and the protection of personal data serves to compensate for the shortcomings of the current regulatory framework governing AI. However, is it pertinent to question whether the European legal framework governing the protection of personal data provides sufficient, clear, and effective legal rules to contain or reduce the risks posed by AI to fundamental rights? In other words, is European data protection the best legal tool to use to limit the potential damage to fundamental rights?

Thus, emerges the hypothesis that using personal data protection to regulate AI does not solve the "risk to fundamental rights", nor does it make AI human-centered through the magic of words.

This would presuppose that:

1. Artificial intelligence (AI) is fundamentally reliant on the processing of personal data.

2. The European personal data protection framework is to be exclusively human-centered in its orientation.

3. The protection of personal data is a matrix protection for the protection of all other individual fundamental rights.

4. The European personal data protection is effective, i.e. its capacity to avert damage to individuals before it occurs.

Prior to addressing these questions, it is imperative to concentrate on the procedure of formulating regulations pertaining to AI within the EU, as well as the context and substance of the forthcoming European style 'Artificial Intelligence Act'.

AI Regulation as part of normative colonialism, with the GDPR as an inaugural example

A. Institutional interactions between data protection and RAI

This contribution comes just a few months before the final voting of the European Artificial Intelligence Regulation (RAI), initially proposed in April 2021 by the European Commission and since profoundly amended because of the advent of ChatGPT and generative AI. The RAI is a European regulation that aims for total harmonization within the EU's borders and whose extraterritorial scope is also provided.

This contribution (November 2023) is also within a few days of the adoption of the opinion of the European Data Protection Supervisor (2023b) on the proposals for two European directives on AI liability rules: 1) The proposal for a "*Liability for defective products Directive*" (European Data Protection Supervisor, 2022a); 2) The proposal of AI Liability Directive (European Data Protection Supervisor, 2022b). It also occurs after the adoption of the EDPS opinion on the RAI in light of recent legislative developments (following the numerous amendments passed by the European Parliament in June 2023).

It is no coincidence that the EDPS has recently become so active in the field of AI. It is precisely because the EDPS and national DPAs become key institutions in the European regulation of AI in general and the European Artificial Intelligence Committee in particular. This institutional aspect of AI regulation renews the interest in questioning the postulate of "data protection as a guarantor of trustworthy AI".

B. The RAI, as part of the European digital strategy

Nevertheless, it is also important to understand that the intensity of European regulatory activity since 2022 should be contextualized within the broader framework of the EU's evolving stance on AI. This stance has been gradually taking shape (1), culminating in the proposal of a regulation (2) and, most notably, the formulation of a comprehensive strategy (3).

(1) The incremental development of a normative framework for AI.

The European Union's approach to artificial intelligence (AI) commenced in April 2018 with the publication of a Commission Communication entitled "Artificial Intelligence for Europe". This document set forth the EU's objective to become a global leader in this field.

This process continued with the establishment in June 2018 of a high-level group of independent experts, charged with the responsibility of drafting the guidelines for trustworthy AI. These guidelines were subsequently published in April 2019 (European Commission [2019a] *Ethics guidelines for trustworthy AI*. High-Level Expert Group on Artificial Intelligence). The guidelines established seven fundamental principles of trustworthy AI, namely: 1) human action and control; 2) technical robustness and safety; 3) privacy and data governance; 4) transparency; 5) diversity, non-discrimination, and equity; 6) societal and environmental well-being; and 7) responsibility.

These principles were set out by the High-Level Group of Independent Experts on Artificial Intelligence (European Commission, [2019b]. *High-Level Expert Group on Artificial Intelligence*: *Mission and composition*) which was set up by the European Commission in June 2018 and published its findings in April 2019.

In February 2020, the European Commission (2020) presented a white paper[2] outlining its guidelines in this area, which were submitted for public consultation. The White Paper expressed the desire for a legal instrument that should be sufficiently flexible to accommodate technical progress while maintaining sufficient precision to guarantee the necessary legal certainty (European Commission, 2020, p. 19).

Finally, in April 2021, the initial proposal for a regulation to establish common rules concerning artificial intelligence was presented (European Commission, 2021).

(2) The content of the proposal

The recently introduced regulatory framework imposes obligations on suppliers and users in accordance with the level of risk associated with AI. The European Commission has adopted a risk-based approach, whereby the potential risks inherent in AI systems (AIS) are classified into four distinct categories: 1) unacceptable risk, 2) high risk, 3) limited risk, and 4) minimum risk.

Unacceptable risk

Unacceptable risk AIS are systems potential to pose a threat to human wellbeing. Consequently, a ban will be enforced on the following types of systems: (a) Cognitive-behavioral manipulation using subliminal techniques on specific vulnerable individuals or groups. This may include, for example, voice-activated toys that encourage dangerous behavior in children; (b) Social scoring by governments. This involves classifying people according to their behavior, socioeconomic status, and personal characteristics; (c) Real-time and remote biometric identification systems, such as those using facial recognition technology.

High risk

The proposal defines high risks in a restrictive manner, due to their adverse impact on the safety of individuals and their fundamental rights as enshrined in the EU Charter of Fundamental Rights. These will be divided into two categories. 1) The use of AI systems in products subject to EU product safety legislation. This encompasses toys, aviation, automobiles, medical devices, and elevators. 2) AI systems in eight particular domains are to be registered in an EU database. These include biometric identification and categorization of individuals, management and operation of critical infrastructures, education and vocational training, employment, worker management, and access to self-employment. Additionally, there is the matter of access to and enjoyment of essential private services and public services and benefits, law enforcement, migration, asylum, and border control management, as well as assistance with legal interpretation and enforcement.

[2] The Commission points out that consumer protection and personal data protection rules will continue to apply to artificial intelligence technologies, although this framework may need to be adjusted to take account of digital transformation and the use of AI. Some of the issues inherent in these technologies are generating new risks, which, according to the Commission, concern the infringement of fundamental rights, on the one hand, and the security and proper functioning of the liability regime, on the other (p. 12-15). To guard against this, a number of rules are to be adapted (p. 15-16), but above all new measures are to be introduced (p. 21-26). These new measures will only apply to "high-risk" artificial intelligence applications (p. 20-21), it being specified that high-risk is determined according to two cumulative criteria: on the one hand, according to the sector (e.g. "healthcare, transport, energy and certain parts of the public sector") and, on the other, according to the use itself. In fact, as the Commission points out, a high-risk sector can accommodate applications that carry no risk, such as a "hospital appointment scheduling system" (Crichton, 2020).

All high-risk AI systems will be subject to evaluation prior to their release onto the market, as well as throughout their entire lifecycle. Mandatory requirements have been proposed for all high-risk AI systems with the objective of promoting trust and ensuring a uniformly high level of protection for safety and fundamental rights. These requirements pertain to the quality of the data sets used for technical documentation, record-keeping, transparency, providing information to users, human control and robustness, accuracy and cybersecurity. The implementation of these requirements would enable national authorities to ascertain whether the AI system has been used in compliance with the law in the event of an infringement.

Limited risk

These AIS adhere to the requisite minimum transparency standards, thereby empowering users to make well-informed decisions. Following interaction with the applications, the user is at liberty to determine whether to continue utilizing them. This encompasses AI systems that generate or manipulate image, audio, or video content (e.g. deep fakes and false content rendered plausible by AI). Generative AI, exemplified by ChatGPT, is expected to adhere to the aforementioned transparency requirements, namely: to indicate that AI has generated content, to design the model in a manner that prevents it from generating illegal content, and to publish summaries of copyrighted data used for training purposes.

Minimum risks

This category encompasses other AI systems that could be developed and used, provided that compliance with current legislation is maintained. No further legal obligations would apply to them. The majority of AI systems currently in use in the EU fall into this category. Providers of these systems may choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct.

Next steps

On 14 June 2023, the European Parliament adopted its negotiating position on the RAI. In this iteration, parliamentarians incorporated new stipulations pertaining to generative AI, which imposed limitations on the use of biometric identification. Furthermore, the necessity for human supervision and assessment of high-risk AIS, which may pose "significant harm to health, safety, fundamental rights of persons or the environment," was introduced. The Parliament has also added a category system that could influence elections and the recommendation algorithms of social networks with over 45 million users in Europe.

(3) RAI in context

According to a Commission press release dated April 21, 2021, this intense AI work is part of the EU's strategy to make Europe "the global hub of trustworthy artificial intelligence". (European Commission, 2021). These words are more broadly in line with the political objective of building European technological sovereignty, a strategy that began factually in 2013 following the "Snowden" affair and legally in 2016/2018 with the implementation of the GDPR. Because of the attribution of international influence to this text due to its extraterritorial scope, the GDPR has become a global model for the protection of personal data.

This "*Brussels effect*," conceptualized by Anu Bradford, is the hallmark of European digital policies (Bradford, 2020). This strategy aims to establish global leadership in ethical digital technology, compensating for the potential delays European legislation could cause to European economic development.

European digital policy (Bertrand, 2023) has accelerated since the COVID-19 crisis, with the adoption of the Digital Services Act, the Digital Markets Act and the Data Governance Act (among many others).

The RAI was born in the geopolitical context of a European Union that no longer wanted to be "the colony of the digital world" (Morin-Desailly, 2013) but instead wanted to take its place in the global digital arena. The European legislator's tool to achieve this is its law, and its "lethal weapon" is the extraterritorial application of the various laws it adopts. As far as AI is concerned, the regulation would apply as soon as the AI is placed on the market or (a) put into service in the Union, regardless of where the supplier is established, (b) or used by a user present or established in the Union, (c) In addition, suppliers and users established outside the Union will be subject to the regulation if the results generated by the system are used in the Union.

This means that European authorities can prosecute foreign companies under EU digital law; to protect themselves, they would have to comply with EU law, which means that judges, lawyers and in-house counsel would have to be trained in EU digital law and adapt their compliance processes. From this perspective, it would not be an exaggeration to call this "normative colonialism". What legitimizes it in the eyes of the European institutions are precisely the universalist foundations of the project, through the guarantee of fundamental rights, democracy and now environmental protection.

While guaranteeing fundamental rights has never been the EU's primary objective, it's important to note that the gap is closing. In January 2022, the European Commission proposed to the European Parliament and the Council a Declaration on Digital Rights and Principles in the Union. Although it has no legal value (for the moment), it represents a political commitment; as an institutional agreement, it is known that it could sometimes have binding legal effects when interpreted by the Court of Justice of the EU (CJEU). In any case, it paves the way for this.

By adopting this declaration of fundamental digital rights, the European institutions are using a powerful symbol of the EU's "political vision" (Bertrand, 2023) for the digital age[3]. But in this "normative colonialism", are the risks to individual rights protected by law, or is their meaning reduced to ethics? Which brings us back to the original question.

Is personal data protection effective enough to limit AI risks to fundamental rights?

A. Accountability, a reduced protection

The answer to this question will be very reserved after a long period of research comparing the legislation of four EU countries from the 1970s to their adaptation to the GDPR, and the

[3] Reading this declaration, the European vision of the digital transition seems to be centered on citizens, solidarity and inclusion, and would include the importance of freedom of choice, participation in the digital public space, security, empowerment and sustainability. Politically, the Declaration reaffirms the need to strengthen democratic control over the digital society and economy. Legally, the Declaration has a modest but ambiguous objective. Traditionally, the Declaration does not affect the lawful limitations imposed on the exercise of legal rights in order to reconcile them with the exercise of other rights, nor the necessary and proportionate restrictions imposed in the public interest.

evolution of European legislation from the Council of Europe (Convention 108 of January 1981) to the EU GDPR (Koumpli, 2024).

The advent of the GDPR in Europe marked a paradigm shift in the protection of personal data. The new data protection model is based on the principle of "accountability". This means that from now on, private and public entities (data controllers) must ensure compliance with the rules throughout the data lifecycle and be able to demonstrate this on an ongoing basis. "The controller shall be responsible for compliance with paragraph 1 and shall be able to demonstrate compliance (accountability)" (Art. 5(2), GDPR).

In other words, and in the words of the French data protection authority accountability refers to the obligation for companies to implement internal mechanisms and procedures to demonstrate compliance with data protection rules (Commission Nationale Informatique & Libertés, 2018).

While the term tends to be translated as 'responsibility', accountability refers to being responsible (in the sense of civil and criminal law) and the duty to account for it. In other words, data protection is now achieved through the managerial and behavioral commitment of the actors involved, in other words by "empowering" them. The accountability corresponds, on the one hand, to the general obligation for companies to implement appropriate technical and organizational measures to ensure that data processing is carried out in compliance with the Regulation and, on the other hand, to the obligation to demonstrate this to the authorities at the time of a possible inspection, on pain of an administrative fine of up to 20 million euros (105,133,736 Brazilian real) or 4% of worldwide turnover, depending on the nature of the non-compliance.

Therefore, the protection authority only intervenes in a posteriori (with rare exceptions) if it has the material resources to do so and if an individual has brought it to its attention through a complaint. It's not just a question of changing the burden of proof, but also of fundamentally changing the way of proving it, moving from ex ante proof to proof throughout and ex post. Therefore, since 2018, this administrative requirement for managing the risks of RGPD breaches has replaced the prior intervention of the protection authority.

This normative choice is very different from the previous choice made by EU Member States under the model provided by Directive 95/46/EC. The previous regime was based on prior formalities to the national data protection authority. Under Directive 95/46/EC, data controllers were required to make a notification to the DPA before carrying out any processing operation – for ordinary processing operations – or to obtain an authorization from the DPA – for sensitive processing operations and the processing of sensitive data (data revealing racial or ethnic origin, sexual preferences, religious beliefs, trade union membership, etc.).

In terms of fundamental rights and freedoms, the receipt of the notification and the decision of the authority to authorized (or not) constituted the institutional and substantive guarantee that the protection corresponds to. This gave meaning to the fundamental right to data protection, which consisted in the right to request that an independent administrative authority verify and validate (or not) the processing (Koumpli, 2024). Consequently, the GDPR marks a transition from a preventive system, in which the proof of protection was based on a system of prior formalities, to a repressive system, in which the proof of protection depends on the data controllers.

The differences in the prior formalities in the Member States, the ubiquity of the processing of personal data, the limited resources of the independent authorities to deal with it and, above all, the obstacle to the EU's competitiveness represented by this preventive approach justified the abandonment of this preventive system. The new system created by the GDPR replaces the prior

intervention of a specialized independent data protection authority with the intervention of the data controller, before and throughout the processing.

The problem is that there are no longer any high-level guarantees, either in terms of independence or in terms of the competence of the person assessing compliance. On the contrary, in the eyes of the EU legislator, the person who has a personal interest in setting up processing operations on which the functioning and profitability of his company depend, i.e. the data controller, may be able and competent to assess and exercise self-control in order to protect personal data. From our perspective, this is an illusion. Either an illusion of the 'GDPR religion' that stakeholders are being asked to internalize (Frison-Roche, 2016)[4], or an illusion of the 'high level' of protection for individuals that the GDPR is aiming for.

For this reason, our thesis argues that the 'accountability' protection regime supports a risk of diminished protection and is likely to be contrary to the European Treaties, which guarantee that European Union law cannot undermine the common constitutional traditions of the Member States in terms of fundamental rights guarantees.

It is clear that the individual appointed as Data Protection Officer (DPO) by the data controller must demonstrate both independence and competence. The Court of Justice of the EU recently emphasized this point in its ruling in the Leistritz case [ECJ, Case c-534/20]. However, while these requirements for an employee of the data controller provide a certain level of assurance, they do not offer the same guarantees as the requirements for independence and competence in IT and freedoms as an independent administrative authority (Koumpli, 2024).

In concrete terms, the effectiveness of personal data protection, which is questioned in this article as AI's limit, is a co-regulation between the legislator and the data controllers, where the authorities only intervene as a specialized police force (Ochoa, 2014). In this "risk management protection model," no actions are prohibited *a priori*; all potential courses of action are permitted. It is necessary to understand how to "tick the right boxes" in the GDPR, that is, how to utilize the "European personal data protection instruction manual". This five-point manual, as outlined by Haas (2022), covers the following key areas: 1) Documenting and implementing procedures to ensure respect for people's rights; 2) Documenting and implementing procedures to ensure lawful data processing; 3) Implementing compliance measures (register, DPO designation, PIA, certifications, code of conduct, etc.); 4) Documenting and implementing processing security procedures; 5) Employee training and awareness.

In the event of an inspection, these documents will be presented to officials from the data protection authority.

The negotiation of penalties as a further argument for reducing effectiveness

Furthermore, the possibility of negotiating penalties raises questions about the effectiveness of the GDPR. Indeed, the GDPR provides that data protection authorities may consider the measures taken by the data controller in breach of the rules when determining the appropriate administrative fine (Art. 83 2(d), GDPR). Furthermore, if the relevant authority issues a formal notice to an organization, the notice may be closed, and the company may ultimately not be sanctioned if it can demonstrate that it has corrected its compliance. This suggests that despite a breach of European data protection standards, a company or administration may ultimately not be sanctioned or may be subject to a relatively small fine.

[4] "The European legislator is integrating local public regulation on a global scale in supranational companies, which are becoming agents of effectiveness with the aim of promoting data protection measures" (Frison-Roche, 2016).

In practical terms, this gives rise to paradoxical results with regard to the perception of the GDPR as a highly protective measure, given the significant penalties that may be imposed. It could be argued that the legislation is only truly protective in the case of large organizations and instances of significant non-compliance. It is therefore encouraging to observe that, in the context of AI, not only has the prohibition of specific AIS deemed to be unacceptably risky been reintroduced[5], but, most notably, the accountability of the relevant parties is subject to the oversight of a third-party body. Consequently, the responsibility for risk assessment does not fall upon developers, suppliers, or users of high-risk AIS.

In light of the aforementioned, it can be argued that the introduction of a graduated approach to risk and the involvement of third-party competent authorities in the RIA are not a direct consequence of the GDPR. Rather, they represent an attempt by the EU legislator to address the potential limitations of the RGPD.

B. The effectiveness of the RGPD risk-based approach – the limitations of PIA methodology on sensitive data processing

From an RGPD perspective, the most evident data protection failure is in the area of sensitive processing, including, for example, algorithmic processing. This is an illustrative example of the limitations of the GDPR in addressing the risks associated with AI. It is likely that this is why the RAI goes beyond the scope of the GDPR.

In particular, the requirement for authorization from the DPA for processing of sensitive data has been replaced with a Privacy Impact Assessment (PIA) in accordance with Art. 35 of the GDPR. The PIA is conducted by the data controller and, in practice, by their DPO.

The Art. 36 RGPD stipulates that the controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Art. 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

To date, the CNIL in France has not been contacted by a DPO or a controller to announce the commencement of high-risk processing. This is a logical consequence of the principle that one should not create problems for oneself. What is particularly noteworthy is that the PIA methodology in Europe has resulted in a "proceduralization" of compliance that distances the assessor (in this case, the controller) from the substantive issues of fundamental rights violations.

While the PIA aims to determine whether a "processing operation is likely to give rise to a high risk for the rights and freedoms of individuals", the methodologies proposed, whether by the European Data Protection Board (European Data Protection Board, WP 248 rev. 01, 2017) or by the CNIL, do not specify which rights and freedoms might be referred to; the most striking example is the CNIL's PIA (Commission Nationale Informatique & Libertés, 2018, p. 3), which states in its introduction that "The term 'privacy' is used as shorthand to evoke all fundamental rights and

[5] Indeed, the AI Act proposes the prohibition of specific AI systems deemed unacceptable, including those that engage in cognitive manipulation of vulnerable users, real-time biometric surveillance, and other ethically controversial applications. This prohibition applies solely to the most dangerous AI applications and does not extend to "high-risk" systems in general; The responsibility for risk assessment of high-risk AI systems cannot be attributed solely to a third party. Developers, suppliers and users bear a significant portion of the responsibility. They are obliged to implement and maintain a comprehensive assessment of the compliance and risks associated with their AI systems prior to and throughout their use. Third-party bodies (notified bodies) primarily serve to verify the compliance of high-risk AI systems. These bodies are involved in the supervision of certain aspects of high-risk AI systems, in particular by carrying out conformity assessments for certain applications. However, this does not signify that total responsibility is transferred to these bodies; it is an additional control measure, not a complete transfer of responsibility. Thus, responsibility for risk assessment for high-risk systems is shared between developers, suppliers, users and, in some cases, notified bodies. The role of third parties is to ensure high levels of safety and compliance, but it does not replace the responsibility of the parties directly involved.

freedoms (in particular, those evoked in the [RGPD], by Arts. 7 and 8 of the [Charter-EU] and Art. 1 of the [Law-I&L]: "privacy, human identity, human rights, and individual or public freedoms".

A few lines further on, without the document identifying the specific rights and freedoms that are being threatened, it is clear that the proportionality control provided for by the GDPR must be applied. However, the principle of proportionality can be a legitimizing tool than a protective one. This is further reinforced when the entity responsible for controlling proportionality is also the entity applying it.

Last but not least, the methodologies do not define what is meant by 'risk' or when this risk becomes significant. This is due to the fact that the "previous stage" has been bypassed, and it has not been specified which of the fundamental rights may be affected by the processing in question.

This issue gives rise to another: when reading these methodologies and in the practice experienced, we see a shift from risks to the fundamental rights of individuals to risks to the information systems of data controllers and therefore cybersecurity risks. This is particularly evident when we compare the methodologies of the EDPB, the CNIL and the ISO 31000 standard to which the EDPB refers, despite the latter having the wrong objective.

It should be noted that cybersecurity standards are designed to protect the company and the data controller and may also protect the data indirectly. In contrast, the RGPD and national data protection laws are intended to protect individual freedoms.

Consequently, the risk to fundamental rights in the PIA is commensurate with issues such as "illegitimate access to data, unwanted modification of data, disappearance of data" (Commission Nationale Informatique & Libertés, 2018, p. 9), which must then be addressed through the following actions: 1) Determine the potential impact on the privacy of the individuals concerned, should it arise, 2) Estimate the severity of the situation, particularly in terms of the potential detrimental impacts and, where appropriate, the measures that could be taken to modify them, 3)Identify the threats to data media that could lead to this feared event and the sources of risk that could cause it, 4) Estimate its likelihood, particularly regarding the vulnerabilities of data carriers, the ability of risk sources to exploit them, and the measures likely to modify them.

The majority of DPOs conclude that the risks are acceptable, or alternatively, that additional safety measures are required to mitigate any residual risks. In the event that this methodology was to be applied to high-risk AIS by notified bodies or notifying authorities, it would be regarded as the "triumph of self-blindness".

C. Is the protection of personal data a matrix for the protection of all other fundamental rights?

One positive aspect of the AI adoption process is the growing awareness that, in the institutional discourse of AI, personal data protection is often seen as a separate issue from privacy. This is an attempt to address the challenges of digital technology in exercising various rights and freedoms. It is asserted, for instance, that "Most notably, AI systems may jeopardize fundamental rights such as the right to non-discrimination, freedom of expression, human dignity, personal data protection, and privacy" (High-Level Expert Group, 2019).

Nevertheless, the question remains: Does the GDPR protect the individual person or the human being? In many instances, the individual is not the fundamental starting point of algorithmic processing, but rather a means or an end result of such processing.

Indeed, it is taught in Europe that the GDPR is a regulation that applies to personal data, defined as "any information relating to an identified or identifiable natural person". This kind of development, allowing the GDPR to be used for non-personal data is not automatic.

Such an extension could be envisaged if the fundamental right set out in Art. 8 CDFUE were to be extended to cover not the identified or identifiable person but the human being, the citizen, and the fundamental freedoms or freedoms. The determination of which of these is applicable in any given case will depend on a rigorous case-by-case examination by the judge.

D. European data protection is itself human-centered?

This returns us to the fundamental premise that underlies the assertion that the advancement of AI technologies that adhere to the European framework for the protection of personal data is a prerequisite for the realization of human-centric AI.

In order for this to be true, it is imperative that European personal data protection is regarded as human-centered legal protection. It would be erroneous to assume that this is as straightforward as it may appear.

Certainly, Art. 16 TFEU represents one of two foundational pillars upon which the future regulation is based. It is invoked in order to fulfil the role of "refocusing the RAI on the human", given that the Commission's initial proposal had as its only legal basis the regulation's Art. 114 TFEU, which provides for the adoption of measures intended to ensure the establishment and functioning of the internal market[6].

Nevertheless, Art. 16 TFEU, which gives the EU a monopoly on data protection competence without Member States being able to defend a higher constitutional protection, such as Art. 8 of the Charter of Fundamental Rights of the European Union, is not as anthropocentric as one might think.

The fundamental right to personal data protection within the EU legal order is bifunctional (Koumpli, 2024). The objective is to guarantee the free circulation of personal data as a fundamental condition for achieving European integration, while simultaneously protecting the fundamental rights of the data subjects. It is argued that this represents a "fundamentalisation" of a protection that may be inferior to that guaranteed by certain Member States prior to the GDPR (Koumpli, 2024).

In any case, the GDPR's bifunctional nature gives rise to paradoxical situations that are in no way protective of AI drifts; the PIA (mentioned above) is one of the most apparent manifestations of its weakness. In this model, personal data protection would be more akin to a user manual than a restraint. Indeed, a study by the European Parliament's research office powerfully illustrates the RGPD's capacity to adapt to any environment like a chameleon: "The GDPR prescriptions are frequently vague and open-ended. The GDPR permits the development of AI and big data applications that successfully reconcile data protection and other social and economic interests, but it provides limited guidance on how to achieve this goal" (European Parliamentary Research Service, 2020).

In conclusion, the GDPR provision that exemplifies the ambiguity and ineffectiveness of this legislation with regard to AIS is to be found within the GDPR itself: "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data" (Art. 1 (3), GDPR).

[6] The Art. 16 TFEU appears in the explanatory memorandum only as a basis for "restrictions on the use of AI systems for remote biometric identification 'in real time' in publicly accessible areas for law enforcement purposes", in other words (cons. 2) for which only it seems appropriate for the European Commission to consult the European Data Protection Committee.

In light of this clause, it is questionable whether the European Personal Data Protection and European Data Protection Authorities will facilitate the human-centered development of AI in a manner that is tenable. Ultimately, this clause either renders the GDPR non-compliant with the Lisbon Treaty or prevents Art. 16 TFUE from representing the human-centered legal basis of the European regulation on artificial intelligence.

References

Bertrand, B. *La politique européenne du numérique*. Paris: Bruylant, 2023.

Bradford, A. *The Brussels Effect*: How the European Union Rules the World. Oxford: Oxford University Press, 2020.

Commission Nationale Informatique & Libertés. *Analyse d'impact relative à la protection des données*: Privacy Impact Assessment (PIA): la Méthode. [*s. l.*]: CNIL, 2018. Available from: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-fr-methode.pdf. Cited: 6 Oct 2024.

Crichton, C. Publication par la Commission de son Livre blanc sur l'intelligence artificielle. *Dalloz Actualités*, 28 Feb 2020. Available from: https://www.dalloz-actualite.fr/flash/publication-par-commission-de-son-livre-blanc-sur-l-intelligence-artificielle#.YiDhay3pNQI. Cited: 6 October 2024.

European Commission. *Artificial intelligence*: Commission takes forward its work on ethics guidelines Brussels - Press Release. Brussels: European Commission, 2019a. Available from: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_19_1893/IP_19_1893_EN.pdf. Cited: 17 Dec 2024.

European Commission. *Ethics Guidelines for Trustworthy AI (AI HLEG)*. Brussels: European Commission, 2019b. Available from: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Cited: 17 Dec 2024.

European Commission. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence legislation) and amending certain union legislative acts (com/2021/206 final)*. Brussels: European Commission, 2021.

European Commission. *White Paper Artificial Intelligence*: a European approach focused on excellence and trust. COM (2020) 65 final. Brussels: European Commission, 2020. Available from: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf. Cited: 6 Oct 2024.

European Data Protection Board. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Brussels: European Data Protection Board, 2017. Available from: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711. Cited: 29 Oct. 2024.

European Data Protection Supervisor. *EDPS at work*: data protection and artificial intelligence (AI). Brussels: EDPS, 2023a. Available from: https://www.edps.europa.eu/system/files/2023-10/2023-10-24-edps-at-work-data-protection-and-artificial-intelligence_en.pdf. Cited: 6 October 2024.

European Data Protection Supervisor. *Opinion 42/2023 on the Proposals for two Directives on AI liability rules*. Brussels: EDPS, 2023b. Available from: https://www.edps.europa.eu/system/files/2023-10/23-10-11_opinion_ai_liability_rules.pdf. Cited: 6 October 2024.

European Data Protection Supervisor. *Proposal for a Directive of the European Parliament and of the Council on liability for defective products*. Brussels: EDPS, 2022a. Available from: https://single-market-economy.ec.europa.eu/system/files/2022-09/COM_2022_495_1_EN_ACT_part1_v6.pdf. Cited: 6 Oct 2024.

European Data Protection Supervisor. *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)*. Brussels: EDPS, 2022b. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496. Cited: 6 Oct 2024.

European Parliamentary Research Service. *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. Study. Brussels: EPRS, 2020. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf. Cited: 6 Oct 2024.

Frison-Roche, M.-A. Le Droit de la compliance. *Recueil Dalloz*, n. 32, p. 1871-1874, 2016. Available from: https://mafr.fr/en/article/le-droit-de-la-compliance-2/. Cited: 6 Oct 2024.

Haas, G. *Guide juridique du RGPD*. La réglementation sur la protection des données personnelles. 3. ed. ENI, 2022. Available from: https://www.editions-eni.fr/livre/guide-juridique-du-rgpd-3e-edition-la-reglementation-sur-la-protection-des-donnees-personnelles-9782409037344?gad_source=1&gclid=Cj0KCQiAvP-6BhDyARIsAJ3uv7bNea1ZaPxgNS8pUP5dkK6dHUzpfUYemEWrYBEXCNC-53YhzGcv_ToaAsaAEALw_wcB. Cited: 17 Dec. 2024.

High-Level Group. *Ethics guidelines for trustworthy AI*. Brussels: European Commission, 2019. Available from: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Cited: 17 Dec 2024.

Koumpli, C. *Les données personnelles sensibles*. Contribution à l'évolution du droit fondamental à la protection des données personnelles: étude comparée: Union Européenne, Allemagne, France, Grèce, Royaume-Un.i Thèse [Doctorat en Droit Public] – Université Paris, 2024.

Morin-Desailly, C. *L'Union européenne, colonie du monde numérique?*. Paris: Sénat, 2013. (Rapport d´Information, nº 443, 2012-2013). Available from: https://www.senat.fr/rap/r12-443/r12-443_mono.html. Cited: 17 Dec 2024.

Ochoa, N. *Le droit des données personnelles, une police administrative spéciale*. Thèse [de Doctorat en Droit Public] – Université Paris, 2014.