Pérez-Llorca

TECHLAW

Artificial intelligence

JANUARY 2024

A challenge for companies and for regulators

Raúl Rubio

Partner, Intellectual Property and Technology

rrubio@perezllorca.com
+34 91 353 45 59

María Chávarri

Lawyer, Intellectual Property and Technology

mchavarri@perezllorca.com
+34 91 423 67 28

_ RAÚL RUBIO AND MARÍA CHÁVARRI

The interaction of artificial intelligence with the protection of personal data

Artificial intelligence ("**AI**") processes information to learn, adapt and make predictions or recommendations. The algorithms used in this area, especially in machine learning, require huge amounts of data for their training.

Although not all AI tools need to use personal data, in many other cases the information used is directly or indirectly connected to the processing of the data of natural persons. The breadth with which the concept of personal data[1] is defined in the European Union, through the General Data Protection Regulation ("**GDPR**") and the way in which this definition is interpreted by regulators, makes it necessary to consider the risk of processing personal data even in more industrial or unconnected uses of AI, such as the Internet of Things (IoT[2]).

Even when processing **anonymised data**, the strict regulatory criteria require us to question to what extent such anonymisation can be considered sufficient to escape the scope of application of data protection regulations.

> ***Even if data is anonymised, the stringency of existing regulations makes us reflect on the effectiveness of this anonymisation to consider whether it is actually excluded from the scope of data protection laws.***

At the same time, the **irreversibility** of anonymisation may pose challenges in assessing the quality of inferences from certain AI tools. In other words, the unlimited collection of personal data can make it difficult to fully explain the proper functioning of an AI system. The more personalised and comprehensive the data, the more effective the patterns and insights that AI can generate.

> ***Herein lies the first sticking point: the wholesale collection and use of personal data clashes with some of the cardinal principles of data protection***

Therefore, it is important to strike a balance between minimising the processing of personal data and the need to collect sufficient data to ensure the explainability[3] and transparency of AI systems.

The evaluation of the legitimate basis for data processing, compliance with the duty to disclose the characteristics of data processing, the limitation of the purpose, privacy by default and by design, and security are some of the other

1 Under Article 4.1 of the GDPR, personal data is "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more elements of that person's physical, physiological, genetic, mental, economic, cultural or social identity".

2 A typical example of the use of AI in the Internet of Things (IoT) - which ostensibly does not process personal data, but in practice does - is traffic and transport monitoring. AI systems in IoT can collect data on users' location, movement and travel patterns, which, while initially appearing not to be linked to personal data, can in fact reveal personal information if analysed in detail. For example, through the collection and analysis of traffic and mobility data, individual behaviour patterns and preferences can be gleaned, which implies the processing of personal data.

3 The "explainability" of AI systems refers to the ability to understand and explain how and why a system makes decisions or performs specific actions. This concept is especially important in the context of complex algorithms, such as those based on deep learning, where decisions may be made by models that are inherently difficult to interpret.

challenges that developers, marketers and users of AI must face when using personal data.

Taking into account the interplay between AI and data protection, this briefing will attempt to briefly and concisely analyse: **(i)** the assessment that European data protection regulators, and, in particular, the European Data Protection Board ("**EDPB**"), have made regarding the future AI Act (the "**AI Act**"); **(ii)** the positioning of these regulators with respect to AI and the impact of the current data protection regulations; and **(iii)** some of the correlations of the future AI Act with personal data protection regulations.

1. The assessment of the future AI Act by data regulators

Through Joint Opinion 5/2021[4], in June 2021, the EDPB - in which the national data protection authorities of all Member States are represented - and the European Data Protection Supervisor ("**EDPS**"), announced their support for the legislature's initiative to address the use of AI in the EU. We will not delve into the details of this document, as it is based on an assessment made well before the recent changes to the approach of the future AI Act, which emerged from the latest negotiations between the European co-legislators. However, we will highlight some aspects that may help us to glimpse what may in future emerge as the tensions between the two regulated areas, that of AI and that of personal data, which from now on will have to coexist:

- The EDPB and the EDPS emphasise that **compliance with data protection requirements must be independently monitored** under Article 16 of the Treaty on the Functioning of the European Union[5].
- Joint Opinion 5/2021 implicitly objects to the possibility that sandboxes can allow exceptions to data compliance and points out that compliance with the GDPR and the Data Protection Regulation for the institutions, bodies, offices and agencies of the European Union should be a precondition for entering the **European market** as a CE-marked product.

European data supervisors have claimed the role of Data Protection Authorities (DPA) in the development and establishment of harmonised rules and common specifications, and it is suggested that DPAs should be designated as national supervisory authorities for AI.

- The EDPB and the EDPS have called for a general prohibition on the use of AI for automated recognition of human traits in publicly accessible spaces. This includes facial recognition, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context.
- The predominant role of the Commission in the European Committee on Artificial Intelligence has been questioned - as the European AI body must be independent of any political influence - and more autonomy for the body is called for, as well as guarantees that it can act on its own initiative.
- European data supervisors have claimed the role of Data Protection Authorities ("**DPA**") in the development and establishment of harmonised rules and common specifications, suggesting that DPAs should be designated as national supervisory authorities for AI.
- For the EDPB and the EDPS, the conflict between the autonomy of decision-making by machines underlying the very concept of AI and the rights to privacy and the protection of personal data is a major concern.
- Joint Opinion 5/2021 highlights the importance of human oversight, especially in AI systems that process personal data, which is crucial to ensure compliance with the right not to be subject to a decision based solely on automated processing.
- The risk-based approach, which applies to all AI systems, is welcomed. However, the regulators consider that the option of providing an exhaustive list of high-risk AI systems could cause a black-and-white effect "with little ability to capture high-risk situations", undermining the general approach of the proposed Act, which is based on risk factors[6].
- The use of AI systems for the remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into privacy and the EDPB and the EDPS consider that a stricter approach is needed. The use of such systems in airports and stations, for example, would involve processing the data of many people to identify only a few, which raises issues of proportionality, transparency and legality under EU law. However, the question of how to adequately inform people and how to guarantee their rights, which affects privacy and freedoms in public spaces, has not yet been resolved. They also understand that such systems have irreversible consequences on people's expectations of anonymity in public spaces.

4 EDPB-EDPS: Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules in the field of artificial intelligence (Artificial Intelligence Act), available at the following link: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

5 Article 16 establishes that: "1. Everyone has the right to the protection of personal data concerning them; 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to control by independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

6 The EDPB and the EDPS do not appear to take into account the legal uncertainty that could be caused by a lack of clarity as to what is considered a high-risk system.

– The use of AI to infer the emotions of natural persons is highly undesirable and should be prohibited, except in certain specific use cases, such as for health or research purposes, with the corresponding safeguards, limits and conditions provided by data protection laws.

For their part, several national data protection authorities have formally endorsed the EDPB and EDPS[7] opinion or, as in the case of Italy, have issued their own formal opinions with very similar approaches[8].

2. Interpretation of the GDPR in the context of AI

The EDPB, for the time being, has not published any formal opinion interpreting the GDPR in the specific field of AI, unlike regulators in different Member States, which have done so.

National authorities in Italy, France and, above all, Spain have been the most active in establishing a softlaw regulatory framework on data protection and artificial intelligence.

The length of this document does not allow us to dwell on the actions of all of these authorities, although we will highlight below some of the activities carried out in this area by France, Italy, Germany and Spain.

2.1. France

In France, in January 2023, the Commission Nationale de l'Informatique et des Libertés ("**CNIL**") created a specific AI department to reinforce its expertise in these systems and its understanding of privacy risks, followed shortly after by an Action Plan[9]. The regulator has identified the following areas as priority areas for the Artificial Intelligence Service and the CNIL's Digital Innovation Lab:

» The fairness and transparency of the data processing underlying the operation of these tools.

» The protection of publicly available data on the web against the use of scraping for the design of tools.

» The protection of data transmitted by users when using these tools, from its collection (through an interface) to its possible reuse and processing through machine learning algorithms.

» The consequences for individuals' rights over their data, both regarding data collected for model learning and data provided by such systems, such as content created in the case of generative AI.

» The protection against bias and discrimination that may occur.

» The security challenges of these tools.

The CNIL has also launched its own sandbox to support three projects using AI for the benefit of public services and an enhanced support programme for three innovative medium-sized companies (scale-ups), including one that specialises in the provision of AI datasets and models.

Finally, the French regulator has published informative guides[10] on the creation of AI-enabled databases, which were subject to public consultation until 15 December 2023[11]. The guides aim to support actors in the AI ecosystem in their efforts to comply with personal data protection legislation and provide concrete answers, illustrated with examples, to legal and technical questions related to the application of the GDPR to AI. In particular, they answer questions relating to the application of the principles of purpose, minimisation and the retention period of databases, as well as the rules applicable to scientific research and the reuse of databases.

2.2. Germany

The federal data protection supervisor in Germany, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit ("**BfDi**"), launched a public consultation process from 30 September 2021 to 17 December 2021, the conclusions of which were presented in a report in 2022[12]. More recently, on 24 May 2023, the BfDi published the Statement of the Federal Commissioner for Data Protection and Freedom of Information on the public hearing of the German Bundestag's Committee on Digital Affairs on "Generative Artificial Intelligence[13]".

7 Intelligence artificielle: l'avis de la CNIL et de ses homologues sur le futur règlement européen, available at: https://www.cnil.fr/fr/intelligence-artificielle-lavis-de-la-cnil-et-de-ses-homologues-sur-le-futur-reglement-europeen (last accessed on: 17/01/2024)

8 Memoria del Garante per la protezione dei dati personali - COM 2021(206) Proposta di regolamento (UE) sull'intelligenza artificiale, available at: https://gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751565 (last accessed on: 17/01/2024)

9 Artificial intelligence: the action plan of the CNIL, available at https://www.cnil.fr/en/artificial-intelligence-action-plan-cnil (last accessed on: 17/01/2024)

10 The guides are available at the following link: https://www.cnil.fr/fr/les-fiches-pratiques-ia (last accessed on: 17/01/2024).

11 Available at: https://www.cnil.fr/fr/intelligence-artificielle-la-cnil-ouvre-une-consultation-sur-la-constitution-de-bases-de-donnees

12 Bericht über das öffentliche Konsultationsverfahren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema: Einsatz von Künstlicher Intelligenz im Bereich der Strafverfolgung und der Gefahrenabwehr, available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Konsultationsbericht.pdf?__blob=publicationFile&v=5 (last accessed on: 17/01/2024)

13 Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur öffentlichen Anhörung des Ausschuss für Digitales des Deutschen Bundestages am Mittwoch, 24. Mai 2023, 14:30 – 16:30 Uhr, zum Thema „Generative Künstliche Intelligenz", available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Generative-K%C3%BCnstliche-Intelligenz.pdf?__blob=publicationFile&v=2 (last accessed on: 17/01/2024)

2.3.Italy

In Italy, the actions of its regulator, Garante per la protezione dei dati personali ("**Garante**"), have so far focused on the health sector, through the publication of a Decalogue for the implementation of national health services through artificial intelligence systems[14]. On an informative level, the Garante has published a series of videos to analyse AI and its relationship with data protection[15].

2.4.Spain

In the case of **Spain**, the Spanish Data Protection Agency ("**AEPD**") has been a pioneer in terms of its reaction to AI. By February 2020, it had already published a Guide for adapting products and services using artificial intelligence to the GDPR[16]. It sets out the conditions that these technologies must meet in order to guarantee and demonstrate that the processing that has been carried out complies with the GDPR, setting out the AEPD's requirements with a view to guaranteeing the quality and privacy of these systems. It also notes that compliance with the GDPR requires AI models to have a certain level of maturity so that the adequacy of processing and the existence of measures to manage its risks can be objectively determined.

a. The processing of personal data in different phases of AI systems

The guide highlights the possibility that personal data may be processed at all stages of AI systems' lifecycles. These include:

a) **Training**: Training the AI system with personal data constitutes processing in and of itself.

b) **Validation**: Processing is deemed to exist if data that corresponds to the actual current situation of processing is used to experimentally assess the effectiveness and quality of the model. Validation is performed in determining the ability of the AI system to make accurate and useful predictions in real-world situations.

c) **Deployment**: Data processing occurs when the AI system includes personal data or there is a way to obtain personal data.

d) **Inference**: Personal data are processed when data belonging to the data subject are used in the AI system to obtain a result, when data belonging to third parties are used to obtain a result, or when data or inferences belonging to the data subject are stored.

e) **Decision-making**: Processing of personal data will be triggered by a mere decision about a data subject made in the AI system.

f) **Evolution**: Processing of personal data will occur when personal data is used to refine the AI system model[17].

g) **Removal**: Service removal can occur for two reasons; either the AI component is withdrawn as it is obsolete in all processing in which it is implemented, or a user of the AI system decides not to use the AI component.

The AEPD considers that any AI technical solution that processes personal data must incorporate certain quality control parameters that must be verified in order to comply with the basic requirements of accountability, transparency and legality. As examples of such control parameters, the AEPD cites the following:

- Precision, accuracy or error rates required by the processing.
- Data input quality requirements for the AI component.
- Precision, accuracy or effective error rates of the AI-based solution depending on the appropriate metrics to measure the eligibility of the AI-based solution.
- Convergence of the model when dealing with training and adaptive solutions.
- Consistency in the results of the inference process.
- Algorithm predictability.
- Any other assessment parameters of the AI component.

The AEPD considers that in order to comply with the fundamental requirements of accountability, transparency and legality, any AI system handling personal data

14 Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale, available at: https://www.garanteprivacy.it/documents/10160/0/Decalogo+per+la+realizzazione+di+servizi+sanitari+nazionali+attraverso+sistemi+di+Intelligenza+Artificiale.pdf/a5c4a24d-4823-e014-93bf-1543f1331670?version=2.0 (last accessed on: 17/01/2024)

15 Available at: https://www.youtube.com/GARAntedatipersonaliGP (last accessed on: 17/01/2024)

16 GDPR compliance of processings that embed Artificial Intelligence. An introduction, available at: https://www.aepd.es/documento/adecuacion-rgpd-ia-en.pdf

17 If we are dealing with evolution carried out in the component acquired by the data subject themselves, in isolation and autonomously, the domestic exception would apply unless the personal data is sent to third parties since this would be a communication of data.

needs to integrate and demonstrate certain quality control standards.

In addition, the AEPD has drafted a document which provides for specific controls to audit personal data processing that uses AI to analyse and guarantee data protection[18]. This guide focuses on the adequacy of processing according to data protection principles and provides methodological notes for these audits.

b. The role of the data controller in AI systems

The Spanish regulator also stresses the need to clearly distinguish responsibilities with regard to data processing. In AI systems in which personal data is processed, the data controller will be the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Throughout the life cycle of an AI system, the role of a data controller may be held by different figures:

i) **Development, training and validation phases:** The organisation that defines the purposes of the AI system components and decides on the data to be used in the training phase. If the developer is a third party and makes decisions about the personal data used to train AI components for its own purposes, it will also be considered the data controller.

ii) **Deployment:** If the AI solution is a component marketed to another organisation and personal data processing is carried out in the context of the AI solution, both the marketing entity and the entity that purchases the solution are data controllers and communication of personal data takes place between them[19].

iii) **Inference/profiling**: The organisation that decides to process data subjects' data through the AI solution for its own purposes[20].

iv) **Decision-making**: The organisation that carries out automated decision-making about data subjects for its own purposes.

v) **Evolution or retraining**: The organisation that decides to process data subjects' data through the AI systems[21]. The organisation that determines the evolution of an AI system component on the basis of the data (either provided directly by the data subjects or by the entity providing the service) is considered the data controller.

The decision to employ an AI-based technical solution within personal data processing activities rests with the controller, who will define the means and purposes of the processing of personal data. The controller will have to decide between the different technological solutions that they consider the most appropriate.

Under no circumstances may the controller evade their responsibility by transferring it to the AI system itself.

c. Obligations to be fulfilled by the data controller in an AI solution

vi) Compliance with the guiding principles of data protection

It should be noted that, in AI systems, the controller must comply with each and every one of the guiding principles of data protection[22]. However, the principle of accuracy is particularly important in the context of AI systems[23] as inaccurate data may compromise not only the processing of personal data but also the functioning of the AI system itself. The principle of accuracy must be present throughout the processing (both in input data, intermediate data and output data), but it is essential in input data, as it can lead to biases that are not part of the AI system itself[24].

vii) The GDPR's duty to inform data subjects and the AI Act's transparency obligation

The GDPR establishes that each controller must provide data subjects with the information set out in Articles 13 and 14 of the GDPR in order to comply with the duty of information. If the data subject is subject to automated decision-making or profiling[25], **the controller must, in addition, provide information on the logic applied and**

18 Audit Requirements for Personal Data Processing Activities involving AI, available at: https://www.aepd.es/documento/requisitos-auditorias-tratamientos-incluyan-ia-en.pdf, (date last accessed: 17/01/2024).

19 This does not apply in the event that the solution is marketed to natural persons, in which case only the marketing entity will have the role of data controller.

20 This does not apply if it is carried out by a natural person on their own personal data or the data of the persons around them for an exclusively personal activity.

21 In the event that it outsources the personal data of AI system users to a third party, the organisation is responsible for the communication of data, provided that there is no controller-processor relationship.

22 Set out in Article 5 of the GDPR.

23 Set out in Article 5.1.d of the GDPR.

24 This is elaborated on in Recital 71 of the GDPR.

25 Those referred to in Article 22 of the GDPR.

on the significance and expected consequences of the processing[26]. Accordingly, **the controller should provide information enabling the data subject to understand the processing behaviour that is occurring with regard to their personal data** in AI systems involving automated decision-making and/or profiling[27].

3. Correlations of the AI Act with the GDPR

Although an exhaustive analysis of the interaction between the AI Act and the GDPR is not currently possible - given that the final text of the AI Act has not been published at the time of writing - we will focus on what has been established with respect to transparency obligations, the exercise of rights and risk management. We will address compliance requirements from the perspectives of data and AI, highlighting the differentiated approaches presented below.

a) Transparency obligations

Therefore, it would not be sufficient to comply with the principle of transparency proposed in the AI Act in order to comply with the duty of information established in the GDPR for the controller.

b) Exercise of data subjects' rights in AI systems

The data controller must comply with the duty to attend to the rights of data subjects established in the GDPR (access, rectification, erasure, restriction, portability, objection and the right not to be subject to automated decision-making)[28], and must establish all the necessary mechanisms and procedures to be able to deal with the requests to exercise rights that they receive. Such mechanisms should be appropriate to the scale of the processing being carried out as a result of the use of AI systems.

Of particular importance in AI systems are the rights of data subjects that may be processed in connection with profiling and/or automated decision-making.

In AI systems, however, the **right to erasure** also plays a key role, which, for example, involves compliance with the principle of data minimisation when the training stage of AI systems has ended. It is also interesting to note the controller's obligation to comply with the **right to rectification** of the data generated by the profiles produced by the AI solution. Likewise, in the event of inaccurate training data in the AI model that may contain inaccurate data of persons who can be re-identified, and may associate erroneous information with such persons, it is necessary to comply with the **right to rectification**.

The transparency principles in the AI Act and in the GDPR have different meanings, establish different obligations, (sometimes) bind different subjects, refer to different types of information and (sometimes) address different recipients.

Furthermore, where processing is carried out by automated means, the GDPR also establishes the right of the data subject to receive the personal data they have provided to a controller in a structured, commonly used and machine-readable form and to transmit it to another controller where the legitimate interest is based on consent or on contractual necessity. A controller that includes AI systems should assess whether the specific processing operations it carries out are subject to the obligation to provide data portability.

c) Risk management and impact assessments

The controller should carry out a risk analysis of the processing, taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Based on this analysis, the controller must implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is compliant with the GDPR[29], and must review and update the measures as necessary. In the case of AI systems, for the purpose of determining the level of risk of a processing operation, the controller must take into account the following:

i) The risks arising from the processing itself, the most common of which is that arising from bias in decision-making systems about individuals or discrimination against them.

ii) The risks arising from processing in relation to the social context and the collateral effects that may result from it.

AI systems, by their very nature, may entail a high risk to the rights and freedoms of data subjects and therefore, in most cases, a data protection impact assessment ("**DPIA**")[30] should be carried out by the controller, in particular, when profiling based on automated processing is carried out. The controller must therefore identify all decisions taken at the various

26 Article 13.2.f of the GDPR.

27 For example, the controller could report on the following extremes: the quality of the training data and the type of patterns used; the data used for decision making; the relative importance of the data in decision making; or the profiling used and its implications, etc.

28 Articles 15 et seq. of the GDPR.

29 Under Article 24 of the GDPR.

30 Provided that the conditions set out in Article 35 of the GDPR are met.

Transparency obligation

	Under the GDPR	Under the AI Act
Transparency obligation	Inform about the processing of personal data and the impact that the processing has on rights and freedoms.	Inform with adequate traceability and explainability, making users aware that they are communicating or interacting with an AI system, duly informing users about the capabilities and limitations of such an AI system and informing affected persons of their rights.
Active subject	The data controller	AI system designer; AI system developer; AI system provider; user implementing the AI system
Passive subject	The data subject	The user of the AI system
Type of information provided	The contents of the GDPR in relation to the duty of information, so that data subjects are aware of the risks, the existence and consequences of profiling, the purposes, rights, safeguards and any other information that is necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data is processed.	Related to the explainability of AI systems, documentation, record keeping and providing information on how to use the AI system. It must be sufficient to: (i) enable users deploying the AI system to comply with their regulatory obligations. (ii) warn individuals that they are interacting with AI systems.

stages of processing, detail them, analyse the operating parameters and assess their impact on the data subjects.

In the event that an AI system is considered high-risk[31], the party implementing such a system must conduct a fundamental rights impact assessment[32]. Where the implementing party is required to carry out a DPIA, the fundamental rights impact assessment must be carried out together with the DPIA.

4. Conclusions and suggested action plan

4.1. Conclusions

The regulation of personal data has a significant impact on the development and application of AI. This interaction between these legal regulations and an evolving technology such as AI can be broken down into several essential aspects:

c) **Legal basis for data processing**: The EU's GDPR requires the processing of personal data to be supported by a lawful basis, which may include consent, but also legitimate interest, compliance with legal obligations or public interest. This means that AI must process personal data based on one of these lawful bases, which may limit the availability of certain data sets for the development, training and exploitation of AI systems.

d) **Purpose of data collection:** Personal data protection regulations require that data be collected for specific, explicit and legitimate purposes. AI, which often finds new applications and correlations in existing data, must adapt its functionality so as not to transgress this constraint, which can pose a challenge in expanding its capabilities and applications.

e) **Data minimisation:** Although AI systems are capable of processing large volumes of data, data protection regulations require that only data strictly necessary for the stated purpose is collected. This may affect the way AI algorithms access and use data, encouraging more selective approaches and a focus on minimising the personal information used.

f) **Transparency and explainability:** Data protection regulations demand transparency and the ability to explain decisions based on personal data. This drives the development of explainable or interpretable AI, which enables the reasoning behind automated actions and decisions affecting individuals to be understood.

31 As established in Article 6 et seq. of the AI Act.

32 Pursuant to Article 29 bis of the AI Act.

g) **Right to be forgotten:** Regulations give individuals the right to request deletion of their personal data. This poses a technical challenge for AI systems, especially those that have integrated this data into their predictive models or knowledge generation.

h) **Data security:** AI can function both as a tool to strengthen data security and as a target for those seeking to exploit vulnerabilities in data protection. Regulation will need to develop in the coming years to protect data integrity but also to seek to establish standards for the safe use of AI.

i) **Accountability and data governance:** The regulation of personal data demands a clear allocation of responsibilities for data processing. In the case of AI, this means that developers and operators of AI systems must establish robust governance mechanisms to ensure compliance.

In short, the regulation of personal data presents a number of constraints and challenges that must be considered in the full lifecycle of AI systems. However, these regulatory frameworks also promote practices that can enhance public trust in AI by ensuring ethical and responsible handling of personal data. Technological innovation in AI must therefore coexist with personal data management that respects individual rights and legal demands - a balance that is not only possible but essential for the sustainable and ethical development of AI.

The regulation of personal data presents a number of constraints and challenges that must be considered in the full lifecycle of AI systems.

4.2.Action plan

The following is a suggested action plan for organisations developing or using AI systems that process personal data:

j) **Assess the basis for legitimate use:** Identify and clearly document the lawful basis justifying the use of personal data in AI systems, ensuring compliance with the requirements established by data protection regulations.

k) **Integrate data protection principles into the design of the AI system:** Implement the concept of "privacy by design" from the beginning of the AI system lifecycle, ensuring that data collection, minimisation, processing and security are aligned with legal principles and obligations.

l) **Develop transparency and accountability mechanisms**: Prioritise the development of AI systems that can clearly and understandably explain their decisions based on personal data, allowing individuals to understand and challenge automated actions.

m) **Establish procedures for managing data subjects' rights:** Implement processes to respond effectively to requests for access, rectification, erasure and objection of personal data, in accordance with the requirements of data protection regulations.

n) **Training and awareness-raising on data protection:** Provide specialised training to professionals involved in the development and use of AI systems, promoting a culture of respect for privacy and personal data protection.

o) **Integrate DPIA:** Conduct DPIA to analyse and mitigate risks associated with the use of personal data in AI systems, working closely with privacy officers within the organisation.

p) **Data governance and accountability:** Establish robust governance structures that clearly define responsibilities and procedures for the processing of personal data in the context of AI, ensuring oversight and accountability at all stages of the process.

q) **Continuous monitoring and adaptation:** Implement monitoring and evaluation systems to identify possible deviations from legal requirements and best practices in data protection in order to make timely adjustments and ensure continuous compliance.

It is important to note that, unlike the future AI Act, the data protection rules applicable to this area are already fully in force. Therefore, by following this action plan, organisations will be able to ensure that the development and operation of AI systems are aligned with personal data protection principles, promoting public trust and mitigating the legal and ethical risks associated with the use of these technologies.

Differences in personal data and AI risk impact assessments

	DPIA	Fundamental Rights Impact Assessment
Active subject	The data controller	The user implementing the AI system
When should it be carried out?	When a processing operation, in particular, where it uses new technologies, is likely, by its nature, scope, context or purposes, to result in a high risk to the rights and freedoms of individuals.	When the AI system is considered high risk.
What elements should it contain?	At a minimum: • A systematic description of the envisaged processing operations and the purposes of the processing and, where applicable, the legitimate interest pursued by the controller; • An assessment of the necessity and proportionality of the processing operations in relation to their purpose; • An assessment of the risks to the rights and freedoms of data subjects; and • The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data, and to demonstrate compliance with the AI Act, taking into account the rights and legitimate interests of data subjects and other affected persons.	At a minimum: • A clear description of the intended purpose for which the AI system will be used; • A clear description of the intended geographical and temporal scope of use of the AI system; • The categories of individuals and groups likely to be affected by the use of the AI system; • A verification that the use of the AI system is in accordance with the laws on fundamental rights; • The reasonably foreseeable impact on fundamental rights of putting the high-risk AI system to use; • Specific risks of harm that may affect marginalised people or vulnerable groups; • The reasonably foreseeable negative impacts of the use of the AI system on the environment; • A detailed plan on how harm and negative impact on fundamental rights will be mitigated; • The governance system to be put in place by the user implementing the AI system, including human oversight, complaint handling and remedies.
When should it be carried out?	Before the start of the processing of personal data. In AI systems, prior to the design, selection or implementation of the AI solution for a given processing.	Before the AI system is put into operation
Should it be reported to the supervisory authority?	No	Yes, to the national supervisory authority, where the user implementing the AI system is not an SME.
Should it be communicated to stakeholders?	No, the opinion of data subjects may be sought in relation to the intended processing	Yes, when the user implementing the AI system is not an SME.

Pérez-Llorca

TECHLAW

Artificial intelligence

JANUARY 2024

A challenge for companies and for regulators

Barcelona
-
Brussels
-
Lisbon
-
London
-
Madrid
-
New York
-
Singapore

perezllorca.com