AI and Personal Data Regulation: From Public Authority Enforcement to Civil Liability Law

*Erwann Picart-Cartron**

ABSTRACT: The administrative procedure before the supervisory authority and the possibility to act under liability law are remedies both available under AI act and GDPR. On one hand, the supervisory authority has an ambivalent role. It operates at the intersection of market regulation and the protection of fundamental rights, combining both ex-ante and ex-post powers. On the other hand, liability law must not be undervalued in ensuring the enforcement of these regulations, especially given its preventive (prophylactic) function. Analyzing these remedies allows to highlight how the GDPR will be a key component in ensuring the effectiveness of the AI Act. Conversely, it illustrates how artificial intelligence provides a new perspective on certain provisions of data protection law.

KEYWORDS: personal data protection; artificial intelligence; regulation; civil liability; supervisory authorities

1. Introduction: the guiding principles of the AI Act and the GDPR

Artificial intelligence is an emerging technology, to the point that its true impact and the progress it generates remain difficult to fully assess. Despite these uncertainties, AI is rapidly integrating into every aspect of daily life, valued by individuals for its inference and automation capabilities. While these features can be used to simplify research or create entertaining content, they are also deployed by companies to monitor virtually every dimension of a person's existence, whether in the workplace, on the street, or in private spaces through smartphone activity.

AI thus becomes a powerful tool for collecting and generating personal data. A striking example is Google Vision, which can infer a wide range of personal information from simple images, from objective data such as eye color to sensitive details like religious or political beliefs.[1] This processing often occurs without individuals' awareness, and the data collected are subsequently used to refine user profiling.

[*] *PhD in law, Contractual Lecturer-Researcher, Associate researcher at IODE Laboratory (Law faculty of Rennes). Mail: erwann.picart@univ-rennes.fr. This article was subject to a blind peer review process.*

[1] This website is based on GoogleVision API in order to show the user what can be inferred from a single photo by the software Google Vision: https://theyseeyourphotos.com/.

This dynamic is central to understanding the risks posed by AI: as a novel technology, it amplifies well-known threats to individuals precisely because it autonomously processes data that, when related to an individual, undoubtedly qualify as personal data under General data protection regulation.[2]

For this reason, AI represents a new lens through which to examine the GDPR, offering fresh perspectives on the regulation of personal data.

The widespread adoption of AI and the extensive use of these technologies have prompted the European Commission to adopt the AI Act.[3] However, economic growth, one of the key benefits promised by AI, remains a critical factor in shaping this regulation.[4] The AI Act strikes a balance by treating AI as a product while aiming to regulate its development without stifling innovation or discouraging investment. To achieve this, the AI Act adopts a human-centric approach, ensuring that AI systems remain under human oversight at all times. For individuals, this means they must always be informed when interacting with an AI system and know whom to contact if needed. In this regard, and in many others, the AI Act shares similarities with the GDPR.

Indeed, the GDPR and the AI Act follow a similar logic. In many ways, the AI Act can be seen as the 'new GDPR' as both aim to regulate the development of emerging technologies. This similarity is evident in the extensive number of amendments proposed during discussions in the European Parliament for each text, as well as in the desire to leverage the Brussels Effect.[5] This effect refers to the extraterritorial influence of European legislation, reflecting the European legislator's ambition to set a global benchmark for high standards of protection, whether in personal data (as with the GDPR) or in artificial intelligence (as with the AI Act).

To achieve this, both European regulations rely on a risk-based approach. This approach pursues two objectives. The first is "to prevent risky activities, meaning activities that combine a probability of harm with varying degrees of severity".[6] The provisions of the GDPR thus aim to regulate the flow of personal data so that their processing does not pose disproportionate risks to the data subjects. As for the AI Act, it is structurally based on this approach,[7] as it adopts a classification of AI systems into four categories: prohibited AI practices,[8] high-risk AI systems,[9] and others.[10] This risk-based approach in European regulations introduces a new paradigm that is not purely based on banning practices but rather on

[2] Art. 4, 1), of 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, or GDPR).

[3] 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) N°167/2013, (EU) N°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, or AI Act).

[4] Recitals 3 and 4 of the AI Act specifically mentioned economic growth linked to development of human centric AIS.

[5] B. ANU, *The Brussels Effect*, in *Northwestern University Law Review*, 107(1), 2012; A. JEAUNEAU, *The Brussels Effect. How the European Union Rules the World*, in *Rev. crit. DIP*, 2021, 525.

[6] A. LATIL, *Digital Law: A Risk-Based Approach*, 2023, 7.

[7] A. LATIL*, Le Règlement relatif à l'intelligence artificielle et l'approche par les risques: application d'une méthode législative structurante*, in *RTD eur.*, 2024, 563.

[8] Art. 5, AI Act.

[9] Art. 6, AI Act.

[10] Art. 51, AI Act.

Downloaded from https://teseo.unitn.it/biolaw ISSN 2284-4503

holding stakeholders accountable.

The accountability principle requires that both the data controller and the AI system operator document all steps taken to comply with applicable regulations. These compliance procedures shape stakeholder practices ex ante by establishing clear expectations. They also enable ex post enforcement, allowing sanctions to be imposed in the event of a proven breach. These two dimensions of accountability, preventive and corrective, are interdependent. If sanctions are insufficient, the principle loses its effectiveness, undermining the regulatory paradigm that supports these frameworks. This is particularly significant because the GDPR and the AI Act may apply concurrently, creating a dual effect: increasing obligations for controllers using AI systems while simultaneously strengthening individuals' rights and means of defense.

The GDPR provides two distinct types of remedies. The first is an administrative remedy, which involves the supervisory authority.[11] This authority plays a unique role in upholding procedural rights. It combines both ex-ante and ex-post capabilities:[12] to oversee personal data processing, the supervisory authority can issue soft law (such as guidelines or recommendations) to assist controllers in achieving compliance.[13] Its ex-post powers come into effect in cases of GDPR violations, encompassing both investigative authority and the power to impose sanctions when necessary.[14]

The second category of remedies is based on the principle of civil liability. Under Article 82 of the GDPR, any data subject who has suffered material or non-material damage due to a breach of the Regulation has the right to claim compensation. This right is conditional on proving both a fault attributable to the controller or processor and the existence of compensable damage.

The AI Act also establishes a similar dichotomy of remedies. While the administrative remedy is directly stipulated within the AI Act itself,[15] civil liability is addressed through an amendment to the European Product Liability Directive.[16] This means that, unlike the GDPR, the liability of an AI controller under the AI Act cannot be directly invoked unless the AI system is deemed defective.

Many questions arise from the similarities between the GDPR and the AI Act, particularly regarding their concurrent application. Since the GDPR's system of remedies has been in force since 2018, it provides a solid basis for analysis. The insights gained from this analysis are invaluable for understanding and anticipating the enforcement of the AI Act. To this end, the paper is based on the French implementation of both regulations.

First, it is possible to identify certain shortcomings in the role of supervisory authorities, particularly in their use of ex-post sanctioning powers (1). From the perspective of data subjects, the sanctioning of GDPR violations serves as a marker of trust in the legal system established by the regulation. However, secondly, if trust in administrative authorities is undermined, individuals may seek alternative remedies, such as civil liability claims against controllers or AI operators, to protect their interests (2).

[11] Art. 77, GDPR.

[12] On this matter: M. HERVIEU, *Independent administrative authorities and the renewal of general contract law*, 118, 2012.

[13] Art. 57, GDPR.

[14] Art. 58, GDPR.

[15] Art. 85, AI Act.

[16] 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.

2. The shortcomings in the role of supervisory authorities

In France, the concept of a supervisory authority first emerged with the adoption of the 1978 Data Protection Act (Loi Informatique et Libertés).[17] This law was introduced in a specific digital context, where only public administrations had access to computer systems. At the time, the supervisory authority, originally the Commission Nationale de l'Informatique et des Libertés (CNIL), was established to monitor the use of these systems by the administration, particularly to prevent the profiling of citizens in their interactions with the state.[18]

This foundational role did not disappear with the evolution of French law. However, the adoption of the GDPR in 2018 significantly modified it. The most notable change lies in the introduction of the accountability principle, which requires data controllers to actively ensure that personal data is processed in compliance with GDPR provisions. Under this principle, controllers must document their compliance procedures to prepare for potential audits by the supervisory authority.[19] While this approach is central to the GDPR's regulatory logic, it has also revealed one of the main weaknesses in France's personal data protection framework: the challenge of effectively enforcing accountability in practice.

The AI Act follows a similar logic, extending the supervisory authority's mandate to ensure compliance by AI operators. This continuity underscores the expanding role of supervisory authorities in regulating emerging technologies, while also raising questions about their capacity to address the complexities of AI governance.

However, the cornerstone of this regulatory paradigm remains the sanctioning of controllers or operators in the event of non-compliance with these provisions. In this regard, the concurrent application of the GDPR and the AI Act creates an overlapping web of administrative authorities (2.1), which could complicate the enforcement of the latter regulation. This challenge is particularly acute given that current GDPR enforcement remains unsatisfactory (2.2).

2.1. The mesh of supervisory authorities

The AI act cite multiples supervisory authorities. Some are created in the giron of the European Commission like the AI office,[20] or the European Artificial Intelligence Board.[21] At national level, the AI regulation lay down on existing administrative authorities. They are the notifying authority in charge of "setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring",[22] or the "market surveillance authority"

[17] M. HERBERT, *Independent administrative authorities: protecting freedoms or social regulation?*, in C.A. COLLIARD, G. TIMSITEDS (sous la dir.), *Independent administrative authorities*, 1988; Conseil d'Etat, *Independent administrative authorities*, public report n. 52, 2001, 257.

[18] J. FRAYSSINET, *The french data protection act 6th January of 1978: a pedagogical and concise overview*, in *R.R.J.*, 2(28) 1987, 191; C. CASTETS-RENARD, *Internet Law: French and European Law*, 2^{e} éd., 2012.

[19] T. DOUVILLE, *Data protection law,* 2023, 265; European Union Agency for Fundamental Rights, *Handbook on European data protection law*, 2018, 194.

[20] Art. 64, AI Act.

[21] Art. 65, AI Act.

[22] Art. 3, 19, AI Act.

nominated under the 2019/1020 regulation concerning market surveillance and compliance of products.[23]

The involvement of market surveillance authorities reveals the dual nature of the EU's approach to AI regulation. While the AI Act aims to promote the development of human-centric AI,[24] its primary focus remains economic: ensuring the security of natural persons while preventing market distortions.[25] As stated in the AI Act, "non-compliant and unsafe products put citizens at risk" and "might distort competition with economic operators selling compliant products within the Union".[26]

Under this framework, market surveillance authorities are tasked with overseeing AI systems that pose risks, treating them like any other product.[27] Their mandate includes monitoring risks "to the health, safety, or fundamental rights of persons".[28] These authorities will assess the compliance of AI systems in the market, assisted by "authorities protecting fundamental rights"[29] already established at the national level.

While data protection authorities are likely to play this role, the European Data Protection Board (EDPB) has also considered their function within the broader scope of market surveillance. This overlap raises questions about the coordination and division of responsibilities between these bodies.[30]

This fragmented regulatory framework creates a mesh of administrative authorities, which risks complicating the oversight of AI's rapid and incessant development. In most EU Member States, including France, multiple administrative bodies are tasked with supervising specific markets.[31] The French government has proposed a "governance scheme for market surveillance authorities", which is currently under parliamentary review.[32] Under this scheme, the Directorate-General for Competition Policy and Consumer Affairs (DGCCRF) serves as the central coordinator. However, responsibilities are divided among several authorities, depending on the category of AI systems identified by the AI Act. For instance, regarding prohibited AI practices under Article 5, the French Data Protection Authority (CNIL) holds jurisdiction over: the use of AI systems for risk assessments of natural persons,[33] the use of AI

[23] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Regulation (EU) 2019/1020 on market surveillance and compliance of products).

[24] Rec. 1, AI Act.

[25] *In this sense: J. Charpenet, Fundamental Rights Put to the Test by the Standardization of Artificial Intelligence*, in *Dalloz IP/IT*, 2025, 591.

[26] Cons. 2, Regulation (EU) 2019/1020 on market surveillance and compliance of products.

[27] *S. Tabani, The European Regulation on Artificial Intelligence: Selected Issues After the First Six Months of the Initial Obligations Coming into Force*, in *Rev. UE*, 2025, 626.

[28] Art. 79, 2, of AI Act refers directly to the art. 3 point 19 of the 2019/1020 regulation on market surveillance and compliance of products.

[29] Art. 77, AI Act.

[30] EDPB, Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework, 16th of july 2024.

[31] Art. 74, 7, AI Act: "By way of derogation from paragraph 6, in appropriate circumstances, and provided that coordination is ensured, another relevant authority may be identified by the Member State as market surveillance authority for the purposes of this Regulation".

[32] The competent authorities for the implementation of the European Regulation on Artificial Intelligence, Directorate General for Enterprises.

[33] AI act, art. 5, §1, d).

systems that create or expand facial recognition databases,[34] the use of AI systems to infer emotions in workplace or educational settings,[35] the use of biometric categorization systems to deduce sensitive data from individuals' biometric information,[36] the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes.[37] For other prohibited practices, oversight is shared between the DGCCRF and the French Regulatory Authority for Audiovisual and Digital Communication (ARCOM).

Therefore, the unification and coherence of AI regulation will primarily be ensured by the AI Office. While national authorities retain jurisdiction over high-risk AI systems within their respective borders, the AI Office holds exclusive competence for general-purpose AI systems. Additionally, it will oversee: cross-border high-risk AI systems, and high-risk AI systems built upon multiple general-purpose AI systems, to prevent jurisdictional overlaps with national authorities. In most cases, the AI Office will also intervene when national authorities encounter difficulties in obtaining sufficient information due to the involvement of cross-border operators, thereby limiting their national competence.[38]

It is therefore clear that administrative authorities overseeing data protection and artificial intelligence serve fundamentally different purposes. The former are primarily focused on safeguarding fundamental rights in the context of computer technology, while the latter are tasked with supervising the AI market as a product. However, reality is far more complex. This complexity arises from: the interconnected web of administrative authorities, the diverse range of competences, and regulatory overlap, particularly in cases where an AI system qualifies as personal data processing. In such scenarios, an AI operator may simultaneously be considered a data controller under the GDPR[39] and an AI operator[40] under the AI Act, creating dual regulatory obligations.[41]

This regulatory overlap, applied to the same subject matter, underscores the complementary yet distinct roles of these administrative authorities. Their broad and varied capabilities are particularly significant when fundamental rights protection is at stake. In this context, an assessment of how the French Data Protection Authority exercises its powers could provide valuable insights for anticipating the future enforcement of the AI Act.

2.2. The uncertainties surrounding sanctions by personal data authorities

The powers of supervisory authorities have evolved as regulations have adapted to the digital society we know today. These powers follow the same logic: the fundamental right of natural persons to the protection of personal data must be guaranteed, thanks to the specific role of supervisory authorities. Indeed, the supervisory authority acts both as a guide for controllers and as a judge in cases of regulatory violations. For example, the French Data Protection Act, which implements certain aspects of

[34] AI act, art. 5, §1, e).
[35] AI act, art. 5, §1, f).
[36] AI act, art. 5, §1, g).
[37] AI act, art. 5, §1, h).
[38] T. Douville, E. Netter, *The Artificial Intelligence Regulation: AI Law in Search of Coherence – Part 2*, in *RTD Com.*, 32, 2025; L. Badiane, M. Bourgeois, L. Bataille *et al.*, *AI Act: Authorities and Legal Remedies*, in *JCP E.*, 3, 2026.
[39] Art. 4, 7 GDPR.
[40] Art. 3, 8 AI Act.
[41] T. Douville, *Artificial Intelligence and Personal Data*, in *Dalloz IP/IT*, 2025, 147.

the GDPR, grants the authority the ability to "publish guidelines, recommendations, or frameworks intended to facilitate compliance with personal data processing";[42] to "handle complaints, petitions, and claims";[43] and, finally, to carry out inspections, either directly or through its staff, of any data processing operations and, where appropriate, to obtain copies of any documents or information media useful for the performance of its tasks.[44]

This consolidation of power must adhere to the principles set out since 1978 in Article 1, which stipulate that the development of information technology "must not infringe upon human identity, human rights, privacy, or individual and public freedoms". At the time, the legislator envisioned this administrative authority, the first of its kind, as "the guardian of societal awareness regarding the use of information technology".[45] However, from a procedural standpoint, this consolidation raised certain concerns. This is why the French Constitutional Council established a framework for this power when it approved the centralization of these prerogatives within administrative authorities,[46] on the condition that they are exercised by an independent body, that any proposed sanction excludes deprivation of liberty, and that the law provides measures to safeguard constitutional rights and freedoms.[47] These guarantees applied both to the French Data Protection Authority and to any other independent administrative authority. Consequently, the supervisory authority responsible for oversight was also required to follow the same principles.

Therefore, administrative authorities possess a range of powers to oversee the enforcement of both the GDPR and the AI Act. One key aspect of these powers is ex-ante supervision, which includes issuing guidelines and soft laws to assist controllers and AI operators in achieving compliance, as well as developing codes of practice.[48] For instance, in 2024, the French data protection authority responded to 1,448 requests for advice from controllers.[49] While this proactive approach is essential for helping controllers comply and enabling individuals to exercise their rights,[50] it is closely tied to the accountability principle which is a key aspect of the AI Act and GDPR.[51]

The accountability principle entails another set of powers, specifically the authority to sanction any breach of these regulations. To fulfill this mission effectively, administrative authorities possess extensive investigative powers to gather sufficient information about data processing. These powers include the right to access "any premises of the controller and the processor, including any data

[42] Art. 8, 2°, b, of French data protection act, mod. by the ord. n°2018-1125 du 12 déc. 2018 (French data protection act).

[43] Art. 8, 2°, d, French data protection act.

[44] Art. 8, 2°, g, French data protection act.

[45] B. Tricot, *Report of the Commission Nationale de l'Informatique et des Libertés*, 1975, 89.

[46] Constitutional Council, Jan. 17, 1989, Law No. 88-248 DC amending the Sept. 30, 1986 law on freedom of communication.

[47] Constitutional Council, July 28, 1989, on the Law concerning financial market security and transparency, No. 89-260 DC.

[48] Art. 56, AI Act.

[49] CNIL, *Report of the Commission Nationale de l'Informatique et des Libertés,* 2025, 9.

[50] French data protection authority answer to 14 654 exercise of individual rights.

[51] A. Latil, *Digital Law: A Risk-Based Approach*, 2023, 131; A. Latil, *The Artificial Intelligence Regulation and the Risk-Based Approach: Application of a Structuring Legislative Method*, cit.

processing equipment and means".[52] In this context, controllers may respond to the report issued by the administrative authority or be heard by the restricted formation responsible for imposing sanctions.[53] In each of this step, the controller may recognize some of the facts, and none of the legal provision mentioned the right to remain silent. Therefore, a constitutional question has arisen regarding the scope of the right to remain silent, particularly in relation to the fundamental right against self-incrimination.[54]
The French Supreme Administrative Court initially ruled that this right was not applicable during investigations conducted by the administrative authority. However, in response to a constitutional challenge, the French Constitutional Council determined that this right must be guaranteed.[55] Consequently, the provisions allowing controllers to submit observations in response to the administrative authority's report or to be heard by the restricted formation must be amended to incorporate this right. In the interim, the right to remain silent must be clearly defined. This incertitude abovementioned illustrate at the same time the extensive powers of French data protection authority, and some of the question remaining concerning the application of AI Act by administrative authority.

Despite the extensive powers granted to administrative authorities, every decision issued by the French data protection authority may be appealed before the Supreme Administrative Court (i.e. Conseil d'État). However, this procedural safeguard is undermined by the limited scope of judicial review exercised by the administrative court. The French data protection authority retains significant discretionary power over the outcomes of its investigations. For instance, it may "remind the party of its legal obligations or, if the observed breach is capable of being remedied, issue a formal notice requiring compliance within a specified timeframe".[56]

The authority enjoys broad discretion in determining how to address a complaint or an alleged breach of data protection regulations. The Supreme Administrative Court has consistently upheld this position,[57] even in cases where complaints are based on actual violations of personal data rights. This raises critical questions about the effectiveness of legal remedies available to individuals and the overall enforcement of data protection regulations.[58]

This broad discretionary power raises questions regarding another capability of the French Data Protection Authority. Since 2022, a simplified sanction procedure has been introduced to deal with cases that are not complex.[59] This procedure was established in response to the growing number of complaints. Several conditions must be met: first, other similar decisions must already have been issued by the French Data Protection Authority, and second, both the facts and the law of the case must be straightforward. The decision to follow this new procedure lies with the president of the Authority. The procedure is simpler because the president of the restricted committee decides alone. Finally, there is no hearing session for the case. Therefore, even though the controller may at any time request to switch

[52] Art. 58, point 1, f, GDPR.
[53] Art. 22, French data protection act.
[54] French declaration of Human and Civil rights of 26th august 1789, art. 9; Art. 6 ECHR.
[55]Constitutional Council, décision n° 2025-1154 QPC, 8 august 2025.
[56] Art. 20, II, French data act; Art. 58, point 2, GDPR.
[57] CE, 19 avr. 2024, n° 473459 ; CE, 10e et 9e ch. réunies, 21 oct. 2022, n° 459254.
[58] N. Martial-Braz, CNIL, *Judicial Oversight and Data Governance: Between Discretionary Power and New Horizons*, in *Communication Commerce Electronique*, 2025.
[59] Art. 22-1, French data protection act.

to the ordinary procedure, financial sanctions under the simplified procedure are limited to €20,000, and may also take the form of a mere reminder or a compliance deadline. This simplified procedure may be a more effective way of handling the steady increase in complaints, but it lacks clear guidance on the use of sanctioning powers.

These uncertainty regarding sanction capabilities of the data protection authority raises question regarding AI regulation. The sanction procedure is not only intended to punish violations of data protection or AI regulations. It also has a preventive function, aiming to discourage others from acting in the same way. It provides regulations and soft law documents with another means of interpretation. However, this simplified procedure conceals the details of cases, the names of the parties, and the reasoning that led to the sanctions. These specificities, combined with the relatively low number of sanctions imposed by the French Data Protection Authority compared to its counterparts in Spain (281 cases, €35 million), Germany (416 cases, €14 million), and Italy (145 cases, €145 million),[60] highlight a more limited use of its sanctioning power. The French authority has issued only 87 sanctions, amounting to €55 million in total—including €50 million against Orange, a French telecom operator. Among these 87 sanctions, only 12 have been published. This means that there is no public information about the sanctioned controllers or the reasoning that led to the sanctions. The legal arguments are only briefly listed on the website of the French Data Protection Authority.[61]

While this procedure is a welcome development for handling multiple complaints, it does not fully serve the function of a sanction. To be truly effective, a sanction must fulfill a preventive function. Its purpose is indirectly to help other controllers achieve compliance by clarifying which practices constitute violations and by protecting individuals from being subjected to them. However, this new simplified procedure falls short of the true purpose of a sanction. It is undeniable that the significant fines imposed on GAFAM or BIATX send strong messages. Yet a violation of fundamental rights is of the same nature regardless of scale. The secrecy surrounding this simplified procedure largely benefits the controller while at the same time weakening the enforcement of the right to data protection.

These analyses are insightful regarding future application of the AI Act by administrative authority. Since French data protection authority will be in charge of any AIS that include personal data processing, the procedure and the jurisprudence in place will have an impact on how AI act will be enforce.

Regarding remedies, administrative enforcement is not the only means for individuals to seek redress or sanctions in the event of a GDPR or AI Act violation. Both regulations allow for the cumulative use of civil liability and administrative enforcement. Consequently, individuals may bring an action before the supervisory authority and also before a civil court. The latter option can serve as a way to compensate for any shortcomings in the administrative recourse.

3. The possible remedies available under civil liability

Civil liability law provides individuals with a means to seek compensation and to hold controllers accountable. This remedy is explicitly provided for in both the AI Act and the GDPR. Furthermore, these two legal avenues can be pursued simultaneously. Article 85 of the AI Act outlines the remedies

[60] EDPB, *Protection personal data in a changing landscape – EDPB Annual report*, 2024, 39.

[61] https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil (last visited 25/09/2025).

Downloaded from https://teseo.unitn.it/biolaw
ISSN 2284-4503

available to individuals or legal entities who believe that a breach of the regulation could warrant a sanction by the market supervisory authority. In such cases, the affected party may lodge a complaint with the designated administrative authority, but this is not their only option.

Indeed, this article mirrors the wording of Article 77 of the GDPR regarding remedies available to individuals. In essence, it states that "without prejudice to any other administrative or judicial remedy"[62] any person may file complaints with the independent administrative authority responsible for data protection or market supervision. Three avenues of recourse are therefore open to the individual: one before the civil courts, another before the administrative courts, and the last before the independent administrative authority. The text does not specify how these remedies interact. This is why a preliminary question was referred to the CJEU in the context of the exercise of the right of access to personal data by a data subject. The question was whether the individual could simultaneously file a complaint with the independent administrative authority and bring a civil action. In short, whether the remedies available under public law and those available under civil law could be exercised in parallel. The CJEU answered in the affirmative, stating that the remedies available to individuals under the GDPR may be exercised concurrently and independently.[63]

From this perspective, the reasoning applied by European judges under the GDPR can be extended to the remedies available under the Artificial Intelligence Act. The prohibition of certain practices under the AI Act would therefore not rely solely on administrative fines. Following the reasoning of the Court of Justice of the European Union outlined above, an individual who believes they have suffered harm as a result of such practices could both lodge a complaint with the relevant market surveillance authority and bring a claim before a judicial court.

The combination of these remedies is justified by two main considerations. First, they serve distinct functions: an administrative fine imposed by a national supervisory authority constitutes a public sanction targeting the AI system as a whole, while civil liability aims to compensate for individual harm. Second, the combination is justified by the regulatory framework governing AI systems, in which 'private enforcement' plays a central role.[64] This concept refers to the active participation of individuals in the enforcement of the regulation through civil actions.

However, unlike the GDPR, the AI Act does not allow for the personal liability of AI operators to be engaged. The AI Act does not provide an autonomous legal basis for civil liability claims. Instead, it follows the logic of treating AI as a product. As a result, the European Directive (EU) 2024/2853 on liability for defective products was amended to include AI-related damages. This means that individuals cannot seek compensation through the personal civil liability of the AI operator (A). One way to overcome these limitations could be to rely on civil liability under the GDPR to hold the AI operator

[62] For comparison, Article 77 of the GDPR states: "Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority (…) if he or she considers that the processing of personal data relating to him or her infringes this Regulation"; whereas Article 85 of the RIA provides: "Without prejudice to other administrative or judicial remedies, any natural or legal person who has grounds to consider that there has been a violation of the provisions of this Regulation may lodge complaints with the competent market supervisory authority".

[63] CJEU, 12 January 2023, Case C-132/21, *Budapesti Elektromos Művek*, ECLI:EU:C:2023:2.

[64] Private enforcement is a distinct notion from 'public enforcement', which refers to the action taken by public authorities to enforce a regulation: M.A. FRISON-ROCHE, J.C. RODA, *Droit de la concurrence*, 2022.

processing personal data accountable (B).

3.1. The limited scope of civil liability under the AI Act

Unlike the GDPR, the AI Act does not establish a separate legal basis for civil liability claims. This is primarily due to the abandonment of the proposed Directive on adapting non-contractual civil liability rules to artificial intelligence, which was discarded by the European Commission on 11 February 2025. The proposed Directive, as outlined by the European Parliamentary Research Service (EPRS), aimed to address "extra-contractual" civil liability—rules that would allow victims to seek compensation for harm caused by AI systems, regardless of any contractual relationship with the liable party. According to the EPRS, the Directive would have ensured that: "Any victim (individual or business) could be compensated if harmed by the fault or omission of an AI provider, developer, or user, resulting in damage recognized under national law (e.g., health, property, privacy, etc.)".[65] This form of liability was designed to be fault-based, meaning it would apply in cases where an AI operator breached a pre-existing legal obligation.[66] Combining this liability framework with the presumption mechanisms of the AI Act would have significantly strengthened protections for individuals harmed by AI systems. However, in a tense international political context,[67] the European Commission ultimately abandoned the Directive, citing simplification efforts as the primary justification.

Therefore, with the abandonment of this directive, the only remaining option for individuals is to invoke non-fault liability for defective products. This type of liability is almost exclusive, precluding other forms of liability. The Court of Justice of the European Union (CJEU) has limited the effects of the option provided by Article 13 of the directive.[68] This article allowed Member States a margin of appreciation in transposing the directive, meaning victims had to choose between liability based on a defective product or another common cause of liability. However, the CJEU restricted this choice to cases involving the producer's fault or warranty against latent defects, excluding the approach adopted by French civil judges based on the lack of expected safety.[69] As a result, the only way for victims to hold the producer liable is to prove damage separate from the defective product itself. For example, the French Cour de cassation (the supreme civil court) allows victims to act on the basis of a failure to provide information or a breach of the duty of care.[70]

In the context of AI, victims must prove that a defect in the AI system caused the damage.[71] This defect is defined as the system failing to provide the level of safety that a person is entitled to expect under EU

[65] M. TAMBIAMA, *Artificial intelligence liability directive*, in *Parliamentary Research Service*, 2023, 5.

[66] M. PLANIOL, *Elementary Treatise on Civil Law*, 11th ed., 1931.

[67] *EU Commission drops AI liability directive amid US criticism*, in *Harici*, 2025, disponible sur https://harici.com.tr/en/eu-commission-drops-ai-liability-directive-amid-us-criticism/, (last visited 15/09/2025).

[68] CJCE, 25 avril 2002, *Commission des communautés européennes c. République française*, C-52/00, D. 2002. 2462, chron. Larroumet; D. 2002. 1670, obs. Rondey; D. 2002. 2935, obs. Pizzio; CCC nov. 2002. Chron. 20, obs. Laporte; RTD civ. 2002. 523, obs. Jourdain; RTD civ. 2002. 868, obs. Raynard; RTD com. 2002. 585, obs. Luby.

[69] See, C. CAILLÉ, *Liability for Defective Products*, in *Rép. civ.*, 102, 2025.

[70] Civ. 1re, 7 mars 2006, 04-16.179, JCP 2006. I. 166, no 8, obs. Stoffel-Munck; RTD civ. 2006. 565, obs. Jourdain; RCA 2006, comm. 164, note Radé.

[71] On this matter: M. BACACHE, *Artificial Intelligence and the Law of Liability and Insurance*, in A. BENSAMOUN, G. LOISEAU eds. (dir.), *Droit de l'intelligence artificielle*, 2022.

or national law.[72] While the AI Act imposes significant obligations on AI operators and provides victims with multiple avenues to demonstrate such defects, operators may still invoke the 'development risk defense'. This exemption, as outlined in the relevant directives, allows operators to avoid liability if the damage was caused by a risk that could not reasonably have been discovered at the time the AI system was placed on the market.[73]

For products that, by their nature, evolve constantly after being placed on the market, this exemption significantly reduces victim protection under this liability regime. Furthermore, the victim's right to bring an action is subject to two statutory time limits. First, the victim has three years to act from the moment the damage occurs, the defect is discovered, and the identity of the AI operator is known.[74] Second, this special liability expires ten years after the product was placed on the market.[75] These time limits favor the producer (i.e., the AI operator) but restrict the victim's opportunities for redress, especially when compared to other liability regimes, such as fault-based liability, which allow a five-year period starting from the discovery of the damage.[76]

Then, the AI act does not provide direct ways for natural person to be compensate in case of AI violation. It's in this particular case where GDPR could be used by individuals to enforce AI Act provision as well as to be compensate in case of a damage linked with personal data violation.

3.2. The extent of remedies under the GDPR

As previously mentioned, the GDPR provides two types of remedies: a complaint before the administrative authority and civil liability of the controller in the event of damage caused by a GDPR violation. These two remedies can be pursued simultaneously for the same damage. However, these are not the only ways individuals can use the GDPR to seek compensation for violations of their personal data processed through an AI system.

Firstly, the right to data protection can be enforced through collective procedures against the controller. Data protection breaches are often collective issues, causing harm to multiple individuals. In such cases, the harm is considered "mass harm", defined as situations where "several individuals suffer individual injuries resulting from the same causative event".[77]

The French government, exercising the discretion granted to Member States, has empowered "a body, organisation, or not-for-profit association" to bring collective actions for effective judicial remedies against data controllers, particularly when the rights of individuals have been violated.[78] This mechanism represents a French adaptation of the US 'class action', but without punitive damages, only compensation for personal harm suffered by victims.

Several entities, including consumer associations and trade unions, are authorized to initiate such

[72] Directive (EU) 2024/2853 of the European Parliament and of the Council on liability for defective products and repealing Council Directive 85/374/EEC, 23 October 2024, art. 7, 1.

[73] *Ivi*, art. 11, point 1, e.

[74] *Ivi*, art. 16.

[75] *Ivi*, art. 17.

[76] Art. 2224 French Civil code.

[77] M. Bacache, C. Larroumet, *Obligations and Extra-Contractual Civil Liability: General Law and Special Regimesx*, 2021.

[78] GDPR, art. 80 §2.

actions. In practice, however, only two class actions were launched in 2019:[79] one by the Internet Society against Facebook, and another by the UFC-Que Choisir[80] against Google. There has been no public update on their progress since then.

Nonetheless, collective actions remain a potentially powerful tool for enforcing the GDPR, especially in light of the increasing number of data breaches in recent months, including several massive incidents.[81] They could serve as an effective complement to the actions (or inaction) of the CNIL, offering two key advantages for individuals: first, unlike administrative procedures, collective actions can directly award damages to victims; second, they reduce the burden on individuals, who might otherwise face time-consuming and costly legal proceedings.

Secondly, the Court of Justice of the European Union (CJEU) has adopted a broad interpretation regarding the actors who may base their legal action on a GDPR violation.[82] According to the CJEU, a breach of data protection regulations can be invoked not only by data subjects or entitled entities (such as consumer associations or labor unions), but also by other parties. This interpretation is grounded in Article 82 of the GDPR, which grants "any person" the right to seek compensation from the controller.[83]

This approach extends the scope of data protection regulation beyond the mere protection of the fundamental right to data protection. It also recognizes the economic value of personal data within the information society, where such data constitute a key competitive advantage for companies. After all, the GDPR pursues two main objectives: the protection of personal data and the free flow of data. The economic dimension of data is central to the digital economy. For this reason, the CJEU has allowed competitors to bring unfair competition claims based on GDPR violations, potentially leading to civil liability proceedings.[84]

These two avenues for engaging the civil liability of a data controller could serve as an interesting procedural remedy for the current lack of specific procedures addressing AI systems. Given that the processing of personal data is a central component of artificial intelligence systems, any violation of provisions related to personal data protection under the AI Act could potentially trigger the civil liability of the AI operator.

Indeed, the human-centric approach advocated by the European Commission places the responsibility for compliance squarely on the AI operator. Consequently, any operator of an AI system that processes personal data could be held liable for damages caused by such processing.

[79] https://observatoireactionsdegroupe.com/registre/registre-france/ (last visited 25/09/2025).

[80] A Consumer rights organisation.

[81] CNIL, *Report of the Commission Nationale de l'Informatique et des Libertés, 2024*, 505-629. Data breach have been listed by the french data protection authority, with some concerning millions of french individuals.

[82] CJUE, 4 octobre 2024, *Lindenapotheke*, C-21/23, D. 2024. 1777; *ivi*, 2115, point de vue F. Megerlin et E. Pinilla; Dalloz IP/IT 2025. 112, obs. V. Younès-Fellous; CCE 2024. Comm. 112, obs. A. Debet; CCC 2025. Comm. 7, obs. H. Aubry; RTD Com. 2025, p.94, note T. Douville; CJUE, 4 juillet 2023, *Meta Platforms e.a*, C-252/21, AJDA 2023. 1542, chron. P. Bonneville, C. Gänser et A. Iljic; D. 2023. 1313; Dalloz IP/IT 2024. 45, obs. A. Lecourt; RTD eur. 2023. 754, obs. L. Idot; CCE 2023. Comm. 94, N. Martial-Braz; Europe 2023. Comm. 340, obs. L. Idot; LEDICO, sept. 2023, DDC201u1, obs. T. Douville; CJUE, 28 avril 2022, *Meta Platforms Ireland Limited c/ Bundesverband der Verbraucherzentralen und Verbraucherverbände*, C-319/20, Dalloz IP/IT 2022, 461, obs. A. Latil; JA 2022, n° 660, 12, obs. X. Delpech; Dalloz IP/IT 2022. 229, obs. C. Crichton; RTD eur. 2023. 426, obs. F. Benoît-Rohmer; CCC 2022. Comm. 124, obs. S. Bernheim-Desvaux.

[83] CJUE, 4 juillet 2023, *Meta Platforms*, cit., nº 50.

[84] CJUE, 4 octobre 2024, *Lindenapotheke*, cit.

Furthermore, the core concept of damages related to the protection of personal data could take on a new dimension with the development of AI.[85] As this technology subtly or rapidly transforms every aspect of society, it may give rise to more nuanced and sensitive types of harm. This evolution could enable individuals to seek redress through the civil liability of AI operators and data controllers.

These two ways to engage civil liability of a data controller could be an interesting procedural palliative to the lack of special procedure for AIS. Since personal data processing are a key part of artificial intelligence systems, a violation of the provision that include personal data protection under AI Act could lead to engage civil liability of the AI operator. Indeed, the human centric approach wanted by the European commission tel the AI operator in charge of the compliance. Therefore, any operator of an AIS processing personal data could be responsible for any damages caused by it. More, the core concept of damages relating to protection of personal data could be gain a new dimension thanks to development of AI. Since this technology change subtly, or quickly, every aspect of our society, it could led to a more sensitive type of damages permitting individuals to act based on civil liability of AI operator and controller of personal data.

4. Conclusion

Far from reaching a conclusion, this section aims to synthesize the key issues at stake in the future development of AI regulation. As seen with the regulation of personal data, and the French perspective of this paper, the powers and role of independent supervisory authorities are central to safeguarding individual rights. However, the increasing complexity of these authorities as implemented in France, coupled with the scope of their powers, does not necessarily indicate a favorable trajectory for regulations that protect individual rights. For this reason, classic procedures derived from common civil rights should not be overlooked.

Despite the lack of specific civil action under the AI Act, the GDPR is likely to remain a common legal basis for civil actions against AI operators. Indeed, the CJEU has already expanded the scope of existing civil actions to allow the GDPR to be applied as broadly as possible (i.e allowing economic actor to act under GDPR for unfair competition). Consequently, this emerging and promising line of jurisprudence could be used to sanction AI operators that process personal data posing the greatest risks to individual rights and freedoms.

Yet, for the GDPR to effectively fulfill this role, it must remain unchanged. This is far from certain, given the proposal for an omnibus regulation that would amend both the GDPR and the AI Act, among others.[86] It will potentially weakened GDPR principles in order to facilitate AI system development.[87]

[85] On the notion of damages relating to personal data protection: J. KNETSCH, *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, in *JETL*, 13(2), 2022, 132.

[86] Proposal for a regulation 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), and 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), 19 novembre 2025.

[87] Digital Omnibus Report V2: Analysis of Select GDPR and Privacy Proposals by the Commission.