

PROTECTING PERSONAL DATA IN THE AI ERA IN THE EUROPEAN UNION: BETWEEN COMPLIANCE AND OPPORTUNITY



Samir Dahmani ^{1*}

Faculty of Law and Political Science Department of Law

University of Tizi Ouzou (Algeria)¹

Submission date: 23/01/2026 Acceptance date: 14/03/2026 Publication date: 30/06/2026



Abstract:

Artificial intelligence (AI) no longer a technology of the future, is now a pervasive reality transforming the way companies operate and interact with their customers. From individualizing services to robotizing operations, artificial intelligence has an immense capacity to improve efficiency and competitiveness. However, this rapid transition is accompanied by considerable challenges, particularly with regard to the protection of personal data.

Indeed, AI is obliged to comply with the legislation on the protection of personal data, in particular the (GDPR) and the (AI Act) in Europe. It is necessary to implement principles such as data minimization, transparency and safeguarding of users' rights. This includes carrying out impact assessments and incorporating the principle of “privacy by design”. In order to meet these criteria, companies are required to develop ethical, fair and secure artificial intelligence, while putting in place strong governance structures to ensure the responsible exploitation of AI.

Key Words: AI; Compliance; GDPR; AI Act; Opportunities; Responsibility.

حماية البيانات الشخصية في عصر الذكاء الاصطناعي في الاتحاد الأوروبي: بين الامتثال

والفرص

ملخص:

الذكاء الاصطناعي الذي كان لا يُعتبر كتقنية للمستقبل، أصبح في هذه الآونة كواقع غير طرق عمل الشركات وتواصلها مع عملائها ورقمنة طريقة تقديم الخدمات والمهام، أين يمتلك الذكاء الاصطناعي إمكانات هائلة لتحسين الكفاءة والتنافسية. ومع ذلك، يُواجه هذا التحول السريع تحديات كبيرة، لا سيما فيما يتعلق بحماية المعلومات الشخصية.

وعليه، يجب أن يَمْتَثِلَ الذكاء الاصطناعي للتشريعات المتعلقة بحماية البيانات الشخصية، وبالأخص تنظيمات الاتحاد الأوروبي المتعلقة بحماية البيانات الشخصية (RGPD) واستعمال الذكاء الاصطناعي (AI Act). حيث يتطلب ذلك، اعتماد المبادئ المتعلقة بتخفيف استخدام البيانات وإرساء الشفافية، وحماية حقوق المستخدمين، وكذا تقييم الآثار المترتبة مع دمج مفهوم حماية الخصوصية في بداية تصميم نماذج الذكاء الاصطناعي. وللوفاء بهذه المعايير، ينبغي على الشركات تصميم نماذج ذكاء اصطناعي تتسم بالأخلاقية والعدالة والأمان، مع إرساء هياكل حوكمة مبنية لضمان الاستخدام الأمثل والمسؤول للذكاء الاصطناعي. الكلمات المفتاحية: الذكاء الاصطناعي، الامتثال، ت.أ.ح.م.ش، ت.ذ.إ، الفرص، المسؤولية.

La protection des données personnelles à l'ère de l'IA dans le cadre de l'Union européenne : Entre la conformité et l'opportunité

Résumé:

L'intelligence artificielle (IA) qui n'est plus une technologie d'avenir, est maintenant une réalité omniprésente transformant la manière dont les entreprises fonctionnent et interagissent avec leurs clients. De l'individualisation des services à la robotisation des opérations, l'intelligence artificielle détient une capacité immense pour améliorer l'efficacité et la compétitivité. Cependant, cette transition rapide s'accompagne de défis considérables, particulièrement en ce qui concerne la protection des données personnelles.

En effet, L'IA est tenue de respecter la législation sur la protection des données personnelles, notamment le RGPD et l'AI Act en Europe. Il est nécessaire de mettre en œuvre des principes tels que la minimisation des données, la transparence et la sauvegarde des droits des utilisateurs. Cela passe notamment par la réalisation d'évaluations d'impact et l'intégration du principe de « protection de la vie privée dès la conception ». Afin de se conformer à ces critères, les entreprises sont tenues de développer des intelligences artificielles éthiques, équitables et sûres, tout en mettant en place des structures de gouvernance solides pour garantir une exploitation responsable de l'IA.

Mots Clés: IA ; Conformité ; RGPD ; AI Act ; Opportunités ; Responsabilité.

Introduction

In the age of artificial intelligence (AI), machines are able to « think », and algorithms make decisions based on a vast amount of collected data. However, it is often difficult to determine where these data come from and whether they are reliable, making any verification complex. This lack of transparency raises a question of trust and raises fundamental concerns regarding the protection of personal information and respect for the privacy of individuals, point of reference in its legal framework, its challenges and its prospects.

However, the emergence of AI has led to increased concerns about its potential adverse effects on individuals, vulnerable people and society as a whole. Therefore, if AI with advanced decision-making skills provided harmful information or facilitated criminal acts, it would result in legal liability of AI actors on the de facto basis of things. This principle in civil law makes it possible to attribute responsibility to the user of the AI that causes harm, even without human fault.

In this regard, AI operates by manipulating large volumes of data, including personal data such as names, addresses, online behaviors and user preferences. This data allows machine learning algorithms to improve their accuracy and provide customized solutions. Nevertheless, their implementation raises legal and ethical questions, in particular regarding the adherence to the General Data Protection Regulation (GDPR) as well as the safeguarding of confidential data.

Indeed, the convergence of AI and personal data protection legislation has created complex challenges and opportunities, especially for programmers and users. However, the rapid rise of AI-based systems, especially those based on personal data, requires a delicate balance between innovation and compliance.

This research aims to analyze how the AI Act and the General Data Protection Regulation (GDPR) address legal issues related to AI technologies, such as liability, data minimization and the legal basis for their processing. It also highlights recent court rulings and regulatory initiatives while setting standards that are detailed enough to distinguish AI from more basic software systems.

The subject of this study highlights a complex issue concerning personal data manipulated by artificial intelligence: **What are the risks that AI represents in terms of personal data protection, and what rules apply in the event of harm caused by artificial intelligence, the (AI Act) or the (GDPR) ?**

In order to address these issues, we followed an analytical and deductive approach, through which we first address in **the first topic** the notion of AI and personal data, and the risks generated by AI in the context of personal data protection, then the contributions of the (GDPR) on AI (third topic), and the contributions of the European Regulation on AI (AI Law), as well as the main differences and complementarities between the (GDPR) and the (AI Law). While, in **the second topic** we analyze the liability of actors for damage caused by AI, and the opportunities of AI for data protection.

THE FIRST TOPIC:

The main differences and complementarities between the (GDPR) and the (AI Act).

The intersection between artificial intelligence (AI) and personal data protection is one of the major challenges of the decade, structured in Europe by the General Data Protection Regulation (GDPR) and the recent European Regulation on AI (AI Act). In addition, these two texts form a complementary regulatory base to frame innovation, with reinforced obligations.

First requirement: the notion of AI and personal data, and the risks generated by AI

Artificial Intelligence (AI) is capable of simulating human intelligence to perform complex tasks. Due to their operation, AI and personal data are involved (**first section**). Furthermore, the use of these technologies carries several major risks (**second section**).

First section: Definition of AI-related terms

There is a deep connection between AI and personal data, and AI uses this information extensively for its learning process, raising questions about collection, transparency and bias. At the same time, it offers solutions to ensure better protection (encryption, access management). Laws such as the (GDPR) and the (AI Act) regulate these practices, imposing responsibilities (agreement, user rights) to ensure ethics and trust, although risks of misuse or disclosure remain.

1- Artificial intelligence (AI) and machine learning

It is well known that defining AI can be difficult, since no definition can satisfy everyone, even within experts. According to *John McCarthy*, a leading player in the industry, AI is a technological innovation that gives computers and machines the ability to mimic learning, understanding, problem solving, decision-making, creativity and human autonomy¹.

For *Marvin Lee Minsky*, one of its designers, artificial intelligence represents « the implementation of computer programs that perform tasks currently better performed by humans because they require advanced cognitive processes such as: perceptual learning, memory management and critical reasoning »². This definition combines the « artificial » element associated with computers and computer processes with the « intelligent » elements that reproduce human behavior, including reasoning and learning.

¹ Cole STRYKER, Eda KAVLAKOGLU, « Qu'est-ce que l'intelligence artificielle (IA)? », article published 16/08/2024, from the following address: <https://www.ibm.com/fr-fr/topics/artificial-intelligence> (accessed on 16/03/2025.)

² Frédéric ALEXANDRE, « Marvin Minsky : l'intelligence artificielle débraillée », 2016, pp. 01-03. HAL Id: hal-01402261 or <https://inria.hal.science/hal-01402261v1> (accessed on 03/10/2025.)

For example, **David SHAPIRO** offers a broad definition of artificial intelligence, describing it as a branch of science and engineering aimed at understanding intelligent behavior through the computer and developing artificial systems capable of reproducing that behavior¹.

Other definitions, such as that of **Maximilien LEVESQUE**, focus on the scientific aspect. He defines AI as the field of study that examines intelligent behavior from a computational perspective. Therefore, Nilsson characterizes AI as a long-term scientific field, which is based on the mechanization of human-level intelligence².

In addition, the AI Act Regulation³, defines AI as « an automated system that is designed to operate at different levels of autonomy and can be adaptable after deployment, and that, for explicit or implicit purposes, deduces, from the inputs it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. »

The key takeaway from these definitions is that artificial intelligence is a broad field that aims to design machines that can replicate human intellectual capabilities. Machine learning, on the other hand, is a branch of AI that harnesses algorithms and data to enable systems to evolve and improve without resorting to direct programming. Therefore, any form of machine learning is considered AI, although not all AI systems use machine learning⁴.

However, AI and machine learning are two closely related but distinct areas⁵ :

⇒ AI refers to systems and machines that can perform tasks that usually require human intelligence. This encompasses a variety of technologies, including natural language processing, machine learning, robotics, image recognition, computer vision and many more. The design of an AI system requires the development of machines and algorithms that can acquire knowledge from

¹ **Moustafa ZOUINAR**, « Évolutions de l'Intelligence Artificielle : quels enjeux pour l'activité humaine et la relation Humain-Machine au travail ? », Activités, 17-1/2020, pp.03-07. <https://doi.org/10.4000/activites.4941> (accessed on 03/10/2025.)

² Ibid.

³ **Art. 03 of Regulation (EU) 2024/1689** of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 206/797 and (EU) 2888 (Regulation on Artificial Intelligence), OJEU L 2024/1689 of 12.7.2024.

⁴ **Wassila TERCHA, Sid Ahmed TADJER, Fathia CHEKIRET et Laurent CANALE**, « Machine Learning-Based Forecasting of Temperature and Solar Irradiance for Photovoltaic Systems », Energies, Vol. 17, No. 5 January 2024, p. 1124. [DOI 10.3390/en17051124](https://doi.org/10.3390/en17051124) or <https://www.mdpi.com/1996-1073/17/5/1124> (accessed on 20/08/2025.)

⁵ **Jason BROWNLIE**, « Computing machinery and intelligence », *Mind*, Oxford University Press, Volume LIX, Issue 236, October 1950, pp. 450-455. [DOI 10.1093/mind/LIX.236.433](https://doi.org/10.1093/mind/LIX.236.433) or <https://courses.cs.umbc.edu/471/papers/turing.pdf> (accessed on 22/08/2025.)

data, capture and manipulate human language, interpret visual information, and suggest solutions based on the data provided.

⇒ Machine learning is a branch of artificial intelligence, which focuses on creating algorithms that can evolve and improve over time. This involves instructing machines to acquire knowledge from data, without requiring explicit programming, which gives them the ability to produce predictions based on huge volumes of data.

2- Personal data

Various legal mechanisms guarantee the protection of personal data, including the General Data Protection Regulation (GDPR), which repealed Directive 95/46/EC within the EU, as well as the Council of Europe Convention No. 108 for the Protection of Personal Data. Many countries currently have dedicated authorities for the protection of personal data, usually independent administrative entities (or their equivalents), responsible for the application of the law on the protection of personal data.

Article 04-1 GDPR¹, defines personal data as “ ***any information relating to an identified or identifiable natural person [...]; is deemed to be an “ identifiable natural person “ a natural person 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 to one or more elements specific to his physical, physiological, genetic, psychological, economic, cultural or social identity*** “. This definition is slightly more detailed than that referred to in Article 02 of Directive 95/46/EC, which stated that the individual becomes identifiable ‘in particular by reference to an identification number or to one or more specific elements characteristic of his physical, physiological, psychological, economic, cultural or social identity’”.

Thus, the **art.04/2 of (GDPR)** defines the processing of personal data as “***any operation or set of operations carried out or not carried out using automated processes and applied to personal data or sets of data, such as collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, limitation, erasure or destruction.***”

What you need to know in the light of these articles, whether direct or indirect identification data refers to information that can uniquely identify a person (surname, first name, etc.) or in combination with other data. Therefore, direct identifying

¹ **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**), Official Journal of the European Union L 119/1 of 04/05/2016.

information includes: surname, first name, address and date of birth, whereas indirect identifying information relates to:

- ✓ **Contact information:** phone number, email address;
- ✓ **Online identifiers:** IP address, login ID, cookies;
- ✓ **Physical information:** Photo, Voice, Fingerprint;
- ✓ **Behavioral information:** Geolocation data, browsing habits etc.

In addition, sensitive data reveal racial or ethnic origin, political or religious beliefs, sexuality or health status. In order for information to no longer be considered personal, it must be irreversibly anonymised, which means that the identification of an individual must not be possible.

Second section: The risks generated by AI in the context of personal data protection

AI offers huge benefits while posing real risks. Some of these risks already translate into harm to individuals and businesses, such as prejudice and discrimination, radicalization of views, privacy breaches, and security issues.

1- Lack of transparency: An (AI) model can incorporate millions or even billions of different parameters. Analyzing each parameter separately is complex, as each has an influence on the outcome. Artificial intelligence is based on a wide variety of data, including images, text and information from sensors. The « black box problem » is often referred to as the difficulty of understanding how AI systems make decisions or generate results¹.

For example, a bank uses an artificial intelligence system to analyze its customers' ability to repay their loans. For the reasons mentioned above, the decision-making process is so complex that the bank cannot understand why loans are refused. Thus, the banking staff cannot provide the customer with an explanation for the refusal of his credit request. As a result, customers do not have the opportunity to enter or challenge the decision.

2- Biased training data: To be successful, AI systems need large amounts of data for their learning. The larger the amount of learning data, the less likely it is that all the classes and variations that the model must recognize will actually be present. If data is limited, the AI model may focus excessively on specific cases. If a group is not sufficiently represented, there is a risk that the models will be misinterpreted².

For example, human resources use AI technology to manage the recruitment process. It is trained on data demonstrating historical discrimination against women.

¹ **Kevin BEAUGRAND**, « Pas d'IA de qualité sans une transparence de qualité », article published on 12 May 2025, on the website: <https://www.itforbusiness.fr/pas-dia-de-qualite-sans-une-transparence-de-qualite-91103> (accessed on 24/08/2025.)

² **Corentin BLANC**, « Les biais en machine learning : les données d'entraînement », article published on 28/03/2024, on the website: <https://www.contentside.com/les-biais-en-machine-learning-les-donnees-dentrainement/> (accessed on 23/07/2025.)

This creates an unconscious inclination for male candidates. If men have often been promoted in the past, it may be because women candidates were on maternity leave at that particular time. Artificial intelligence makes an incorrect assumption by considering gender as an indicator of professional success.

3- Infringement of copyright: One of the major legal challenges of artificial intelligence concerns intellectual property. The more data-driven an AI application is the more accurate and efficient it becomes. It is common practice to form the model from publicly available data, such as news articles, for example. However, they are subject to copyright. If artificial intelligence generates content that closely resembles copyrighted works, it could be a copyright infringement¹. For example, a French media company filed a lawsuit against Google, claiming that « Gemini, » its AI-based assistant, was trained from the content of their publication without their prior consent. In March 2023, Google was fined €250 million by the French competition authority². The New York Times is suing Microsoft and OpenAI because ChatGPT was formed with millions of media content³.

4- Profiling and monitoring: Profiling analyzes elements of a person's personality, behavior, interests, and routines to make predictions or determine actions against them. As a result, artificial intelligence can promote new methods of monitoring and tracking people, raising ethical and legal questions about the boundaries of the use of

¹ **Tommaso STELLA**, « Entrainement de l'IA et droit d'auteur : violer pour créer ? », article published on 28/12/2023, on the website: <https://www.village-justice.com/articles/intelligence-artificielle-droit-auteur-entrainement-violer-pour-creer,48301.html> (accessed on 20/08/2025.)

² **Competition Authority (France). Decision 22-D-13 of 21 June 2022** regarding practices implemented in the press sector. pp. 01-68. <https://www.autoritedelaconurrence.fr/sites/default/files/commitments/2022-10/Decision%2022D13%20V%20EN.pdf>

Cases N°19/0074F, 19/0078F AND 19/0080F - Related rights commitments proposal of Alphabet INC, Google LLC, Google Ireland Limited and Google France, 9 May 2022, pp. 01-17. <https://www.autoritedelaconurrence.fr/sites/default/files/attachements/2022-10/Proposition%20d%27engagements%20Google%20EN%20VERSION.pdf>

Competition Authority (France). Decision 21-D-17 of 12 July 2021 on compliance with the injunctions issued against Google in Decision 20-MC-01 of 9 April 2020, pp. 01-127. https://www.autoritedelaconurrence.fr/sites/default/files/attachements/2022-02/21-d-17_en.pdf

Competition Authority (France). Decision 20-MC-01 of 9 April 2020 on requests for interim measures by the French Magazine Publishers Association, the Alliance of the general news press and others and Agency France-Press, pp. 01-72. <https://www.autoritedelaconurrence.fr/sites/default/files/2022-06/20mc01.pdf>

³ **Angela WEISS**, « Le « New York Times » poursuit en justice Microsoft et OpenAI, créateur de ChatGPT, pour violation de droits d'auteur », *Le Monde avec AFP*, article published on December 27, 2023 at 4:13 pm, modified on December 27, 2023 at 4:40 pm, on the website: https://www.lemonde.fr/pixels/article/2023/12/27/le-new-york-times-poursuit-en-justice-microsoft-et-openai-createur-de-chatgpt-pour-violation-de-droits-d-auteur_6207946_4408996.html (accessed on 24/08/2025.)

private data and their exploitation in profiling¹. For example, AI systems can unlawfully scrutinize customer information and behaviors to detect their specific tastes, and thus adjust product suggestions or advertising communications accordingly.

5- Creating deepfakes and false information: AI is capable of producing highly compelling and misleading information or content, including « deepfakes » (fake videos or audios), that could harm the privacy and good reputation of individuals. AI technologies therefore have the ability to generate misleading images or videos that can influence politics and society². For example, they can be used to write propaganda articles that look like they come from a reliable source. In addition, artificial intelligence could be used to generate multiple versions of specific content to improve its visibility and reliability image.

6- Lack of control and consent: In many situations, individuals have very few means to oppose the use of their data by artificial intelligence systems or to properly manage their preferences. Currently, there are very few guidelines for establishing ethical use of AI systems in legislation. How can we oppose something we don't know about? ³.

For example, a mobile application uses artificial intelligence to present customized advertising. The application collects and reviews personal information without the consent of users, and without notifying them. In November 2022, Google was sued in the United States for collecting location information from users while this feature was disabled on the smartphones of the individuals concerned.

7- Transparency and compliance risks: The complexity of algorithms and the volume of data processed by artificial intelligence can make it difficult for users to understand how their information is manipulated, which compromises compliance with informed consent. It can therefore be difficult to determine the liability of developers, users or companies for harm or breach of privacy caused by an AI system⁴.

¹ Antonio MOURUGANDY, « L'intelligence artificielle : une révolution ... sous haute surveillance », article published on 13/03/2025, on the website: <https://www.randstaddigital.fr/fr/actus-et-tendances/articles/blog/blogs/lintelligence-artificielle-une-revolution-sous-haute/> (accessed on 24/08/2025.)

² Romain DAVID, « Intelligence artificielle et fake news, un cocktail qui fait trembler nos démocraties », article published on 10/04/2024 at 07:30, on the website: <https://www.publicsenat.fr/actualites/societe/intelligence-artificielle-et-fake-news-un-cocktail-qui-fait-trembler-nos-democraties> (accessed on 26/08/2025.)

³ Francis DONNAT, « L'intelligence artificielle, un danger pour la vie privée ? », La revue Pouvoirs, 2019/3, N° 170, pp. 98-100. DOI 10.3917/pouv.170.0095 (accessed on 27/08/2025.)

⁴ Sabine MARCELLIN, « IA et données personnelles : question sensible », article published on 15/05/2024, modified on 12/09/2024, on the website: <https://www.village->

8- Data breaches (malicious use): A data breach is defined as a security event during which confidential information has been revealed. Like all computer systems, artificial intelligence systems have security vulnerabilities. Disclosure or theft of data can have severe consequences. According to IBM's « Cost of a Data Breach Report 2022 », a health data breach resulted in an average cost of US\$10.10 million. For the first time, the costs of data protection breaches have crossed the 10 million threshold¹.

For example, a hospital uses artificial intelligence to examine patient information. On the one hand, the absence of certain data can lead to errors in the medical field. Moreover, if hackers manage to steal confidential health information stored in the system, it would violate the privacy of thousands of patients, with the potential for identity theft.

Second requirement: The contributions of the GDPR and the AI regulation (AI Act) and their main complementarities

The General Data Protection Regulation (GDPR) and the European AI Act form the twin pillars of digital regulation in Europe. The GDPR protects individuals' personal data (**first section**), while the AI Act governs the design and use of AI systems according to their level of risk (**second section**). They apply cumulatively (**third section**).

First section: GDPR's contributions to AI

The General Data Protection Regulation (GDPR) is a European legislation, implemented on May 25, 2018, that regulates all technologies handling personal data. It can therefore be inferred that it also applies to advanced AI technologies. The same is true for technologies related to blockchain, connected objects, non-fungible tokens (NFTs) and other nascent innovations. Therefore, the principles and rules established by the GDPR can be applied regardless of the location in question, as long as personal data is manipulated.

However, AI systems often require a large amount of personal data to guarantee their performance. Whether for the development of language models or the implementation of recommendation systems, personal data is crucial. Nevertheless, the (GDPR) imposes strict standards, obliging developers to navigate between utility and privacy preservation.

To better understand the evolution of AI and effectively respond to the challenges it poses, European data protection bodies have launched investigations into certain forms of AI such as ChatGPT or Midjourney. The (CNIL) in France

justice.com/articles/donnees-personnelles-question-sensible,49756.html (accessed on 26/08/2025.)

¹ IBM Security, "Cost of a Data Breach Report 2022", July 2022, pp. 29-43.
<https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf>

released its final notes on AI on July 22, 2025, detailing the criteria for applying the GDPR to models, security requirements and rules regarding the annotation of learning data¹. In fact, the (CNIL) guides the actors in the implementation and recording of the analysis necessary to determine whether the application of their model is governed by the (GDPR) or not. It also offers practical approaches to prevent this application from leading to the processing of personal data, such as the introduction of solid filters at the level of the system encapsulating the model.

Among the main principles of the (GDPR) that AI developers must respect ²:

- 1- **Legality, fairness and transparency:** The collection and processing of data must respect at least one of the bases of legality. Individuals must be clearly and intelligibly informed (Articles 05-09 and 12 of the GDPR). This means that AI systems must ensure transparency in their data management, allowing individuals to capture how their data is used.
- 2- **Purpose limitation:** According to Articles (05) and (18) of the (GDPR), developers are required to specify specific purposes for the use of the data and must not use them for other purposes without a legal justification. In other words, it is imperative to collect personal data only for specific, legitimate and clearly defined purposes. It will not be possible to treat them differently afterwards.
- 3- **Data minimization:** According to Article (05) of the GDPR, personal data must be appropriate, relevant and limited to what is essential for the purposes for which they are processed. This means that only data that is essential to the established objectives must be collected and manipulated.
- 4- **Guaranteeing the security of the development of an AI system:** Article (32) of the GDPR imposes the need to guarantee the security of the processing of personal data. It states that it must be applied taking into account “the current state of knowledge, the costs of implementation, as well as the nature, scale, context and objectives of the processing, not to mention the risks that may vary in terms of probability and severity for the rights and freedoms of individuals”. It is therefore imperative to implement risk-appropriate measures to ensure the safety of the treatment.
- 5- **Accuracy:** According to Art.(05) of the (GDPR), the accuracy of data is a fundamental principle requiring that personal data be accurate, complete and kept up to date to reflect reality. Controllers must take reasonable steps to erase or rectify inaccurate data without delay, and data subjects have a right of

¹ CNIL, « IA : la CNIL finalise ses recommandations sur le développement des systèmes d’IA et annonce ses futurs travaux », 22/07/2025. <https://www.cnil.fr/fr/ia-finalisation-recommandations-developpement-des-systemes-ia> (accessed on 26/08/2025.)

² For more information, see: La CNIL-France, « IA et RGPD : la CNIL publie ses nouvelles recommandations pour accompagner une innovation responsable », published on 07/02/2025 on the website : <https://www.cnil.fr> (accessed on 25/08/2025.)

rectification to correct or supplement their information, thus avoiding erroneous decisions and damages.

- 6- Limitation of retention:** Information of inactive individuals may not be retained beyond 36 months, unless anonymized. According to Article (05) of the (GDPR), a consent request must be made every thirteen (13) months.
- 7- Integrity and confidentiality:** The (GDPR) emphasizes protection as a crucial point. It is the responsibility of the data controller to ensure their security and confidentiality. (Arts. 05 and 25 of GDPR). To this end, the (GDPR) requires that personal data be accurate, complete and unmodified, while guaranteeing their confidentiality (access limited to authorize persons). Companies are therefore required to implement technical and organizational measures (encryption, access management, and training) commensurate with the risks in order to ensure security throughout the lifetime of the data. In the event of non-compliance, they are liable to penalties. This is a key element in defending people against unauthorized access and offenses.
- 8- Transfer of data by AI systems outside the EU:** According to the (GDPR), a comparable level of protection to that in the (EU) is required, either through an adequacy decision (as is the case for the (US) with the Data Privacy Framework)¹, or by using appropriate safeguards such as standard contractual clauses or Binding Corporate Rules (BCR). Without these conditions, transfers are prohibited, apart from certain specific exceptions mentioned in Article (49) of the GDPR. In addition, a Data Transfer Impact Assessment (DTIS) must be carried out.

Second section: The contributions of the European AI Regulation (AI Act)

On June 3, 2024, the European AI Regulation was adopted. Its aim is to establish an evolving regulatory framework for these technologies and to foster responsible AI innovation in the European Union, while safeguarding fundamental rights and values.

This regulation distinguishes two (02) major families of AI systems² :

- a. Specific-purpose AI systems**, where risk is assessed according to their specific use case (e.g. recruitment, credit, education, justice, etc.).
- b. General Purpose AI (GPAI) models**, they are treated separately because of their potential to be reused in a wide range of contexts, often difficult to predict³.

¹ For more information on the subject, see the following website: <https://www.dataprivacyframework.gov/Program-Overview> (accessed on 20/08/2025.)

² Richard EUDES, Nicolas FLEURET, « EU AI Act : comprendre le premier cadre réglementaire sur l'intelligence artificielle », article published on 23/06/2025 on the website : <https://www.deloitte.com/fr/fr/our-thinking/explore/tech/EU-AI-Act.html> (accessed on 18/08/2025.)

³ For more information, see the arts. 53-55 of AI Act.

For systems with a specific objective, the level of risk determines the specific obligations applicable. Four categories have been established ¹.

1- Unacceptable risk

Article (05) of the AI Act defines prohibited practices for determining whether an AI system falls into this category. E.g. Social scoring, behavioral manipulation, facial or emotional recognition in schools or the workplace, etc ².

2- High risk

Article (06) of the (AI Act), sets out the rules for the classification of AI systems as high risk. In order to determine whether the AI system falls into this category, it should be clarified whether that system is intended to be used as a **safety component of a product** or whether the **AI system itself as a product** is subject to a third-party conformity assessment for the placing on the market or putting into service of that product in accordance with the Union harmonization legislation listed in **Annex I**, such as: *machinery, toys, safety devices, cars, etc.*, or do AI systems fall within any of the specific sectors listed in **Annex III to the AI Act**, such as: *essential public and private services, biometrics, digital, traffic, health, justice, combating crime, etc.* However, the AI system listed in **Annex III** is not considered to be highly risky, if it does not present any significant risk to *health, safety or harm rights fundamental rights of natural persons, including those that do not have a significant impact on the outcome of decision-making*³.

3- Limited risk

Although the concept of ‘limited risk’ systems is not clearly defined, the AI Act imposes specific transparency obligations referred to in Article (50), which must be met by 02/08/2026. To determine whether the AI system is subject to it, it must be determined whether the system is intended to interact directly with natural persons (Chabot, etc.), or the AI is capable of generating video, audio, image or text content, or the AI is capable of recognizing emotions or performing a biometric classification of persons, or the AI is capable of generating deepfakes⁴.

¹ Guillaume AVRIN, « Qu'est-ce que l'« AI Act » ? », article published on may 24, 2024, modified on June 4, 2025, on the website : <https://www.info.gouv.fr/actualite/quest-ce-que-lai-act> (accessed on 01/09/2025.)

² For more information, see the art. 05 of AI Act.

³ Art.03 of AI Act: “ For the purposes of this Regulation, the following definitions apply: [...] ; 2) ‘risk’ means the combination of the probability of an occurrence of harm and the severity of that harm; [...] ; [...] ; 14) ‘safety component’ means a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property; [...].”

For more information, see the arts. 06-27, 43-49 of AI Act.

⁴ For more information, see the art. 50 of AI Act.

4- Minimum risk

No specific obligations, but the possibility of voluntary adherence to codes of conduct, in accordance with Article (56) of the (AI Act).

This classification makes it possible to target regulation where it is most needed, without hindering innovation in low-impact uses¹.

Third section: The main complementarities between the (GDPR) and the (AI Act)

It is rare to find an area that has not benefited from the evolution of artificial intelligence, and such rapid progress could not be achieved without prompt supervision to guarantee the rights and freedoms of individuals. In addition, the coexistence of the two legal texts (GDPR and AI Act) offers an exceptional opportunity for the (EU) to distinguish itself in the development of ethical AI, while providing companies with the opportunity to create cutting-edge technologies while safeguarding people's fundamental rights. To this end, the main gaps and complementarities between the (GDPR) and the (AI Act) can be summarized as follows:

- 1- The (GDPR) encompasses all personal data and focuses on individual rights and data processing, while the (AI Act) focuses more on the risks associated with AI systems and focuses on the lifecycle of these systems and their possible repercussions (discrimination, bias, etc.)² ;
- 2- The GDPR aims to protect personal data (privacy, consent, transparency), while the IA Act manages AI systems according to their level of risk, thus strengthening the GDPR with specific rules for ethical, secure and transparent AI. In particular, it requires human control and imposes strict standards for AIs considered to be high risk, while pursuing common objectives of protecting rights and freedoms³ ;

¹ For more information, see the arts. 56-59 of AI Act.

² See: the arts.02, 03 of GDPR, and 02 of AI Act.

³ Art. 01 of (GDPR):” ‘Subject-matter and objectives’

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. 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. 01 of (AI Act): “ ‘Subject matter’

1. The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation.

- 3- Both the General Data Protection Regulation and the European Artificial Intelligence Regulation (AI Act) establish systems of accountability, governance and control. Nevertheless, they have distinct roles within the framework of AI-related regulatory objectives¹;
- 4- The main purpose of the GDPR is to safeguard personal data and does not specifically mention particular technologies, such as artificial intelligence. It is applicable whenever an entity, located within the European Union or in a third country under the conditions stipulated in Article 3(2) of the GDPR, processes personal data, whether through artificial intelligence or otherwise²;
- 5- The AI Act recognizes that the use of AI raises broader ethical and societal issues, which go beyond the limits of the GDPR. For example, some methods using AI or machine learning may reproduce cultural biases or discriminatory behavior, or create security risks³.

2. This Regulation lays down: (a) harmonized rules for the placing on the market, the putting into service, and the use of AI systems in the Union;
(b) prohibitions of certain AI practices;
(c) specific requirements for high-risk AI systems and obligations for operators of such systems;
(d) harmonized transparency rules for certain AI systems;
(e) harmonized rules for the placing on the market of general-purpose AI models;
(f) rules on market monitoring, market surveillance, governance and enforcement;
(g) measures to support innovation, with a particular focus on SMEs, including start-ups.”

¹ See: the Arts.10 and 25 of (AI Act), and 24-34, 41 of (GDPR).

² Art. 03: “[...]. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behavior as far as their behavior takes place within the Union. [...].“

³ Julien LAUSSON, « *Minime à inacceptable : l'Europe définit quatre niveaux de risques pour l'IA* », article published on April 23, 2021 at 4:16 pm on the website: <https://www.numerama.com/tech/706461-minime-a-inacceptable-leurope-definit-quatre-niveaux-de-risques-pour-lia.html> (accessed on 01/09/2025.)

Alex McFARLAND, « *Disséquer la loi sur l'intelligence artificielle de l'UE : implications et réaction de l'industrie* », article published on 25/05/2023 on the website: <https://www.unite.ai/fr/diss%C3%A9quer-les-implications-de-la-loi-eus-sur-l'intelligence-artificielle-et-la-r%C3%A9action-de-l'industrie/> (accessed on 01/09/2025.)

THE SECOND TOPIC:

The legal responsibility of AI actors and the opportunities of AI for data protection

The regulation of artificial intelligence in Europe is undergoing a major turning point with the gradual implementation of the EU AI Act. Legal liability is becoming clearer, distinguishing suppliers from users, while AI paradoxically becomes a key tool for compliance and personal data protection (GDPR). In addition, AI presents risks (profiling, bias), and offers new ways to strengthen GDPR compliance.

First requirement: The legal liability of AI actors under the IA Act and the GDPR

The legal responsibility of AI actors rests on the dual requirements of the AI Act (which regulates AI systems according to their risk level) and the GDPR (which protects personal data) (**first section**). However, joint responsibility arises when two or more entities jointly determine the purposes (objectives) and means of processing personal data (**second section**). Conversely, a data processor acts solely on the instructions and on behalf of the data controller, without deciding on the purposes (**third section**).

First section: Actors' liability for damage caused by AI

The (ACT AI) identifies various systems based on a risk-based approach: prohibited AI systems (AIS), high-risk (AIS), and other (AIS) with specific and negligible risks. If personal data is used by (AIS), the regulations of the (IA ACT) and the (GDPR) apply to both the designers and suppliers and the users of these (AIS). However, neither the (AI Act) nor the (GDPR) explicitly state how to implement the principles of civil or criminal liability, but they do establish a foundation for joint responsibility between developers and AI users.

To this end, actors involved in the AI sector must ensure their compliance with the (GDPR) criteria. Depending on the situation, they may be referred to as controllers, joint controllers or processors, which would significantly influence their duties.

In addition, the attribution of legal status to stakeholders under the (GDPR) must be done individually, considering not only the framework of the implementation of AI systems (AIS), but also the distinctive role of each in the initiative, structure and execution of the data processing integrated into these systems. This assessment also considers each AI-related transaction, which allows multiple (GDPR), (AI Act) statuses to be applied simultaneously to the same actor. An actor may simultaneously assume the role of controller for certain operations and that of subcontractor for others.

Second section: Responsibility of the controller and the joint controllers

If the software or algorithm developer has used the collected data to develop models or optimize the performance of the artificial intelligence system without complying with personal data protection standards, it may be held liable for the processing of such information¹.

If personal data is used by the AI system, the General Data Protection Regulation (GDPR) requires AIS creators and suppliers (distributors) to collect process, and protect such data responsibly while respecting the privacy of individuals. In other words, the developer and the supplier will be required to comply with the principles of the (GDPR).

It should be noted that the controller is defined as the one who determines the purposes and procedures of the data processing².

Where a number of controllers feed into the learning database of an artificial intelligence system for the purpose of achieving a commonly defined objective, they could be classified as joint controllers within the meaning of article (26) of the (GDPR)³.

To this end, the French data protection authority (CNIL) recommends distinguishing between the data controller, who facilitates access to personal data for reuse, and the user, who uses the data for their own purposes, within the context of reusing data collected by another company. Generally, these companies will assume

¹ Olivier CHAPUIS, « Responsabilité juridique des fabricants d'IA embarquée: enjeux, limites et perspectives », article published on 14/07/2025, on the website : <https://www.annabellebourgavocat.fr/responsabilite-juridique-des-fabricants-dia-embarquee-enjeux-limites-et-perspectives/> (accessed on 27/08/2025.)

² Art. 04 of (GDPR): "For the purposes of this Regulation: [...]; (7) 'controller' means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; [...]."

³ For more informations, see the arts. 26, 27 of (GDPR) and 25, 26 of (AI Act).

responsibility for carrying out separate processing operations, as they will determine the purposes and methods of their own processing¹.

Third section: The responsibility of the user of the AI tool (Processor)

Reckless use of AI by the user could potentially make them liable as a data controller or processor, especially if they misinterpret the results or do not check the AI suggestions before they are implemented. Therefore, this user could be subject to negligence lawsuits if he causes damage through his reckless use of AI².

According to Article 04-8 of the GDPR, the **processor** is described as the one who processes personal data on behalf of the controller. Thus, its functions are limited to the instructions given by the controller, usually included in a data protection contract. For example, if a processor wishes to hire another processor, it must obtain prior written authorization, specific or general, from the controller. If a general written authorization is granted, the processor is required to notify its controller of any planned changes relating to the addition or replacement of other processors. This gives the controller the opportunity to raise objections against these changes.

It will be crucial to pay particular attention to the level of autonomy of the processor and the assurances it provides in terms of data protection and confidentiality (Art. 32 of GDPR). It is imperative that the data protection agreement is formulated with careful precision, as the precise definition of roles and limits will have significant implications for various strategic aspects such as the ability to exploit the data generated by the use of the service, or the responsibility for the compliance of the AI system(AIS) concerned³.

¹ CNIL : « Ouverture et réutilisation de données personnelles sur Internet : la CNIL publie ses recommandations », June 12, 2024. Available on the website: <https://www.cnil.fr/fr/ouverture-et-reutilisation-de-donnees-personnelles-sur-internet-la-cnil-publie-ses-recommandations> (accessed on 25/08/2025.)

² Manon HOTTIN, « Intelligence artificielle et protection des données personnelles : entre opportunités et conformité », article published on 15/11/2024, modified on 18/11/2024, on the website : <https://www.village-justice.com/articles/intelligence-artificielle-protection-des-donnees-personnelles-entre,51446.html> (accessed on 27/08/2025.)

Adrien BASDEVANT, Aurélie JEAN, et Victor Strachan, « IA : « Les acteurs techniques doivent travailler avec les acteurs de la justice », article published on 15/09/2021 at 10:30, on the website: <https://www.actu-juridique.fr/professions/intelligence-artificielle-les-acteurs-techniques-doivent-travailler-avec-les-acteurs-de-la-justice/> (accessed on 30/08/2025.)

³ Éric A. CAPRIOLI, « Économie des données et intelligence artificielle : un ensemble contractuel complexe », article published on 16/11/2022, on the website : <https://www.caprioli-avocats.com/fr/informations/economie-des-donnees-et-intelligence-artificielle--un-ensemble-contractuel-complexe---innovation-21-336-0.html> (accessed on 31/08/2025.)

Art. 28 of GDPR: “‘Processor’ 1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate

Second requirement: The opportunities of AI for data protection

To remain competitive, companies implement artificial intelligence solutions to optimize their processes (**first section**). In this context, they must follow data protection rules to avoid any legal risk and ensure their compliance both technically and legally (**second section**). It is therefore imperative that developers develop AI systems (AIS) that comply with current data protection rules, as harmony between

technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations. [...].”

innovation and data backup is essential to ensure the sustainability and stability of the company (**third section**).

First section: Improved data security

Artificial intelligence can improve data security by detecting and responding quickly to threats. AI has the ability to identify abnormal and suspicious behaviors in accessing information, allowing for a rapid response to cyber attacks. This helps companies comply with data security standards set out in the (GDPR) and the (AI Act)¹.

Second section: Automation of compliance processes

Artificial intelligence can automate various operations related to (GDPR) and (AI Act) compliance, such as processing consents, responding to requests from data subjects and managing data processing registers. This reduces the administrative burden on businesses while improving compliance efficiency².

Third section: Predictive analysis for risk management

AI can be used to perform predictive analytics, identifying areas with potential data protection risk. By anticipating risks and vulnerabilities, companies are able to implement preventive measures to protect private data, thereby adhering to the standards of the (GDPR) and the AI law³.

¹ CNIL(France), «Sécurité : Piloter la sécurité des données », article published on 14/03/2024 on the website : <https://www.cnil.fr/fr/securite-piloter-la-securite-des-donnees> (accessed on 02/09/2025.)

² Stéphanie BIRON, « Veille réglementaire : comment anticiper et assurer votre conformité grâce à l'IA ? », article published on 14/04/2025 on the website : <https://www.auxodynamics.com/blog/veille-reglementaire-comment-anticiper-et-assurer-votre-conformite-grace-a-lia> (accessed on 02/09/2025.)

³ Julien KARACHEHAYAS, « IA prédictive : comment exploiter vos données mieux piloter l'activité de l'entreprise », article published on 08/08/2025 on the website: <https://www.francenum.gouv.fr/guides-et-conseils/intelligence-artificielle/analyse-et-exploitation-des-donnees-metiers-avec-lia-4> (accessed on 02/09/2025.)

Thomas BLANC, « Comment l'IA est-elle utilisée dans la protection des données », article published on 07/01/2025 from the following address : <https://donnees.net/comment-lia-est-elle-utilisee-dans-la-protection-des-donnees> (accessed on 02/09/2025.)

See also: Art.27 of (AI Act) and 35 of (GDPR).

Conclusion:

In light of this study, we conclude that AI compliance refers to the framework of rules, laws and ethical standards that an AI system must adhere to in order to operate in a fair, secure and legislated manner. This approach aims to ensure the preservation of individual rights, the protection of private data and the integrity of systems, in particular under the authority of the European (AI Act) which imposes standards of transparency, risk management and supervision of AI. Compliance requires risk assessment, proper governance, and the safeguarding of personal data (GDPR), with timelines and requirements that vary depending on the level of AI risk.

To this end, the (AI Act) does not replace the (GDPR), but presents itself as a complement that requires criteria for the creation and implementation of trustworthy artificial intelligence systems. The (GDPR) applies to all processing of personal data, and during the development and implementation phase of an information system containing personal data.

In addition, the (AI Act) refers to the design, marketing or integration of artificial intelligence systems and models, while the (GDPR) is applicable to all processing of personal data. Then, the (IA Act) takes a risk-based approach while the (GDPR) is based on the application of fundamental principles, risk assessment and liability.

However, striking a balance between the use of artificial intelligence systems and compliance with data protection rules in these AI systems is a major challenge in our ever-changing digital society. While AI can improve efficiency and spur innovation, it also raises legitimate concerns about privacy and the protection of personal data. It is therefore essential for companies and organizations to take a proactive approach by integrating data protection principles at the design stage of their AI system (AIS), including through the implementation of forms and conformity assessments. This proactive approach requires not only the establishment of strict processes within the entity, but also increased user awareness.

When it comes to responsibility in the AI era, humans are still in a position of decision-making power over AI as an object, because they are the ones who designed it. It will therefore be held liable in case of damage. Therefore, various liability regimes may be relevant to AI actors in addition to the (AI Act) and the (GDPR) depending on the context. This includes in particular, general civil liability law Council Directive 85/374/EEC of 25 July 1985 on liability for defective products, and Regulation 2022/1426 on the approval of automated vehicles, etc.

Indeed, the issue of liability for the use of AI is particularly complex particularly, in terms of contractual law. A company can be held liable if an AI system (AIS) it has implemented causes harm. In addition, it can be difficult to establish liability if the error stems from AI machine learning rather than human negligence. Moreover, in the context of tort law, lawyers question the possibility of considering AI as a « third party » with regard to tort liability, given that its decisions

result from its autonomous development and not from an identifiable programming failure.

Finally, we submit to the Algerian legislator a series of recommendations to better regulate the use of artificial intelligence systems:

- 1- Establish legislation that regulates the use of AI by establishing requirements related to transparency, accountability and data protection, while providing penalties for non-compliance;
- 2- Training judges in new technologies is essential to ensure legal protection for litigants, as AI is a constantly evolving field.
- 3- The storage of personal data in the context of AI requires global cooperation. Partnerships with other countries and international entities are crucial to share best practices, share experiences and share efforts on common challenges.
- 4- Establish a specific liability regime for AI to facilitate redress for victims, as current liability rules are not fully effective in AI;
- 5- Easing the burden of proof for AI victims by establishing a rebuttable presumption of causation in the event of fault, thus relieving victims of the obligation to demonstrate the nature of the fault or omission causing the damage;
- 6- Establish a procedure to simplify access to evidence held by companies or suppliers, which would allow victims to request a court to order the disclosure of information related to AI systems.

Bibliography List:

A- Journal article:

1. Francis DONNAT, « L'intelligence artificielle, un danger pour la vie privée ? », revue Pouvoirs, 2019/3, N° 170, pp. 95-103. DOI 10.3917/pouv.170.0095 (accessed on 27/08/2025.)
2. Jason BROWNE, « Computing machinery and intelligence », *Mind*, Oxford University Press, Volume LIX, Issue 236, October 1950, pp. 433-460. DOI 10.1093/mind/LIX.236.433 or <https://courses.cs.umbc.edu/471/papers/turing.pdf> (accessed 22/08/2025.)
3. Moustafa ZOUINAR, « Évolutions de l'Intelligence Artificielle : quels enjeux pour l'activité humaine et la relation Humain-Machine au travail ? », *Activités*, 17-1/2020, pp.01-39. <https://doi.org/10.4000/activites.4941> (accessed on 03/10/2025.)
4. Wassila TERCHA, Sid Ahmed TADJER, Fathia CHEKIRE and Laurent CANALE, « Machine Learning-Based Forecasting of Temperature and Solar Irradiance for Photovoltaic Systems », *Energies* 2024, 17(5), p. 1124. DOI : 10.3390/en17051124 or <https://www.mdpi.com/1996-1073/17/5/1124> (accessed on 20/08/2025.)

B- Internet websites:

1. Adrien BASDEVANT, Aurélie JEAN, et Victor Strachan, « IA : « Les acteurs techniques doivent travailler avec les acteurs de la justice », article published on 15/09/2021 at 10:30, on the website: <https://www.actu-juridique.fr/professions/intelligence-artificielle-les-acteurs-techniques-doivent-travailler-avec-les-acteurs-de-la-justice/> (accessed on 30/08/2025.)
2. Alex McFARLAND, « Disséquer la loi sur l'intelligence artificielle de l'UE : implications et réaction de l'industrie », article published on 25/05/2023 on the website : <https://www.unite.ai/fr/diss%C3%A9quer-les-implications-de-la-loi-eus-sur-l'intelligence-artificielle-et-la-r%C3%A9action-de-l'industrie/> (accessed on 01/09/2025.)
3. Angela WEISS, « Le « New York Times » poursuit en justice Microsoft et OpenAI, créateur de ChatGPT, pour violation de droits d'auteur », *Le Monde avec AFP*, article published on December 27, 2023 at 4:13, modified on december 27, 2023 at 4:40 pm, on the website: https://www.lemonde.fr/pixels/article/2023/12/27/le-new-york-times-poursuit-en-justice-microsoft-et-openai-createur-de-chatgpt-pour-violation-de-droits-d-auteur_6207946_4408996.html (accessed on 24/08/2025.)
4. Antonio MOUROUGANDY, « L'intelligence artificielle : une révolution ... sous haute surveillance », article published on 13/03/2025, on the website : <https://www.randstadigital.fr/fr/actus-et-tendances/articles/blog/blogs/lintelligence-artificielle-une-revolution-sous-haute/> (Accessed on 24/08/2025.)
5. CNIL-France, « IA : la CNIL finalise ses recommandations sur le développement des systèmes d'IA et annonce ses futurs travaux », published on 22/07/2025. <https://www.cnil.fr/fr/ia-finalisation-recommandations-developpement-des-systemes-ia> (accessed on 26/08/2025.)

6. CNIL-France, « IA et RGPD : la CNIL publie ses nouvelles recommandations pour accompagner une innovation responsable », published on 07/02/2025 on the website : <https://www.cnil.fr> (accessed on 25/08/2025.)
7. Cole STRYKER, Eda KAVLAKOGLU, « Qu'est-ce que l'intelligence artificielle (IA)? », article published on 16/08/2024, from the following address : <https://www.ibm.com/fr-fr/topics/artificial-intelligence> (accessed on 16/03/2025.)
8. Corentin BLANC, « les biais en machine learning: les données d'entraînement », article published on 28/03/2024, on the website: <https://www.contentside.com/les-biais-en-machine-learning-les-donnees-dentrainement/> (accessed on 23/07/2025.)
9. Éric A. CAPRIOLI, « Économie des données et intelligence artificielle : un ensemble contractuel complexe », article published on 16/11/2022, on the website : <https://www.caprioli-avocats.com/fr/informations/economie-des-donnees-et-intelligence-artificielle-un-ensemble-contractuel-complexe---innovation-21-336-0.html> (accessed on 31/08/2025.)
10. Frédéric ALEXANDRE, « Marvin Minsky : l'intelligence artificielle débraillée », 2016, pp. 01-03. HAL Id: hal-01402261 ou <https://inria.hal.science/hal-01402261v1> (accessed on 03/10/2025.)
11. Guillaume AVRIN, « Qu'est-ce que l'« AI Act » ? », article published on May 24, 2024, modified on June 4, 2025, on the website: <https://www.info.gouv.fr/actualite/quest-ce-que-lai-act> (accessed on 01/09/2025.)
12. IBM Security, “Cost of a Data Breach Report 2022”, July 2022, pp. 01-58. <https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf>
13. Julien LAUSSON, « *Minime à inacceptable : l'Europe définit quatre niveaux de risques pour l'IA* », article published on April 23, 2021 at 4:16, on the website : <https://www.numerama.com/tech/706461-minime-a-inacceptable-leurope-definit-quatre-niveaux-de-risques-pour-lia.html> (accessed on 01/09/2025.)
14. Kevin BEAUGRAND, « pas d'IA de qualité sans une transparence de qualité », article published on May 12, 2025, on the website : <https://www.itforbusiness.fr/pas-dia-de-qualite-sans-une-transparence-de-qualite-91103> (accessed on 24/08/2025.)
15. Manon HOTTIN, « Intelligence artificielle et protection des données personnelles : entre opportunités et conformité », article published on 15/11/2024, modified on 18/11/2024, on the website : <https://www.village-justice.com/articles/intelligence-artificielle-protection-des-donnees-personnelles-entre,51446.html> (accessed on 27/08/2025.)
16. Olivier CHAPUIS, « Responsabilité juridique des fabricants d'IA embarquée: enjeux, limites et perspectives », article published on 14/07/2025, on the website : <https://www.annabellebourgavocat.fr/responsabilite-juridique-des-fabricants-dia-embarquee-enjeux-limites-et-perspectives/> (accessed on 27/08/2025.)
17. Richard EUDES, Nicolas FLEURET, « EU AI Act : comprendre le premier cadre réglementaire sur l'intelligence artificielle », article published on 23/06/2025 on the website : <https://www.deloitte.com/fr/fr/our-thinking/explore/tech/EU-AI-Act.html> (accessed on 18/08/2025.)
18. Romain DAVID, « Intelligence artificielle et fake news, un cocktail qui fait trembler nos démocraties », article published on 10/04/2024 at 07:30, on the website :

<https://www.publicsenat.fr/actualites/societe/intelligence-artificielle-et-fake-news-un-cocktail-qui-fait-trembler-nos-democraties> (accessed on 26/08/2025.)

19. Sabine MARCELLIN, « IA et données personnelles : question sensible », article published on 15/05/2024, modified on 12/09/2024, on the website : <https://www.village-justice.com/articles/donnees-personnelles-question-sensible,49756.html> (accessed on 26/08/2025.)
20. Tommaso STELLA, « entraînement de l'IA et droit d'auteur : violer pour créer ? », article published on 28/12/2023, on the website: <https://www.village-justice.com/articles/intelligence-artificielle-droit-auteur-entrainement-violer-pour-creer,48301.html> (accessed on 20/08/2025.)

C- Legal texts:

1. 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), OJEU L 119/1 of 04/05/2016.
2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJEU L 2024/1689 of 12/7/2024.

IV- Various:

1. Competition Authority (France). Decision 20-MC-01 of 9 April 2020 on requests for interim measures by the Syndicat des éditeurs de la presse magazine, the Alliance de la presse d'information générale and others and Agence France-Presse, pp. 01-72. <https://www.autoritedelaconurrence.fr/sites/default/files/2022-06/20mc01.pdf>
2. Competition Authority (France). Decision 21-D-17 of 12 July 2021 on compliance with the injunctions issued against Google in Decision 20-MC-01 of 9 April 2020, pp. 01-127. https://www.autoritedelaconurrence.fr/sites/default/files/attachments/2022-02/21-d-17_en.pdf
3. Competition Authority (France). Decision 22-D-13 of 21 June 2022 regarding practices implemented in the press sector. pp. 01-68. <https://www.autoritedelaconurrence.fr/sites/default/files/commitments/2022-10/Decision%2022D13%20V%20EN.pdf>
4. Cases N°19/0074F, 19/0078F AND 19/0080F - Related rights commitments proposal of Alphabet INC, Google LLC, Google Ireland Limited and Google France, 9 May 2022, pp. 01-17. <https://www.autoritedelaconurrence.fr/sites/default/files/attachments/2022-10/Proposition%20d%27engagements%20Google%20EN%20VERSION.pdf>