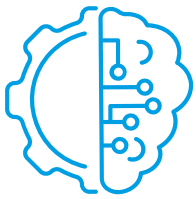


ARTIFICIAL INTELLIGENCE

European legislation and legal issues

GIDE

GIDE LOYRETTE NOUEL

FOREWORD

With the development of artificial intelligence –and of generative artificial intelligence in particular–, it would seem that a new technological revolution is upon us. Beyond the increasingly widespread questions as to the practical implementation of such technology, we feel it is important to consider the legal implications that it may entail through the prism of our profession, and more specifically, of the leading law firm that is Gide. In its constant quest for excellence spanning over a century, Gide has been providing its clients with a highly acute understanding of the issues that shape the future of French and European business law.

Artificial intelligence per se is not quite a novelty. Already widely present in our daily lives, smartphones, office automation platforms and solutions, the European Union is now working on regulating it.

Following the political agreement reached on December 8, 2023 between the co-legislators (the Council of the European Union and the European Parliament), the permanent representatives of the Member States, who met on February 2, 2024 unanimously approved the proposal for a European regulation on artificial intelligence (as amended by the political agreement). The proposal was also approved in identical terms by a joint vote of the European Parliament's IMCO and LIBE committees on February 13, 2024. The adoption of European legislation on artificial intelligence therefore seems imminent; this would be the first-ever comprehensive legal framework on artificial intelligence worldwide.

Spearheaded by Gide 255, this Booklet is the fruit of cross-disciplinary work carried out in conjunction with all of Gide's practice groups, under the supervision of its Scientific Council and in close collaboration with the Knowledge Management team.

With this Booklet, our ambition is to provide readers far and wide with free access to thorough insight on the major orientations of future European legislation and the legal issues raised by AI.

Part 1 of the Booklet presents the future European legal framework for AI (origin, philosophy and key points), as well as the European AI Office, i.e. the first body having monitoring and sanctioning powers to enforce binding rules on AI, with varying constraints based on the risk profile (high or low) for humans. In doing so, the European Union's goal is clear: embrace the advent of AI in the business world, while guaranteeing the safety and fundamental rights of people and businesses. It is imperative that AI remain a human-centric technology and to make sure that humans retain the upper hand at all times.

Part 2 of the Booklet calls upon Gide's manifold and cross-disciplinary skills. The legal issues raised by AI are examined in the light of ten fields: intellectual property and personal data; competition law; banking and finance; insurance law; mergers and acquisitions; arbitration; real estate; labor law; and environmental law.

Naturally, this Booklet is not set in stone, given the constantly evolving nature of artificial intelligence. We will be sure to update our analysis in future editions. In the meantime, we hope you will enjoy this first edition of what we trust is a comprehensive insight of what's to come.

Philippe Dupichot

Professor at Université Paris I (Panthéon-Sorbonne)
Head of Gide's Scientific Council

Emilie Leygonie

Associate, KM & Documentation Manager

CONTENTS

01 EUROPEAN LEGISLATION

1.1 INTRODUCTION

Author:
Thierry Bonneau - *Senior Counsel*

Genesis

The genesis of the notion of artificial intelligence ("**AI**") is a subject of debate. Some trace it back to the founding fathers of information technology[1]. Others believe the expression was coined by Johan McCarty and Marvin Minsky, during a lecture given at the Dartmouth College in the summer of 1956[2].

The use of the words "artificial" and "intelligence" may come as a surprise, as the notion of AI refers to machines and robots. "Man, whose intelligence was believed to be the distinguishing mark, the mark of nobility, has conceded this quality to a digital interface, a machine"[3].

AI refers to a robot's acquisition of human cognitive skills, and therefore of human knowledge and reasoning abilities.

What is AI?

There are many forms of AI. Different approaches have been proposed. If we simplify the oppositions, it is possible to distinguish two forms of AI[4]:

- a so-called weak AI, "where it is possible to conceive that reasoning per se is not necessary, and that the machine merely translates innate animal-like reactions into a form of symbolic representation"[5];
- a so-called strong AI, "where it is possible to conceive that the full range of human intellectual capacities can be reproduced, as the machine can learn from statistical data and thus go beyond the initial symbolic representation"[6].

From this perspective, AI is "a process by which an algorithm evaluates and improves its performance without human intervention"[7]: it designates a "self-learning mechanism"[8].

AI comprises two essential elements: an algorithm, on the one hand, and data, on the other hand[9]. The algorithm is "the description of a finite and unambiguous sequence of steps (or instructions) for producing results (output) from initial data (input)"[10]. Data is "information in digital form that can be transmitted or processed" by a computer (Merriam-Webster dictionary definition). In light of these elements, AI can be defined as "a computer system based on an algorithm endowed with cognitive capacities developed with the help of data, enabling it to be autonomous in the choices it makes and the decision-making it carries out"[11].

> ***Decision autonomy is one of the essential features of AI. Learning on the basis of the data provided is another, even though it is not the very essence of AI***
> (Ibid spéc. n°2).

In 2017, the Financial Stability Board (FSB) defined AI "as the theory and development of computer systems able to perform tasks that traditionally have required human intelligence. AI is a broad field, of which 'machine learning' is a sub-category. Machine learning may be defined as a method of designing a sequence of actions to solve a problem, known as algorithms, which optimize automatically through experience and with limited or no human intervention"[12].

This approach was taken into account by the European Union ("**EU**") in its White Paper published in 2020: "AI can perform many functions that previously could only be done by humans" (Ibid p 13) and in the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (AI Act) and amending certain Union legislative acts adopted by the Commission on April 21, 2021 (hereafter "**Proposal for an AI Act**"[13]).

To ensure that the definition of an AI system provides criteria that is precise enough to distinguish AI from simpler software systems, the compromise agreement reached by the EU institutions on December 8, 2023 aligns the definition with the approach proposed by the Organization for Economic Cooperation and Development ("**OECD**") (see Section 1.2 p. 10).

1 P. Bessières, L'IA a connu des vagues successives d'enthousiasme, Hors-série Banque & droit, octobre 2019 p 4.
2 E. Jouffin, Faut-il redouter l'IA?, Hors-série Banque & droit, octobre 2019 p 7.
3 M. Teller, Ethique et IA : un préambule pour un autre droit, Hors-série Banque & droit, octobre 2019 p 38.
4 N. Martial-Braz, L'apport de l'intelligence artificielle à la banque, Enjeux et contraintes en matière de données à caractère personnel, Rev. dr. bancaire et financier nov-déc. 2019, Dossier 53.
5 Ibid spéc. n°1
6 Ibid.
7 Ibid.
8 Ibid.
9 Ibid spéc. n° 2.
10 CNIL (Commission nationale de l'informatique et des libertés - French Data Protection Authority), report How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence, December 2017, spéc. p 5.
11 Martial-Braz, L'apport de l'intelligence artificielle à la banque, Enjeux et contraintes en matière de données à caractère personnel, préc. spéc. n° 2.
12 FSB, Artificial intelligence and machine learning in financial services. Market development and financial stability implications, 1er novembre 2017, spéc. pp. 4 et 35.
13 References in this document to the Proposal for an AI Act may, where appropriate, incorporate amendments made in the course of negotiations between the European institutions to finalize the text.

Which business sectors and which players?

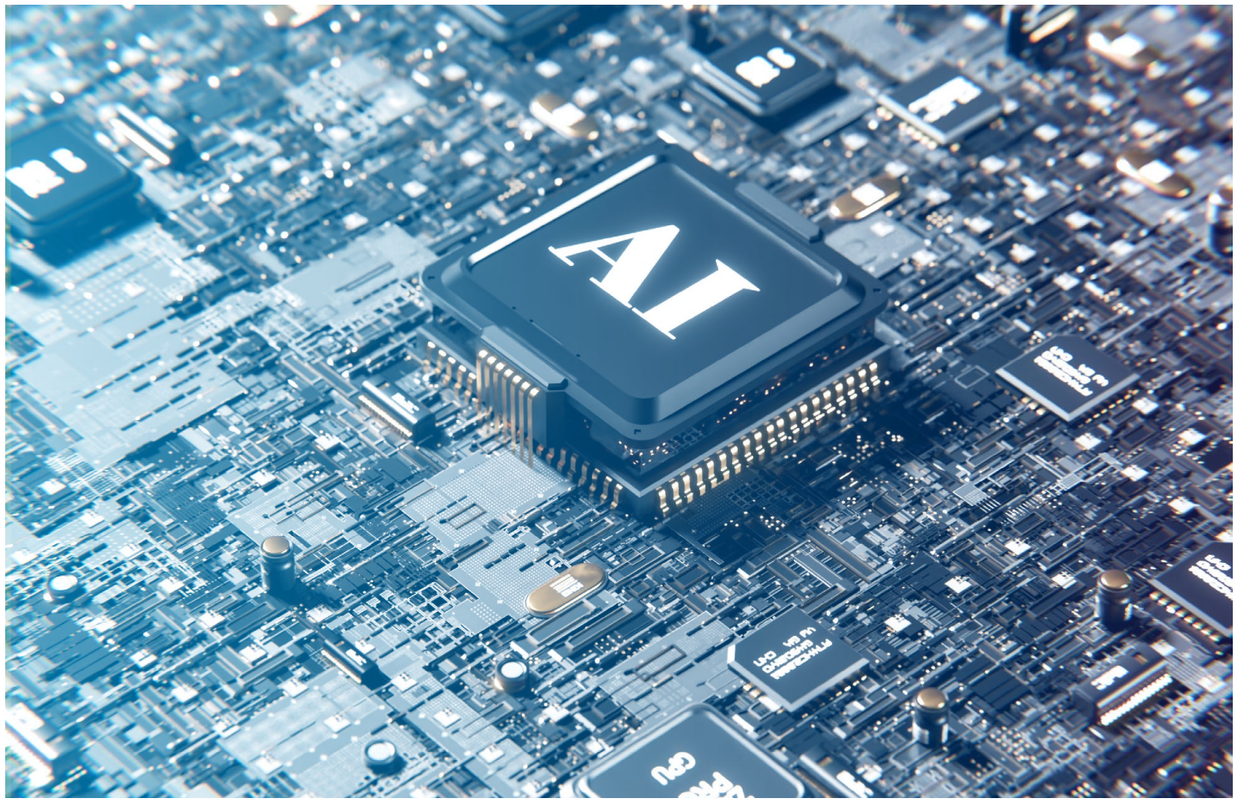
As we will see in more detail in the second part of this booklet devoted to sectoral issues, AI can be used in all business sectors, including banking and finance. For example, it has been pointed out that "trading firms are looking to AI and machine learning to use data to improve their ability to sell to clients[14]. For example, analyzing past trading behavior can help anticipate a client's next order"[15].

These examples are illustrative. In fact, AI can be used in many other sectors, such as real estate, education, journalism, and the preparation of court decisions and legislation. It can also be used by professionals, in their relations with customers or in their internal management and, more generally, in the organization of employees' work. It can also be used by authorities, particularly supervisory and regulatory bodies, wishing to exercise more effective control over the professionals they supervise.

What are the benefits and risks of AI?

"By improving prediction, optimising operations and resource allocation, and personalising service delivery, the use of artificial intelligence can support socially and environmentally beneficial outcomes[16] and provide key competitive advantages to companies and the European economy. Such action is especially needed in high-impact sectors, including climate change, environment and health, the public sector, finance, mobility, home affairs and agriculture. However, the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society" *(Explanatory memorandum, Proposal for an AI Act, spec. p 1)*. AI generates new risks, for both people and IT systems. It also amplifies existing risks, notably by increasing the dangerousness of cybercriminals[17]. These risks explain why certain AI systems are banned or more or less strictly supervised.

Because of the characteristics of the technology used by AI –opacity, complexity, heavy reliance on data, so-called autonomous behavior–, its use may infringe a number of fundamental rights enshrined in the EU Charter of Fundamental Rights *(Explanatory Memorandum, Proposal for an AI Act, spec. p. 12)*, "cause harm to public interests and rights that are protected by Union law" *(Recital no. 4, Proposal for an AI Act*). AI "can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices" *(Recital no. 15, Proposal for an AI Act)*; it can also be used "to distort human behavior, whereby physical or psychological harms are likely to occur" *(Recital no.16, Proposal for an AI Act)*.



The recitals of the Proposal for an AI Act give a number of examples.

For instance, AI systems that "evaluate or classify the trustworthiness of natural persons based on their social behaviour" may lead to the exclusion of certain individuals from certain groups even though the contexts taken into account are different *(Recital no. 17, Proposal for an AI Act*). Similarly, AI systems for "real-time" remote biometric identification of individuals in publicly accessible spaces can affect the privacy of part of the population and "evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights" *(Recital no.18, Proposal for an AI Act)*.

AI does not only pose risks to individuals. Computer systems themselves are threatened by AI. Flooding, for example, aims to skew AI results by introducing falsified or useless data that renders the AI system unusable, "for example by saturating its bandwidth or causing network machines to 'crash'"[18]. Similarly, "adversarial" attacks mislead the pattern-recognition system through a slight alteration *(ibid)*.

Ethics or regulation?

Public trust in AI is essential. So the question is how should AI be approached? Should we be content with an ethical approach, or should we introduce regulations? In the latter case, the question arises again as a choice has to be made between sector-specific and/or general regulations.

In the context of an ethical approach, a number of principles have been put forward: respect for the human person, prevention of any harm, principle of fairness, principle of explicability[19]. As regards the first principle, it is emphasized that "human beings interacting with AI systems must be able to retain their full and effective self-determination". The second principle insists on the fact that AI systems must not harm human beings. The third principle puts forward the idea that everyone should derive a fair benefit from AI and be able to challenge the decisions made by these systems. The fourth and final principle relates to transparency: the characteristics and purposes of AI systems must be known to everyone[20].

Artificial intelligence ◆ 1. European legislation

The ethical approach may lead to the exclusion of all hard law instruments. However, this is not the approach that has been chosen. It should be noted that sector-specific legislation already exists. For example, the MiFID 2 Directive of May 15, 2014[21] defines high-frequency trading[22], which relies on algorithms and software. The Market Abuse Regulation of April 16, 2014[23] takes high-frequency trading into account in its approach to market manipulation.

However, this approach is not considered sufficient. Hence the proposals for a regulation and a directive, the first concerning the supervision of AI[24] (see sections 1.2 and 1.3 p. 10 to 18) and the second non-contractual liability[25] (see section 1.4 p. 19). The Proposal for an AI Act reflects the ethical concerns raised by AI. It should be noted that the future AI Act encourages the adoption of codes of conduct and their voluntary application by AI systems that are not subject to the requirements of the future AI Act.

14 FSB, Artificial intelligence and machine learning in financial services. Market development and financial stability implications, op. cit., spéc. pp. 18.
15 FSB, Artificial intelligence and machine learning in financial services. Market development and financial stability implications, op. cit., spéc. pp. 18.
16 See section 2.10 p. 54.
17 E. Caprioli, Intelligence artificielle et sécurité des systèmes d'information dans le domaine bancaire, Hors-série Banque & droit octobre 2019 p 22, spéc. p 25 et 26.
18 Caprioli, Intelligence artificielle et sécurité des systèmes d'information dans le domaine bancaire, art. préc., spéc. p 25.
19 M. Teller, Éthique et IA : un préambule pour un autre droit, op. cit.., spéc. 40.
20 M. Teller, Éthique et IA : un préambule pour un autre droit, op. cit.., spéc. 40.
21 Directive 2014/65/EU of the European Parliament and of the Council of May 15, 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.
22 Regarding high frequency trading, see. Th. Bonneau, Régulation bancaire et financière européenne et internationale, 6° éd. 2022, Bruylant, n° 495 et s, spéc. n° 504 (MIF) et 506 (abus de marché).
23 Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.
24 Proposal for an AI Act, op. cit.
25 Proposal for a directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), Brussels, 28.9.2022, COM(2022) 496 final, 2022/0303 (COD).

1.2 FUTURE EUROPEAN AI ACT

Authors:
Michel Servoz - *Senior Counsel*
Matthieu Lucchesi - *Counsel*

As the potential risks presented by AI are a major concern, it is therefore legitimate for industrialized countries to seek to regulate it. The European Union is the first region in the world to embark on an ambitious regulation, as part of a wider digital rulebook that regulates different aspects of the digital economy like the General Data Protection Regulation ("**GDPR**"), the Digital Services Act and the Digital Markets Act designed to safeguard the health, safety and fundamental rights of EU citizens. The European Commission published its Proposal for an AI Act in April 2021. Adoption of the future European AI Act is expected in the first half of 2024.

The future AI Act is still under finalization. A political agreement was reached on the AI Act by the EU institutions on December 8, 2023. This political agreement defines the global approach on specific topics to be regulated under the future regulation. It was voted by the Member States on February 2, 2024. However, the text resulting from the political agreement between the EU institutions is still being finalized and will then have to be formally adopted by the European Parliament before being officially promulgated (see section 1.3 p. 15). The developments below are based on the main elements of the version voted on February 2, 2024 and may need to be adapted in light of the final version of said Act.

The future AI Act will be enforced in conjunction with other measures, such as the revision of the General Product Safety Directive and the new AI Liability Directive (see section 1.4 p. 19), which specifically addresses non-contractual liability issues resulting from AI systems.

The Future AI Act will introduce safeguards to ensure Europeans can trust AI systems. However, while most AI systems pose limited to no risk, conversely certain AI systems present risks against which protective measures need to be taken. Very often, it is impossible to find out why an AI system generates a prediction or takes a particular action. So, it may become difficult to establish whether someone has been unfairly disadvantaged. Yet, incidents have been widely covered in the media: a biased recruitment tool; another systematically predicting a higher risk of recidivism for black defendants than white defendants; or a car insurance premium tool providing residents of disadvantaged areas with more expensive quotes.

> ***The Future AI Act will set out a harmonized legal framework for the development, market launch and use of AI systems in EU countries, based on the categorization of risks presented by these systems and accordingly imposing different obligations on parties providing, developing, or deploying AI systems.***

The future AI Act relies on a traditional European product safety legislation approach, considering that AI providers (put simply, the software company that develops the AI) are the equivalent of the manufacturers of products like dishwashers or toys and should therefore bear the main responsibility of ensuring the safety of AI systems (see section 1.4 p. 19). There are also specific requirements for developers (a software company that adapts the AI systems to a specific use) and for deployers/users (a company that is using the AI system in its business operations).

What is the scope of the future AI Act?

The future AI Act will apply to AI systems understood as machine-based systems that, for explicit or implicit objectives, generate output such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Ablbeit broad, this definition, in line with the approach of the Organisation for Economic Cooperation and Development (OECD), is meant to exclude simpler software systems.

The territorial scope will be wider than the EU, meaning it will cover AI systems that are "placed on the market, put into service or used in the EU". So, in addition to providers, developers and deployers in the EU, it will also apply to non-EU companies as soon as they will make their system or its output available to users in the EU (see section 1.3 p. 15).

In substance, certain AI systems will be excluded from the scope of application: AI systems exclusively developed or used for military, defense and national security purposes; AI developed for scientific research; and to a certain extent, free and open-source AI systems (unless they correspond to a prohibited AI system or a high-risk AI system).

In addition, AI regulatory sandboxes, which provide for a controlled environment for the development, testing and validation of innovative AI systems, will allow for testing of AI systems before they are marketed in compliance with the new AI Act. In principle, these sandboxes will be launched at national level, but could also be established at regional level or jointly by several Member States. The future AI Act will also enable AI systems to be tested in real-world conditions, subject to compliance with specific requirements.

What is meant by the risk-based approach set out in the future AI Act?

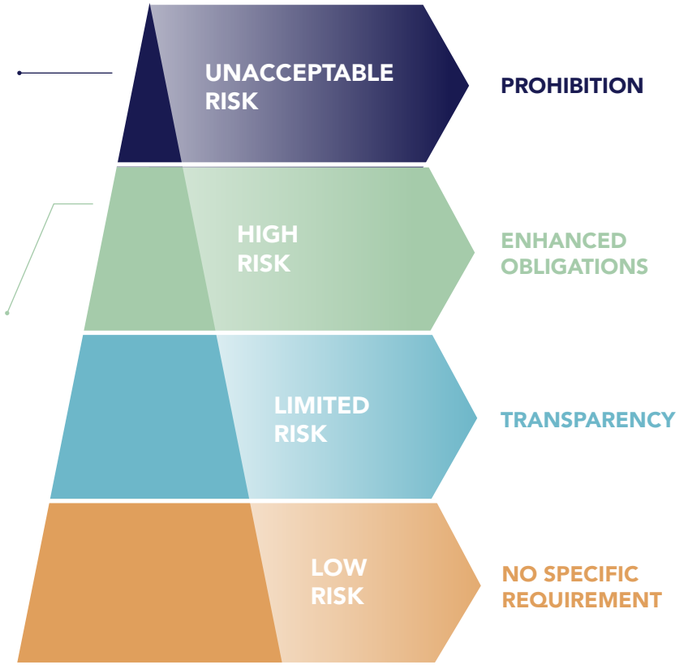
The future AI Act will link the obligations applicable to AI systems to the level of risk involved, considering their design and intended use. Based on the risk level, it will introduce requirements in terms of documentation, auditing, transparency and obligations. Four distinct levels of risk are considered as it stands:

- **Systems presenting unacceptable risks:** Examples are the manipulation of individuals through cognitive and behavioral manipulation, the untargeted scraping of facial images from the Internet or CCTV footage, social scoring, inferring emotions of a natural person in the workplace and education institutions, biometric categorization to infer sensitive data, and real-time and post remote biometric identification systems. These AI systems are banned from the EU market. However, as regards real-time remote biometric identification systems in public spaces, they would be allowed for the victims of certain crimes, for the prevention of serious threats, such as terrorist attacks, and for the search for suspects of the most serious crimes.
- **High-risk systems:** Systems that can have a significant impact on the lives of users, such as AI systems used in education, employment, law enforcement or the administration of justice. In principle, these systems will have to meet stringent requirements before being deployed on the EU market.
- **Systems with limited risk:** Systems that present neither unacceptable nor high risks, but interact directly with natural persons. Examples are chatbots and deepfakes. The obligations for these systems will be related to transparency, where users must be duly informed that they will interact with an AI.
- **Low-risk systems:** Examples are spam filters or AI-enabled video games. These systems will not be subject to additional constraints as it stands, but they will have to comply with existing legislation.

List in art. 5:
Example : AI system using subliminal techniques that substantially alter behaviour and cause harm to the user or a third party

List in Annexes II & III including:
- Biometric identification and verification of natural persons
- Critical infrastructure
- Education and vocational training
- Etc.

Possible extension of the list



What are the requirements regarding high-risk AI systems?

High-risk AI systems are listed in the future European AI Act. They include two categories: (i) systems integrated as a safety component into a product already subject to existing safety standards (such as AI integrated into a medical device), listed in Annex 2 of the future AI Act; and (ii) autonomous systems presenting a significant risk to people and used in the following eight sensitive areas listed in Annex 3: biometrics, critical infrastructure, education and vocational training, employment and workers management, access to essential services, law enforcement, migration and border control, administration of justice and democratic processes.

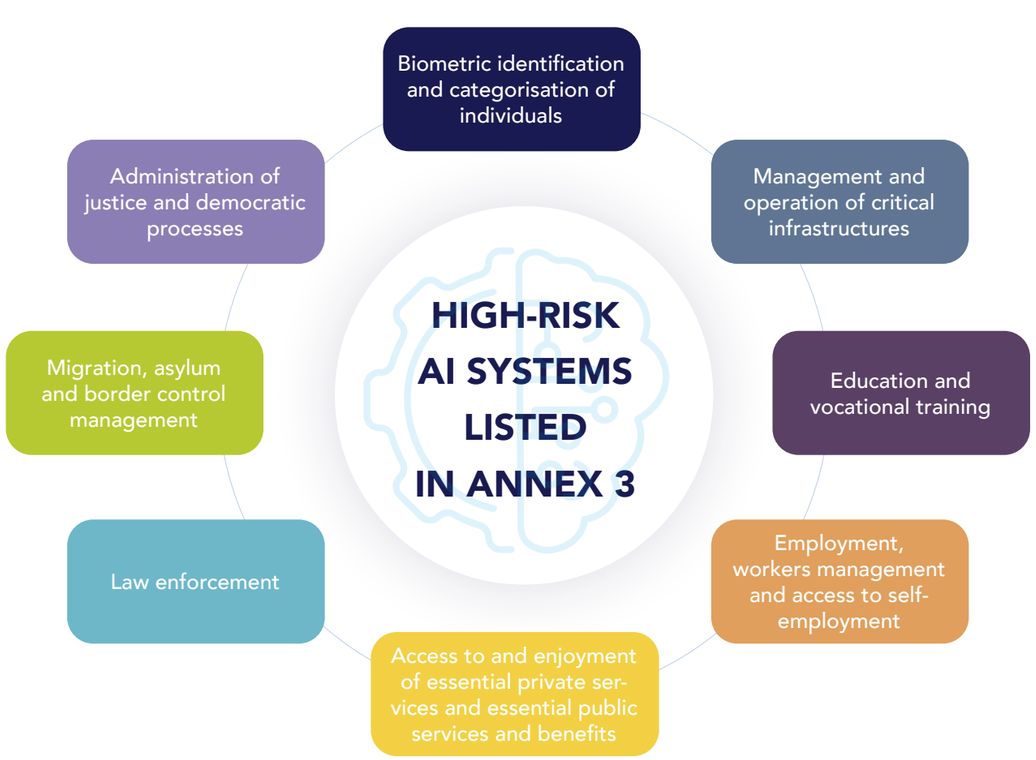
Providers and developers will determine their AI system's risk category themselves and will be able to self-assess and self-certify the conformity of their AI systems and governance practices with the future AI Act.

A legislative amendment has introduced the possibility for providers of high-risk systems to inform the competent supervisory authorities when the former consider that their system does not pose significant risks.

As it stands, the requirements for high-risk systems would be as follows:

- a continuous and iterative risk management system throughout the system's entire life cycle;
- data governance ensuring that the data for the training, validation and testing of systems are appropriate for the system's intended purpose;
- a design allowing appropriate transparency and provision of information to users, and appropriate human oversight to prevent or minimize risks to health, safety and/or fundamental rights;
- a fundamental rights impact assessment before a high-risk AI system is launched on the market;
- accuracy, robustness and cybersecurity throughout the system's life cycle.

To ensure compliance with the relevant obligations, conformity assessments must be carried out. The system must then be registered in the EU database and should bear the CE marking to indicate its conformity before it can be placed on the market.



COMPLIANCE MILESTONES FOR HIGH-RISK AI SYSTEMS

1. Mapping of high-risk AI systems
2. Conformity assessment
3. Drafting the declaration of conformity
4. CE marking
5. Market launch

Once placed on the EU market, a reporting system for serious incidents should be set up to ensure proper monitoring. A serious incident is defined as an incident that is responsible for or could have caused, in particular, serious damage to a person's health, serious damage to property or critical infrastructure or the violation of fundamental rights. The relevant authorities should be notified of such incidents and records should be maintained of the AI system's operation to monitor compliance with the AI Act.

What is the situation for limited and low-risk AI systems?

An AI system is considered as posing a limited or low risk if it does not belong in any other category. The future AI Act introduces transparency requirements for certain limited-risk AI systems. These apply to AI systems that engage with humans, including *chatbots*, emotion recognition systems, biometric categorization systems, and systems that generate or manipulate content to mimic existing people, objects or locations, also known as *deepfakes*. When using AI systems such as *chatbots*, users should be aware that they are interacting with a machine, so they can make an informed decision to continue or request to speak with a human instead. Artificially generated or manipulated content should be flagged as such to users.

AI systems that pose a low risk are essentially unregulated. These applications are already widely deployed and make up most of the AI systems with which we interact. Examples include spam filters, AI-enabled video games and inventory-management systems.

The particular case of foundation models and general-purpose AI (GPAI)

At the time of the European Commission's Proposal for an AI Act in April 2021, foundation models and general-purpose AI were not well-known to the public: this is why the future AI Act did not initially contain any provisions in this regard. Foundation models (e.g. ChatGPT4) are AI models that are designed on the basis of a large amount of data and are capable of performing a wide range of distinctive tasks, i.e., generating video, text, images, conversing in [natural/lateral] language or generating computer code.

GPAI are AI models that have a wide range of possible uses, intended or not by the developers, and can be applied to many different tasks in various fields, with or without substantial modification.

It became an important subject in the legislative negotiations between the EU institutions. More recently, there was a significant debate about the degree to which foundation and GPAI models ought to be regulated.

- The agreement foresees that GPAI models will have to comply with transparency obligations before being launched on the market: providers will have to provide procedures and technical documentation for their models (including training and testing), and make the appropriate information and technical documentation available to providers of AI systems integrating the models. These obligations would not apply to GPAI provided under a free and open licence.
- In addition, model providers must ensure compliance with European copyright regulations (see Section 2.1 p. 23) and must publish a summary of the content used to train the model.
- GPAI models will be able to use codes of conduct to ensure their compliance with the AI Act.
- However, GPAI models with a systemic risk will have to comply with stricter requirements, including having to conduct model evaluations, assess and mitigate systemic risks, conduct adversarial testing, report to the Commission on serious incidents, ensure cybersecurity and report on their energy efficiency.

A priori, the following would be considered as presenting a systemic risk: notably, "general purpose AI models that were trained using a total computing power of more than 10^25 FLOPs" [(which corresponds to the most advanced general-purpose AI models currently available)][26].

26 European Commission, Artificial Intelligence – Q&As (europa.eu), updated as of December 12, 2023.

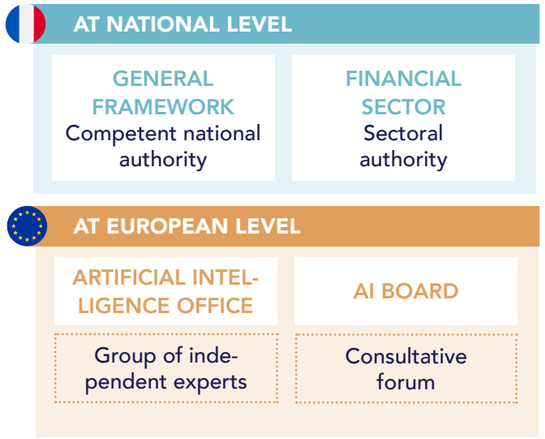
AI and resource performance

Specific requirements will apply in terms of reporting and documentation processes to improve the performance of AI systems in terms of resource consumption, such as reduction of energy and other resource consumption of the high-risk AI system during its life cycle, and on the energy efficient development of general-purpose AI models. To this end, in consultation with the relevant stakeholders, the Commission will issue standardization requests to the European standardization organizations within six months after the date of entry into force of the future AI Act.

How is the enforcement of the future AI Act organized?

Member States will be required to designate or create national regulatory bodies responsible for enforcing the AI Act and the European Commission will coordinate EU-wide issues. Architecturally, the future AI Act resembles the supervision and enforcement module under the GDPR in that it will bring various competent national authorities together in an Artificial Intelligence Board, similar in function to the European Data Protection Board.

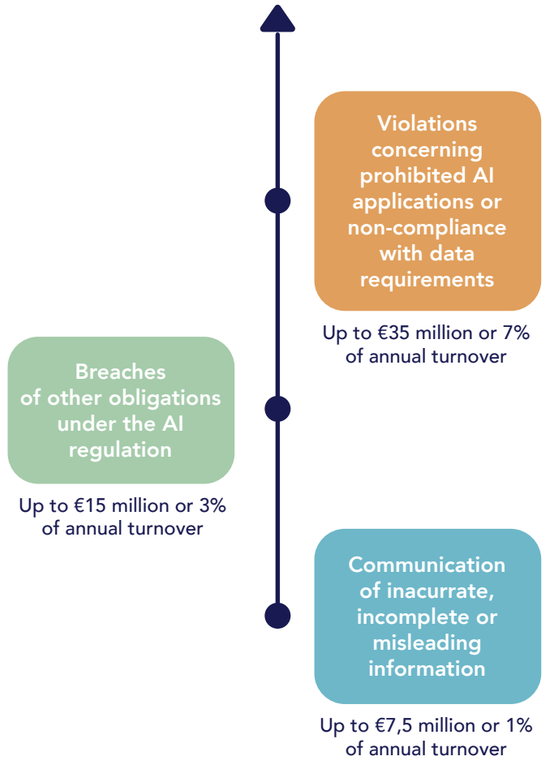
This European Artificial Intelligence Board will be assisted by the expertise of a consultative forum bringing together market players, including representatives from the industry, SMEs, civil society and academia. Following the new rules on foundation models and GPAI models, an AI Office within the Commission, supported by a scientific panel of independent experts, will be tasked to oversee the most advanced AI models, contribute to fostering standards and testing practices, and enforce the common rules in all Member States. By decision dated January 24, 2024, the European Commission specified the operating conditions of the AI Office, with this organization taking effect on February 21, 2024.



What are the sanctions in the event of a breach?

Violations will be sanctioned by fines set as a percentage of the offending company's global annual turnover in the previous financial year or a predetermined amount, whichever is higher, with the exception of SMEs, for which the lower is used. These fines could reach:

- up to 35 million euros or 7% for breaches concerning prohibited AI applications or non-compliance with data requirements;
- up to 15 million euros or 3% for breaches of other obligations under the AI Act; and
- up to 7.5 million euros or 1% for providing inaccurate, incomplete or misleading information.



1.3 PRACTICAL ISSUES RAISED BY THE FUTURE AI ACT

Authors:
Michel Servoz - *Senior Counsel*
Matthieu Lucchesi - *Counsel*

The future European AI Act will be the first AI legislation worldwide; it will regulate both how providers of AI systems and GPAI models should develop their systems to minimize risks and how deployers of such AI systems will have to control them.

Practitioners will soon be faced with a new set of regulations and will have a decisive role to play: they will have to contribute to the stable and predictable application and interpretation of the future AI Act. What's more, knowing that systems using artificial intelligence are advancing at a dizzying rate, the future AI Act must not become a regulatory framework that is difficult to apply, as shown by the EU co-legislator's recent attempts to capture the legal implications of foundation AI models (such as ChatGPT).

A precedent can be drawn from the EU's General Data Protection Regulation. Like the GDPR, the scope of the future AI Act is very broad, since it applies to all areas of society. There is however a significant difference between these two regulations: where the GDPR was developed by drawing on an old directive that had given rise to decades of practical application, the future European AI Act is a creation largely made *ex nihilo*. It is however inspired *mutatis mutandis* by European legislation on defective products, which is bound to pose practical difficulties here, as this is an intangible product (see Section 1.4 p. 19).

The following section looks at some of the practical problems that companies using AI will encounter when implementing the new legislation.

Scope of the future AI Act

One of the biggest stumbling blocks with the future European AI Act has been how artificial intelligence should be defined in a legal sense, which is essential to determine whether the system that a company buys or uses is covered by legislation. This issue illustrates the fact that not even data scientists, engineers and similar professionals working with artificial intelligence have come up with a suitable description of what artificial intelligence is and what it is not. The center of the lexical contention lies between two poles: On the one hand, the definition of AI should not cast the net too widely and include things as simple as spreadsheet calculations. On the other hand, overly precise definitions will hamper the regulation's efficacy: being "future-proof" is especially critical for legislation in a field defined by rapid technological changes. The EU's aim has been to keep the definition of artificial intelligence broad and the future AI Act contains several general guidelines that would apply to all aspects of artificial intelligence (see Section 1.2 p. 10). At the same time, the future AI Act goes even further, touching on, for example, the technical operating mechanisms of individual systems. Companies will have to watch carefully whether their systems fall within the scope of the Act.

Distinction between providers and deployers

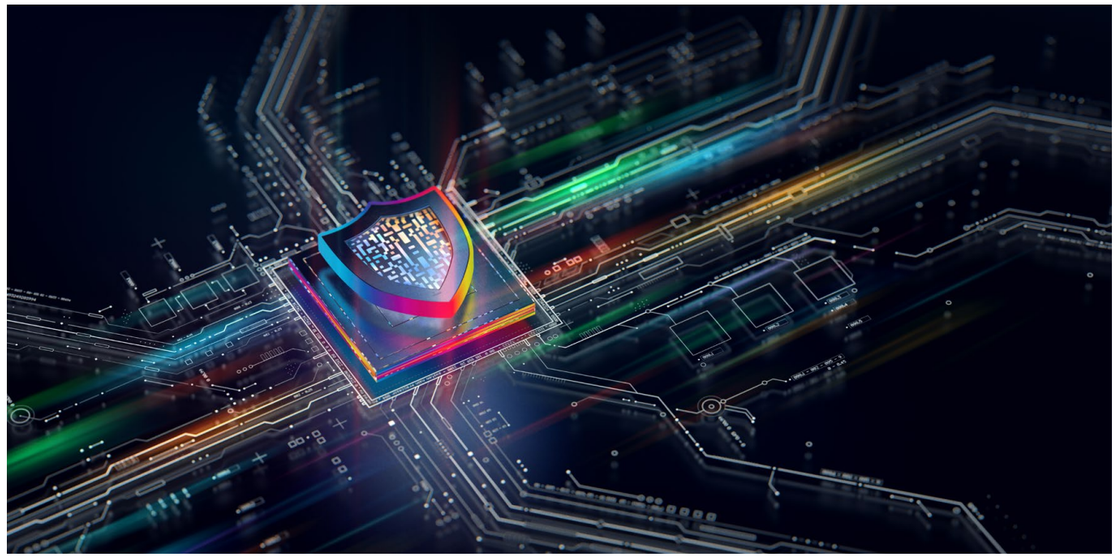
The future European AI Act is modelled on existing European product safety legislation: in particular, it considers that AI "providers" (put simply, the software company that develops the AI) are the equivalent of the manufacturers of physical products like dishwashers or children's toys. For these kinds of products, it is indubitably the initial manufacturer that knows best how to make the product safe. However, comparison is not always possible as AI is not a dishwasher and the way downstream deployers use it and adapt it may be as significant as how it was originally built.

Many AI products are thus dynamic –as opposed to static– products: they will change with new data, new uses and new integrations, which will impact their risk profiles. This raises the question of who falls within its scope and of who should be held accountable for the different phases of the AI's life cycle.

Furthermore, AI systems can be of general purpose, meaning the same system can be applied to different contexts and can have an impact that differs for different individuals and groups. For example, a provider of a facial recognition system can sell its product to a phone manufacturer using face identification for unlocking phones or to governments for surveillance and security at airports.

In the future AI Act, by analogy with the manufacturers of physical goods, the primary responsibility is placed on the initial "provider", unless a "substantial modification" is made to the system afterwards.

Yet, many obligations in the future AI Act, such as ensuring that "human oversight" is correctly implemented (in high-risk systems), can only effectively be put in place by "deployers" (the company that uses the AI), which will often buy a system off the shelf.



In this complex web of actors, data, models, and services, it will be essential for a company to precisely identify its applicable legal regime together with the duties and rights of the identifiable actors in its supply chain.

Technical feasibility of AI standards

The purpose of the future AI Act, like all European product legislation, is to lay out essential requirements only, which are specific enough to create legally binding obligations.

It will be necessary to fill in the blanks left by legislation: two of the three European Standards Organizations ("**ESOs**"), organizations independent of the EU, will be responsible for creating harmonized standards for AI. They will set the bar that systems must meet (by defining tests and metrics) and will outline how the systems should be developed (by describing tools and processes that can be used).

Adherence to these harmonized standards will offer an objectively verifiable way of complying with European legislation and will provide companies that follow them with a presumption of conformity. However, the challenge lies in the actual ability of ESOs, which have little experience outside product standards and no experience regarding AI, to develop standards that are meaningful and operational for companies. It is going to be crucial for companies and industry representatives to be closely involved in the development of such standards.

Human oversight

The future AI Act will set a general obligation for providers of high-risk AI systems to design them in a way that can be effectively overseen by natural persons.

The obligations are placed on the providers, highlighting the preventive nature of the Article. The future AI Act does not identify mechanisms to effectively implement human oversight. It does not specify when and where humans shall have the final word on the decision.

Paradoxically, the deployers, which are the best placed to set up effective human oversight, are absent from this Article. Their obligations consist in monitoring the operation of the high-risk AI system based on the instructions of use, informing the provider or distributor, and suspending the use of the system in case of an incident presenting a safety risk.

Here again, this approach is linked to the fact that the future AI Act is a product safety legislation and therefore does not concern the end users of an AI system.

However, in practice, systems falling within the high-risk category in the future AI Act use personal data and therefore are subject to the GDPR. Under Article 22 of GDPR, with some exceptions, the end user has the right not to be subject to a decision based solely on automated processing, which means the right to human oversight. In other words, if a bank bases its refusal to grant a loan on an AI system or if a telecommunications provider does not accept a customer on the basis of a negative result rendered by a creditworthiness agency via an IA system, this customer has the right to obtain a review of the decision made by a human, to express his point of view and challenge the decision. This means that any company using AI for decision-making must see to it that at any moment, humans can review the decision made by the AI.

Transparency obligations

Under the future AI Act, AI-based systems must be transparent in their functioning, so that users can understand how decisions are made and the logic behind them.

From a practical standpoint, high-risk AI systems should be designed and developed in such a way that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately, and that appropriate human-machine interface tools exist to enable oversight.

In addition, for all AI systems with a human interface, it is required that users be informed that they are interacting with an AI system.

The future AI Act includes a potentially powerful mechanism for ensuring systematic transparency: a public database for high-risk AI systems, created and managed by the Commission. However, the draft legislation is silent as to the level of transparency and interpretability that will be imposed on AI systems.

There is also a lack of consensus on the meaning of interpretability and on how exactly the provision of information will enable interpretability.

Finally, the obligation to register high-risk AI systems only applies to providers, but not to those deploying them, which means that no input will be provided on how high-risk systems are used, which arguably is what matters the most. Overall, the lack of direction on the level of transparency and interpretability required in concrete situations will create major legal uncertainty for companies. If an AI system is being used for medical applications or legal applications versus entertainment purposes for example, this will have a considerable impact on the degree of transparency and evaluation required.

Extra-territoriality

Like the GDPR, and other recent European legislation in the Tech sector, the future AI Act will likely have a significant extra-territorial effect.

It will apply to organizations outside the EU, essentially to providers launching AI systems on the market or putting AI systems into service in the EU, irrespective of whether these providers are located within the EU or in a third country.

It will also apply to AI system users located in the EU and to AI system providers and users located in a third country, where the output produced by the AI system is used in the EU. Consequently, the future AI Act applies in principle if an AI system or its output is used within the EU. As an example, the use of a *chatbot* to answer enquiries from EU-based individuals regarding a credit or a Swiss bank's use of AI systems to check the creditworthiness of individuals in the EU would likely trigger the application of the future AI Act. In fact, some of the policymakers involved in the legislation have made it clear that their goal is to create a worldwide AI standard, in what they see as a race to regulate AI.

> ***Therefore, for companies located outside the EU, it could be easier to adapt all their operations to the requirements of the future European AI Act, so as to simplify their business process.***

GPAI AI model and intellectual property

When it comes to copyright, there are a number of important questions that practitioners will have to answer. One of these is the use of protected works in training models for AI systems. Several complaints were lodged in 2023 concerning this issue, and the mobilization of rights holders has recently gained momentum. The European legislator has therefore chosen to respond by establishing a principle of transparency regarding the use of protected works by AI systems, and an obligation to comply with European copyright regulations (see Section 2.1 p. 23). The latter measure could prove difficult to implement however, as the recognition and identification of protected works used by AI during the training of AI systems may prove particularly difficult in practice.

Entry into force

Once adopted, the future AI Act will enter into force 20 days after its publication in the Official Journal of the European Union, which should take place in the first half of 2024.

Once in force, it will be implemented gradually: after publication in the Official Journal of the European Union, the future AI Act should be applicable in principle 24 months after its entry into force, i.e. *a priori* in the first half of 2026.

> ***By way of exception, certain provisions of the future AI Act could be applicable before this date, notably 6 months after its entry into force for systems presenting unacceptable risks.***

Others may not come into force until 36 months after said entry into force, for AI systems considered to be high-risk in already regulated areas according to Annex II of the future AI Act.

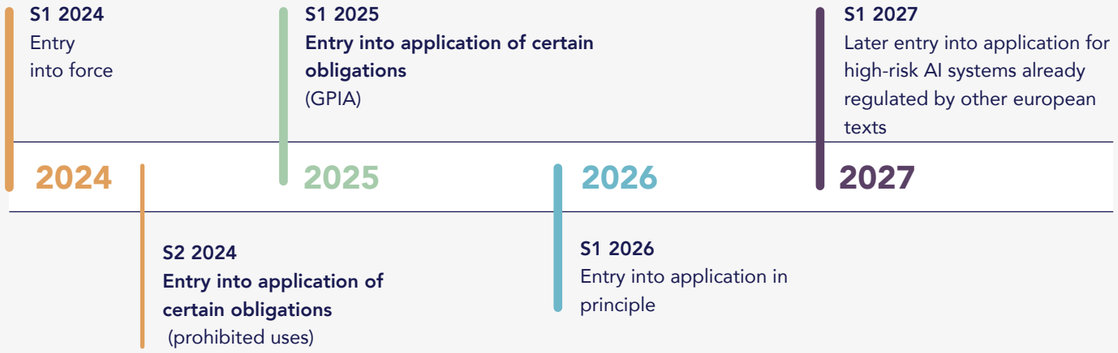
Anticipation

As most of the provisions of the future AI Act will have to be implemented within two years of its publication, organizations developing and using AI systems will need to anticipate the new rules by adapting their governance structures and management systems to mitigate risks.

This means in particular:

- Map the AI systems that a company uses in order to precisely identify the obligations that will apply to them under the future European AI Act.
- Introduce an AI risk assessment framework that will need to consider the risk of bias at every stage, understand and document the intrinsic characteristics of the data, carefully calibrate the algorithm, and use appropriate datasets to train the AI.
- Adapt the governance infrastructure, bearing in mind that human supervision throughout the system's life cycle will be mandatory, and that transparency must be built in so that users can interpret the system's results.
- Improve privacy protection programs to ensure that adequate safeguards are in place to enforce the rights of data subjects.
- Improve AI skills, not only for teams working directly with the systems, but also for those operating alongside them. Legal departments will need to familiarize themselves with the operation of their organization's AI systems to ensure that they comply with the proposed regulations.

AI Pact In view of the phased implementation of the new Act, on November 15, 2023 the European Commission launched the AI Pact to encourage European and foreign companies, on a voluntary basis, to commit to voluntarily applying the obligations arising from European AI legislation before its general application and to share their best practices. The Commission will bring together interested companies, in the first half of 2024, to discuss the ambitions of the AI Pact..



1.4 NON-CONTRACTUAL CIVIL LIABILITY FOR DAMAGE CAUSED BY AN AI SYSTEM

Author:
Thierry Bonneau - *Senior Counsel*

Liability constitutes one of the obstacles to the use of AI by businesses[27]. The latter are reluctant to adopt AI because the distribution of responsibilities between the various economic operators involved in the AI chain is uncertain[28]. What's more, as regards potential victims, given the characteristics of AI systems, they may find it "difficult or prohibitively expensive for victims to identify the liable person and prove the requirements for a successful liability claim" (Expl*anatory Memorandum*, Proposal for a Directive, *p. 1).*

National rules, current EU legislation and proposed Directive

These difficulties are linked to the rules that currently apply. "Member States" general fault-based liability rules usually require that person to prove a negligent or intentionally damaging act or omission ('fault') by the person potentially liable for that damage, as well as a causal link between that fault and the relevant damage. However, when AI is interposed between the act or omission of a person and the damage, the specific characteristics of certain AI systems, such as opacity, autonomous behavior and complexity, may make it excessively difficult, if not impossible, for the injured person to meet this burden of proof. In particular, it may be excessively difficult to prove that a specific input for which the potentially liable person is responsible had caused a specific AI system output that led to the damage at stake". *(Recital no. 3, Proposal for a Directive).* In other words, it can be difficult to detect and prove possible breaches of the law *(White Paper, op. cit. spec. p. 16).*

At European level, legislation on product safety[29] and liability for defective products[30] are "two complementary mechanisms to pursue the same policy goal of a functioning single market for goods that ensures high levels of safety, i.e. minimize the risk of harm to users and provides for compensation for damages resulting from defective goods"[31]. The second provides for a system of strict producer liability for damage caused by product defects[32]. As for the former, it "allocates the responsibility to the producer of the product placed on the market, including all components e.g. AI systems. But the rules can for example become unclear if AI is added after the product is placed on the market by a party that is not the producer. In addition, EU product liability legislation provides for liability of producers and leaves national liability rules to govern liability of others in the supply chain"[33].

The proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence "is to contribute to the proper functioning of the internal market by harmonizing certain national non-contractual fault-based liability rules, so as to ensure that persons claiming compensation for damage caused to them by an AI system enjoy a level of protection equivalent to that enjoyed by persons claiming compensation for damage caused without the involvement of an AI system. This objective cannot be sufficiently achieved by the Member States because the relevant internal market obstacles are linked to the risk of unilateral and fragmented regulatory measures at national level. Given the digital nature of the products and services falling within the scope of this Directive, the latter is particularly relevant in a cross-border context" *(Recital no. 7, Proposal for a Directive).*

27 Explanatory memorandum, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), Brussels, 28.9.2022, COM(2022) 496 final, 2022/0303 (COD), spéc. p 1.
28 European Commission, White Paper, Artificial Intelligence, On Artificial Intelligence - A European approach to excellence and trust, Brussels, l 19.2. 2020, COM(2020)65 final, spéc. p 16.
29 Directive 2001/95/EC of the European Parliament and of the Council of December 3, 2001 on general product safety.
30 Council Directive 85/374/EEC of July 25, 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.
31 European Commission, Report from the Commission to the European Parliament, the Council and the European economic and social committee, Report on the safety and liability implications of artificial intelligence, the internet of things and robotics, Brussels, 19.2.2020, COM(2020) 64 final, spéc. p 12.
32 Ibid p 14.
33 Ibid p 16-17.

General approach to the proposal

The proposed Directive concerns only non-contractual fault-based civil law claims for damages, in cases where the damage caused by an AI system occurs after *(Art. 1, § 2, para. 1)*. Criminal liability is expressly excluded *(Art. 1, § 2, para. 2, Proposal for a Directive)*.

> ***The proposal is limited in scope. It aims only to establish common rules concerning the disclosure of evidence on high-risk AI systems and the burden of proof.***
> *(Art. 1§ 1, Proposal for a Directive)*
> *(see Section 1.2 p 10)*

The proposal enshrines "a minimum harmonization approach". "Such an approach allows claimants in cases of damage caused by AI systems to invoke more favorable rules of national law" *(Recital no.14 and Art. 1, § 4, Proposal for a Directive)*.

Disclosure of evidence and rebuttable presumption of non-compliance

The question of the role of the parties and the judge with regard to the burden of proof is enigmatically framed by Articles 1353 of the French Civil Code and Article 9 of the French Code of Civil Procedure[34]. However, as Article 9 states that "it is incumbent on each party to prove, in accordance with the law, the facts necessary for the success of its claim", it can be deduced from this that proof of the alleged facts rests with the parties, in principle at least, and that the judge cannot directly introduce evidence into the debate, such as documents in his/her possession[35]. He/She may however "take the initiative of ordering any investigative measure useful in ascertaining the truth"[36]: "the judge has the authority to order sua sponte any legally appropriate investigation measures" (Art. 10, French Code of Civil Procedure). It should be noted that, barring exceptions[37], this is not an obligation for the judge[38].

The proposed Directive seems to go further, as Article 3, which deals with the disclosure of evidence, seems to impose an obligation on the judge. This obligation is strictly defined.

In particular, with regard to the potential claimant –defined as the natural or legal person who/that intends to bring an action for damages, but has not yet done so– the proposed Directive requires that the potential claimant approached the debtor of the disclosure obligation, that the claim was refused and that, in support thereof, the potential claimant produced sufficient facts and evidence to support the plausibility of an action for damages. It should also be noted that the judge must ensure respect for business secrecy and that failure to comply with an injunction to disclose or preserve evidence gives rise to a rebuttable presumption.

This system approximates the AI rules to criminal law rules. On the one hand, the criminal judge is under the obligation to investigate both sides of the case (Art. 81, French Code of Criminal Procedure). On the other hand, despite the presumption of innocence, presumptions consisting in "assuming that the existence of the material element of the offence is an established fact"[39] are admitted.

Rebuttable presumption of a causal link

Under ordinary law, the perpetrator of damage can only be held liable if there is a causal link between the fault and the damage. This raises the question of whether the causal link must be proven by the victim or whether it is presumed, in which case the defendant must prove the absence of a sufficient causal link[40]. The answer, in domestic law, is clear: "It is up to the plaintiff to establish the causal relationship between the wrongful act and the damage. In other words, any doubt as to the existence of this link is, in principle, to the defendant's advantage" *(Ibid)*.

Article 4 of the proposed Directive establishes a presumption. Causality between the fault of the defendant, supplier or user of the AI system and the result produced by the AI system, or its inability to produce a result, is presumed. However, the presumption is not irrebuttable: the defendant can rebut it. Moreover, in the case of an action for damages against the supplier or user of a high-risk AI system, the condition of fault on the part of the defendant is defined in restrictive terms.

Timetable

The proposal for a Directive adapting the rules on non-contractual civil liability to the field of artificial intelligence was published on September 28, 2022.

On this basis, discussions within the European Parliament and the Council of the EU have begun. However, they remain conditional on the progress of negotiations to finalize the future European AI Act, on which this proposed Directive is directly dependent.

34 C. Chainais, F. Ferrand, L. Mayer et S. Guinchard, Procédure civile, Droit interne et européen du procès civil, 34° éd. 2018, Dalloz, n° 610 p. 479
35 Ibid n° 612 p 479.
36 Ibid n° 613 p 479.
37 Ibid n° 616 p 481.
38 Cass. civ. 2, 23 avril 1980, Gaz. Pal. 1981.89, note J. Massip ; Cass. Civ. 1, 14 mars 2000, Bull. civ. I n° 87 ; Cass. Com. 14 décembre 2004, Bull. civ. IV n° 224.
39 S. Guinchard et J. Buisson, Procédure pénale, 16° éd. 2023, Lexisnexis, n° 535 p 488.
40 F. Terré, Ph. Simler, Y. Lequette et F. Chénedé, Droit civil, Les obligations, 13 éd. 2022, Dalloz, n° 1092 p 1215.

Artificial intelligence ◆ 1. European legislation

02

LEGAL ISSUES

2.1 INTELLECTUAL PROPERTY

Authors:
Julien Guinot-Deléry - *Partner*
Marie-Ange Pozzo di Borgo - *Counsel*

Among the multitude of questions being raised, only one thing seems certain: the development of AI calls for a rethink –or at least an adjustment– of the fundamental rules and principles of intellectual property law.

What protection is there for AI systems and the people who develop them?

Intellectual property law protects various forms of creations and inventions through distinct regimes (patents, copyright, software, databases, etc.). While offering a wide array of components of use, AI is likely to fall within the scope of several of these regimes; however, AI also relies heavily on algorithms, which are considered excluded from intellectual property (as mathematical formulas that are part of the realm of ideas, they are *a priori* unprotectable).

How can AI be regulated while respecting the fundamentals of intellectual property law? It is possible to resort to a distributive classification based on the object of the protection sought (software law for computer programs, database law for machine learning, etc.), although this has already shown its limits, particularly in the field of video games. Far from being ruled out however, the creation of a *sui generis* right is expressly envisaged by certain academics.

Patent protection may also be considered if the AI system is presented as a technical solution applied to solve a technical problem. Know-how can also provide additional, or even exclusive, protection, although this requires that special procedures be put in place within the companies concerned to ensure that this know-how is recorded, identified and protected as soon as it is created.

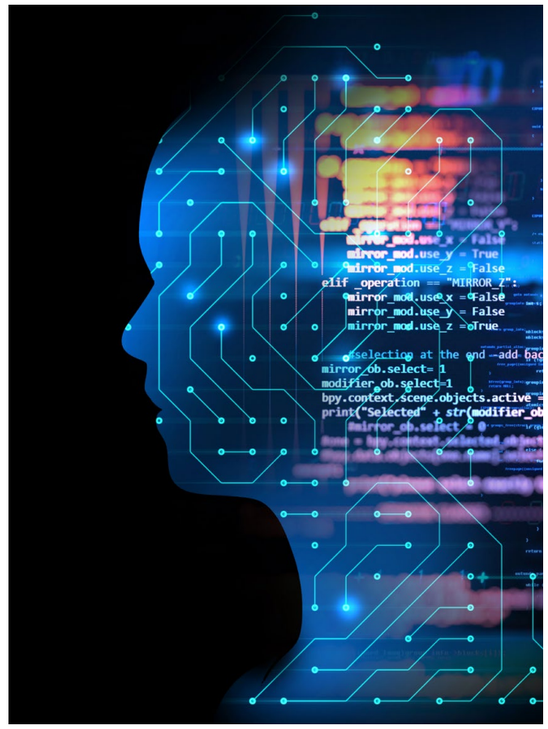
The search for adequate protection is an issue of the utmost importance, not only because of the upcoming competition between major AI suppliers, but also because AI is likely to attract many other "traditional" operators wishing to develop and exploit their own AI systems, which presupposes an effective strategy for protecting their rights.

How can AI-generated results be protected?

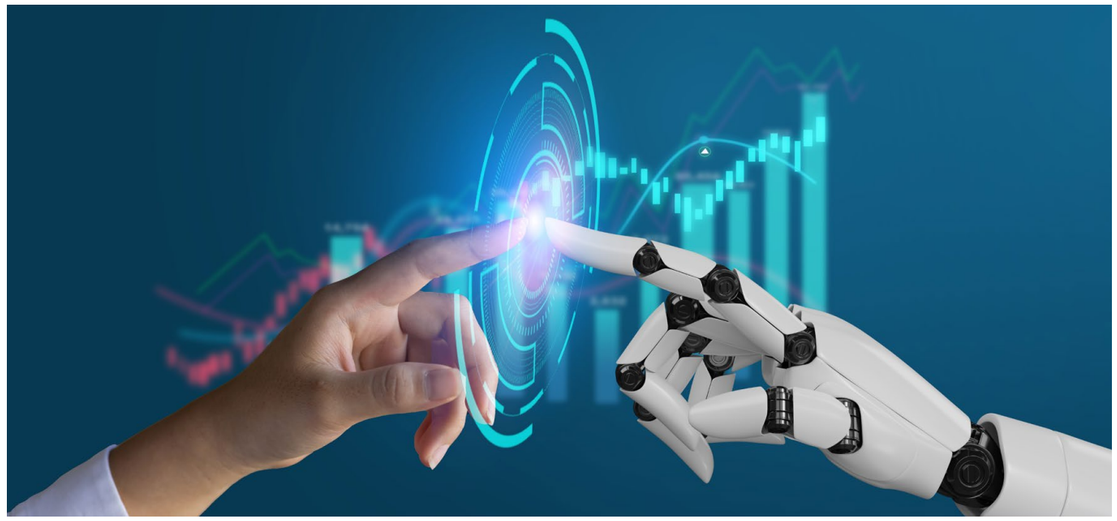
Generative AI is revolutionizing all sectors of the creative and cultural industries (text –publishing, journalism–, music, audiovisual, graphics, images, video games, etc.), whose content is traditionally protected by copyright.

However in France, copyright is a humanist right, attached to the personality of the creator (as a human being). Therefore, creations generated by AI –without human intervention– are *a priori* not likely to benefit from this protection. In the United States, several courts have also ruled against copyright protection for results generated by AI[41].

Various solutions have been put forward to address this issue, some of which have already been the subject of legislative proposals: refusing all protection to AI-generated creations, granting protection to the owners of the rights to the works used by AI to design new content, creating a new typology of intellectual property rights, or even using neighboring rights –which might be better adapted to the economic logic of the protection sought.



41 THALER v. PERLMUTTER Register of Copyrights and Director of the United States Copyright Office (August 18, 2023), United States District Court, District of Columbia, Civil Action No. 22-1564 (BAH).



AI is also changing scientific and industrial sectors, where it can be widely applied. While the results of generative AI may constitute patentable inventions, the possibility of taking advantage of this protection is limited by the current requirement, in Europe, to designate a natural person as the inventor. An inventive process in which an AI has itself identified the technical problem, and generated a solution without human intervention, would therefore today be excluded from patentability. Thus, only inventions in which AI was used as a simple tool available to the human user can be patented, with the latter designated as the inventor.

The definitive legal framework will certainly take shape as the various AI services are deployed and their value enhanced. However, the issue will be inseparable from that of the rights of third parties whose works and content are integrated upstream into learning models, with new problems linked to the value sharing.

Particular attention will also need to be paid to the consequences of the lack of harmonization of legal systems worldwide, with regard to the protection of AI-generated content. In China, for example, the *Beijing Internet* Court recently recognized the copyright protection of AI-generated images. This decision, handed down on November 27, 2023, which appears to be in complete opposition to the initial French, European and American positions, necessarily calls for vigilance in the event of content being exploited internationally.

What risks are associated with the use of AI in and by companies?

In addition to the risks associated with confidentiality and data protection (see Section 2.2 p. 26), the use of AI systems in companies raises a significant intellectual property risk. While it is certainly futile or illusory to seek to fully control or proscribe the use of AI for multiple activities (communications and marketing, IT development, R&D, design, creation, etc.), the integration of AI results in products and services or in corporate communication poses a twofold risk for companies: firstly, a risk of infringement proceedings, and secondly, a risk of weakening their intellectual property rights, which are likely to be challenged.

These risks can be mitigated by both technical means and the implementation of internal procedures.

What impact will AI have on the protection of inventions under patent law?

The use of AI by intellectual property offices can lead to changes in the practice of patent granting procedures (classification, search of prior art documents and automatic translation).

The question also arises as to the impact of using AI when offices examine the validity of patents, at the time of grant or following third-party actions. AI can be used to assess validity conditions such as the existence of an inventive step or the sufficiency of the description. This will entail redefining the notion of obviousness, as well as the machine's level of information: reference to the legal fiction of the person skilled in the art, adopted until now, implies a level of general knowledge of a natural person.

As the strength of titles in this new framework may be compromised, alternative forms of protection, such as trade secrets, will need to be considered.

Artificial intelligence ◆ 2. Legal issues - Intellectual property

How can inventions or content protected by training models be used?

As far as **patent law** is concerned, when AI uses data protected by an existing patent, it is likely to develop an improvement invention. This invention will necessarily fall within the scope of the prior patent. In practical terms, the exploitation of the second invention will be an infringement of the first, and so it will be necessary to obtain a license or assignment of the first invention in order to exploit the second invention freely.

In terms of **copyright**, several complaints were filed in 2023 concerning the use of protected works by AI system training models, but these actions immediately raised a number of questions. As noted by the Conseil Supérieur de la Propriété Littéraire et Artistique (CSPLA) as early as 2020[42], the concrete terms and conditions of use of works by AI systems do not fit well with the conditions for copyright infringement (qualification of acts of reproduction and communication to the public)[43], while the recognition and identification of works used by AI are proving particularly difficult.

> ***These initial developments could have argued in favor of rethinking or adapting intellectual property law to meet the specific needs of AI, but the solutions currently being developed seem to be taking a different path, by imposing new rules on suppliers of general-purpose AI models.***

Following a major mobilization of rightsholders' representatives, the future AI Act (see section 1.2 p. 10) contains a number of initial provisions that seem designed to guarantee the protection of pre-existing works, notably via a principle of transparency regarding their use by AI systems (*detailed summary of the content used*), as well as a general principle of respect for (European Union) copyright and, in particular, the right of opposition that can be put in place by rightsholders (opt-out). The right of opposition is set out in article 4 paragraph 3 of Directive (EU) 2019/790, transposed in France into Article L.122-5-3 of the French Intellectual Property Code. It enables rightsholders to render inoperative the exception, provided for in these same texts, and regarding data mining and authorizing automated data analysis techniques inherent in AI tools.

For copyright rightsholders, the granularity of "*detailed summaries of the content used*" will be decisive in asserting their rights. A template should be provided by the recently created AI Office. Such summaries will have to be disclosed as soon as AI models (including open source models) are releases on the market, but not in the prototyping phase.

The text also includes a particularly noteworthy provision designed to ensure that all suppliers of AI models placed on the market in the European Union will be subject to the same regime, regardless of their country of origin or the territorial organization of their activities, by specifying that the obligation to respect copyright applies "regardless of the jurisdiction in which the copyright-relevant acts underpinning the training of these foundation models take place" *(Recital no. 60(j) of the future AI Act).*

Without even waiting for this new European regulation, many media and organizations representing rightsholders (such as SACEM) have announced that they are exercising their right of opposition to ensure that their protected works and content are not captured and used by AI system training models. The future AI Act seems to validate the relevance of this approach.

However, the effectiveness of the right of opposition still raises serious questions, and the market is looking for standards or norms to harmonize practices. At the same time, other operators have chosen to enter into partnerships with certain generative AI providers, while a revision of Directive (EU) 2019/790 could be put on the Commission's work program for the coming months.

The year 2024 therefore promises to be decisive for the progress of these various projects, and for the emergence of a clear and efficient legal framework for the use of protected content by AI models and systems.

42 Conseil Supérieur de la Propriété Littéraire et Artistique, Mission IA et Culture, Final report of January 27, 2020.
43 Generative AI does not proceed by copying or superimposing pre-existing works or content, but by learning their meaning and characteristic features, for the purpose of recomposition.

2.2 DATA PROTECTION

Authors*:
Thierry Dor - *Partner*
Julien Guinot-Deléry - *Partner*
Aurélie Pacaud - *Counsel*

*The authors would like to thank Gabrielle Lambert for her contribution to this article.

The possibilities offered by AI systems, based in particular on the massive collection of data and the discovery of new uses as they are processed, generate tension with the principles of personal data protection law. In particular, the aim of these principles is to enable data subjects to be informed of the processing of their data and to give them control over such processing. We illustrate this difficult reconciliation through three examples.

Large Language Models (LLM) and the rights of data subjects: how to "unlearn" data?

Data protection law grants data subjects rights, and in particular the rights of access, rectification, deletion and opposition. How can the creators of LLMs, which ingest large quantities of data (including personal data) for their training, enable data subjects to effectively exercise their rights?

Several datasets are involved: the original dataset used to train the model, and then the history of "prompts" submitted to the LLM –which are questions asked to obtain an answer– also used to improve the model. In theory, the aforesaid rights could also apply to the results generated, whether they are accurate or "hallucinations", i.e. incorrect, incoherent or imaginary results.

> ***In practice, exercising the right of objection or erasure would mean that the model stops processing or erases all personal data concerning a person, and thus "unlearns" this data, which raises a number of questions.***

The first approach, "*machine unlearning*", can take several forms, the most obvious of which is to delete all input data on the person concerned, so that the algorithm can no longer feed on it, but also to re-train the model stripped of this data. This would likely generate substantial costs and delays, which would be neither economically viable if the exercise has to be repeated each time a request is exercised, nor compatible with the response time frames provided for in Article 12 of the GDPR, which is a maximum of three months (one month being extendable by two months).

On the other hand, some researchers question the real possibility for a LLM to forget data, insofar as a model's training data exists in its weights and parameters, and is undefinable until it is used to generate a result, the so-called "black box" effect (or "inexplicability" of an AI model).

Other solutions have been explored, such as "reinforcement learning from human feedback", whereby an algorithm learns to perform a task by using feedback from humans to guide its learning. Without having to delete the data or re-train the model, it could be taught to no longer generate any results including certain data, but this would be more of a "workaround" solution, not meeting the obligations of the GDPR, and moreover would not be infallible.

Lastly, for LLMs that include only pseudonymized personal data and do not allow data subjects to be identified without recourse to additional data, another means mentioned in the doctrine would be recourse to Article 11 of the GDPR, which would thus exempt the data controller from responding to exercise requests, in compliance with the data minimization principle, unless the data subject provides additional information that allows his/her identification for the purposes of exercising his/her rights.

There are many scientific studies and articles on the subject, which need to be understood from both a technical and legal point of view.

The importance of the principle of purpose limitation

Case study: a clinical study sponsor collects medical data for cancer research, and realizes during the course of the study that these data can also be used to highlight certain biomarkers responsible for other pathologies (serendipity). When the dataset was collected, the sponsor had no idea of the possibilities it offered, given that the uses revealed themselves as the processing and combinations were carried out.

Similarly, AI systems can be trained on publicly accessible data (via "scrapping" tools), initially disseminated for specific purposes having little to no connection with the training of an AI system.

The question of the infinite reuse of data had already arisen with the advent of Big Data, and is resurfacing in the age of AI, coming up against one of the essential principles of data protection law: the principle of purpose limitation. Stated in Article 5 of the GDPR, it provides that the purpose pursued by the use of personal data must be determined, explicit, and legitimate; **it is thus forbidden to use personal data for a purpose other than the one established upstream of its collection**.

The French Data Protection Authority ("CNIL") reiterates the importance of this essential rule, insofar as it conditions the application of the principles of (i) transparency (data subjects must be informed of the purpose of the processing, so that they know why their personal data is collected and understand how it will be used); (ii) minimization (the data selected must be adequate, relevant and limited to what is necessary with regard to the purposes for which they are processed); and (iii) limited retention periods (data may only be kept for a limited period, defined according to the purpose for which it was collected).

In a context where AI systems are based on *deep learning*, where the more data fed into the model, the more efficient the learning process, the accumulation of data and the possibility of reusing it for as yet unknown purposes are major challenges.

How can the reuse of data by AI systems be reconciled with respect for the principle of purpose limitation?

Under the GDPR, data collected may not be further processed in a manner incompatible with the defined purpose, unless the consent of the data subject is obtained. This means, *a contrario*, that data can be subsequently reused for compatible purposes.

Prior to the adoption of the GDPR, the G29 had addressed the issue of compatibility in its Opinion 2013/03 of April 2, 2013 on purpose limitation. Since then, the criteria for determining the compatibility of further processing have been reiterated in Article 6.4 of the GDPR, but create legal uncertainty by leaving data protection authorities a wide margin of interpretation.

In addition, the GDPR provides for cases where further processing is "presumed" to be compatible, such as processing for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, as long as these are subject to appropriate safeguards in accordance with Article 89 of the GDPR, in particular via pseudonymization.

The GDPR does not provide a definition of scientific research, but its Recital 159 indicates that this purpose should be interpreted broadly, and provides some examples: technological development and demonstration, fundamental research, applied research and privately funded research, or studies carried out in the public interest in the area of public health. The CNIL also provides a set of indicators to be taken into account: the nature of the organization, the method of financing, the novelty of the results obtained, the creativity of the work, the uncertainty of the processing as to the final result, the systematicity of the methodology implemented, and the transferability/reproducibility of the results in a wider field.

In its report on Artificial Intelligence and Privacy, the Norwegian Data Protection Authority questions whether the development and application of AI systems could in themselves constitute "scientific research", irrespective of the field of application, given that the discovery of new knowledge and know-how is inherent to AI systems. One may also wonder whether an AI application in the deployment phase, e.g. an application designed to determine an individual's creditworthiness, could be analyzed as scientific research, especially when the algorithm is continuously learning. Conversely, it is clear that for "*static*" models that simply apply the algorithm and stop training, qualification will be difficult to achieve.

In the Data Protection and Digital Information Bill currently under discussion, the UK has chosen to expressly confirm that scientific research is compatible processing, and to define the notion of scientific research in order to provide greater legal certainty for players in the sector, and to promote research in the health sector.

Finally, in its fact sheets on AI , the CNIL mentions this principle of purpose between the lines, distinguishing between AI systems the operational use of which in the deployment phase is identified as early as the development phase, and those the operational use of which in the deployment phase is not clearly defined as early as the development phase (general-purpose AI systems). It interprets this principle flexibly, giving recommendations on the conformity of a purpose defined very broadly at the development stage. For example, the foreseeable capabilities of the AI system that present the greatest risk in the operational phase (e.g., the case of AI systems identified as "high-risk" under the future AI Act, see section 1.2 p. 10), functionalities excluded by design, or examples of operational use cases or purposes of the AI system (e.g., traffic regulation for a computer vision system capable of detecting and quantifying vehicle flows) should be mentioned.

As the CNIL has not rendered any public decision on what makes further processing compatible or incompatible since the GDPR came into force, it will be interesting to follow its approach with regard to the uses of AI systems.

Generative artificial intelligence, voice deepfakes and biometric data

Hollywood actors on strike against generative AI systems, dubbing actors united in an international collective at the last Cannes Film Festival: technologies enabling the creation of image or voice "scans" or synthesis, and no longer requiring the presence of actors, are multiplying. As a recent example, a teaser for the spinoff series "The Walking Dead": Daryl Dixon was released, featuring the voice of actor Norman Reedus' French dubbing voice actor, without the latter's participation in the recording.

The beginnings of what are commonly known as *deepfakes* appeared in 2017 on the "Reddit" platform. Since then, numerous examples have made headlines, from the video of Barack Obama insulting Donald Trump, to the deepfake voice of English actress Emma Watson reading "Mein Kaempf" on the 4chan platform.

How is this possible?

ElevenLabs, Murf, Play.ht, HeyGen... these are just a few of the increasingly powerful voice generators that can synthesize voices using the *deep learning* technique known as "generative adversarial networks" (GAN). This technique pits two algorithms against each other: the first, known as the *generator*, creates the most plausible content possible, then the second, known as the *discriminator*, seeks to detect the errors produced by the first. The two algorithms progress in this way until the first generates content in which the second can no longer detect any errors (or at least errors so minimal that they would escape the human eye or ear)[44].

What are the legal issues raised by these uses?

Independently from issues relating to rights to publicity or other personality attributes, protected as falling within the scope of "private life" under Article 9 of the French Civil Code, and which can only be exploited under well-defined conditions, certain attributes unique to an individual such as a fingerprint, iris or voice constitute biometric data that are subject to special protection as "sensitive" data, under the regime of Article 9 of the GDPR. Thus, as a matter of principle, it is prohibited to collect and process biometric data without falling within the scope of one of the exceptions restrictively listed in the same article.

What is the reason for this? Biometric data is data that enable or confirm the identification of an individual by his/her physical, physiological or behavioral characteristics. As the CNIL has pointed out, "they are produced by the body itself and characterize it in a definitive way. They can sometimes be used to track and identify an individual, even without his/her knowledge. This data is particularly sensitive because it is permanent".

> ***A person is indeed recognizable by his/her voice, which is unique to that person.***

The use of voices generated by artificial intelligence thus entails numerous risks for the individuals concerned. Examples abound: voice cloning to reproduce the voice of a loved one on the telephone to demand a sum of money, or to simulate an attempted kidnapping in order to receive a ransom.

In another case, a voice identification system, presented as a reliable means of identification, was "fooled" by an AI-generated voice. Using a clone of his voice created by ElevenLabs, a journalist managed to fool Lloyds Banks' voice identification system and access his bank account by conversing with the voice identity verification tool.

Is the use of these voice generators legal?

The implementation of this system will have to comply with the provisions of the GDPR, and in particular those of the aforementioned Article 9. The relevant exceptions are limited and impractical: would it be possible to obtain consent from individuals for the use of their voice recordings? This is doubtful, given the reputational, financial and legal risks that such use raises for the individuals concerned. Could these voice recordings be considered to have been manifestly made public by the person concerned? The European Data Protection Board (EDPB) points out that this exception must be interpreted restrictively. Moreover, any dissemination by an individual of an audio or video recording concerning him/her seems difficult to reconcile with a desire to make public biometric data that is inseparable from these recordings. The question therefore remains open.

It is worth noting that the use of such systems could be punishable under criminal law for identity theft or infringement of personal portrayal. Finally, the draft bill to secure and regulate the digital space, known as the "SREN" law, proposes to supplement article 226-8 of the French Criminal Code to expressly punish the dissemination of content about a person generated by artificial intelligence without that person's consent, if it is not obvious that the content is algorithmically generated or if it is not expressly mentioned.

44 Gleize B., Maffre Baugé A., under the scientific direction of Bruguière JM. and Fauchoux V., Deepfakes : faut-il légiférer?, Revue Lamy Droit civil, n°181, 1er mai 2020

2.3 COMPETITION

Authors:
Laura Castex - *Partner*
Sofia Vukovic - *Associate*

Confronting AI with competition law may seem surprising. However, consideration must be given to this subject: AI may serve anti-competitive purposes or consolidate dominant positions.

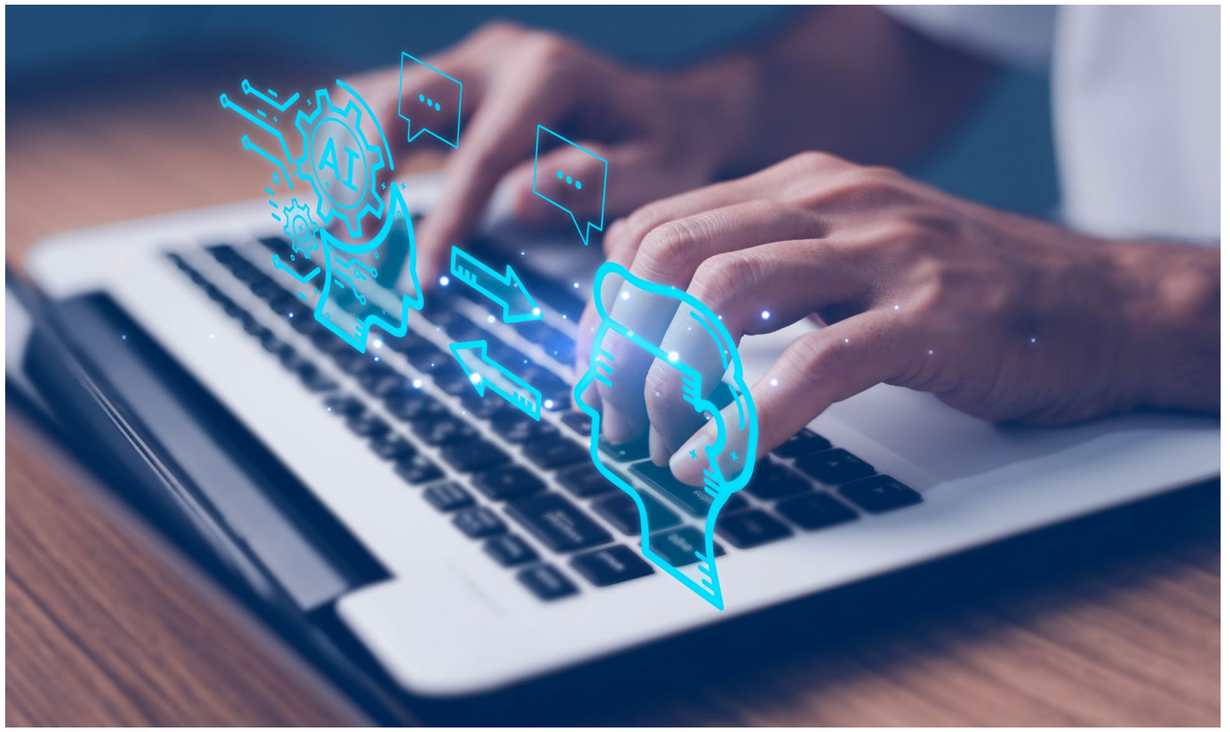
NB: While virtual worlds and generative AI systems are rapidly evolving, the European Commission wishes to carry out a prospective study on the impact and risks raised by these technologies when it comes to competition law. To this end, it has launched a call for contributions on these two topics, accessible here. Interested parties may submit their input until March 11, 2024. As for the French Competition Authority, it initiated *ex officio* an inquiry on the competitive situation in the generative AI sector, and also launched a public consultation until friday March 22, 2024, accessible here.

AI as a potential vector for collusion between competing companies

Competition law prohibits agreements or concerted practices that have the object or effect of restricting competition, including exchanges of sensitive information between competitors that may contribute to the coordination of their behavior. Traditional anti-competitive practices are based above all on contacts –direct or indirect– between human beings (agreements, exchanges of sensitive information).

While the adoption of parallel behavior on a market does not constitute a collusive practice when it is the result of autonomous and individual choices by each operator, the increasing use of AI-based tools may raise questions when it leads to an alignment of behaviors on the market, both in terms of breach of competition law and liability of the user companies.

The risks associated with algorithms, and by extension AI technologies, are expressly mentioned in the new Guidelines on horizontal cooperation agreements published in July 2023 in §379: *"[...] algorithms can also be used to monitor (pre-existing) anti-competitive agreements between competitors. When used as part of an act of collusion, price monitoring algorithms can increase market transparency, detect price deviations in real time and make punishment mechanisms more effective. Undertakings can also use behavioral coordination algorithms to agree on essential parameters of competition. Algorithms then become a device to facilitate collusion (collusion by code)."*



Competition authorities are paying particular attention to pricing tools that incorporate algorithms that make it possible to monitor market changes almost in real time and react instantly (or even automatically) by dynamically adjusting prices, because of their potential anti-competitive effects. Similarly, AI can contribute to the emergence of tacit collusion between companies.

While using deliberately and in a concerted way AI tools as support for a collusive agreement between companies or to facilitate its implementation does not raise any doubt as to its anti-competitive nature, this possible qualification, where applicable, is more complicated when an alignment of behaviors results, for example, from the use by competing companies of the same AI tool supplied by third parties or tools, developed internally or by third parties, with similar objectives or functionalities.

From a competition law perspective, the assessment should notably address the following questions:

- Is the design of the AI tool or its configuration intended to enable the alignment of key competition parameters between economic operators (e.g. prices)?
- Were the user companies aware that their competitors were using the same tools or were using the services of the same AI supplier?
- Did the user company know or could reasonably have foreseen that the tool was intended or was likely to lead to anti-competitive conduct?
- Did they sufficiently distance themselves from anti-competitive behaviors to avoid being held liable?

The AI tools used by economic operators may also give rise to risks with regard to competition law either when they interact with each other, potentially characterizing a form of "communication" between companies or exchange of sensitive information, or when they are based on data sharing –particularly from competing operators (e.g., "learning" AI or generative AI tools that need to process a large volume of data to achieve optimal efficiency).

The risk of tacit collusion in connection with AI-based technologies and the liability of user companies were already mentioned back in 2017 by European Commissioner Margrethe Vestager: *"[...] companies can't escape responsibility for collusion by hiding behind a computer program. What they can –and must do– is to ensure antitrust compliance by design"*[45].

> ***Companies are therefore invited to incorporate compliance with competition law from the early design stage of AI-based tools, through the notion of compliance by design.***

While this requirement seems achievable in the context of the internal development of AI tools (and sufficiently traceable if justifications are required by a competition authority), both at the level of the design and configuration through the cooperation between legal and technical personnel, the expectations expressed by competition authorities in the case of AI tools supplied by third parties may appear severe. Indeed, given the sophistication of such tools (which will only increase over time), what degree of understanding should a user company have of the underlying design rules and the specific configuration of a tool offered by a third-party supplier (if this third party is ready to disclose such details) and what evidence should it submit to justify that such tool is *compliant by design* or, at the very least, that the company carried out sufficient due diligence to make sure of this?

AI and market power

By giving their users a major competitive advantage, AI-based technologies are subject to specific considerations, particularly with regard to the prohibition of abuse of a dominant position.

A company that acquires a strong market position thanks to its exclusive access to an AI tool (either because it owns it or because it holds exclusive rights over its use), or because it is its only supplier, must be particularly aware of its special responsibility as far as competition law is concerned and refrain from implementing practices that may be considered abusive.

45 Speech of March 16, 2017 at the 18th Bundeskartellamt Competition Conference, quoted in the joint study "Algorithms and Competition" by the Bundeskartellamt and the French Competition Authority published in 2019.

In particular, if AI-based technologies are, or become, essential for the access of third-party operators to certain markets, these technologies could qualify as an "*essential facility*". This could entail, under certain conditions, the risk that denying access to this technology, or discriminatory access conditions thereto, be qualified as abusive practices, and that the company exploiting such technologies be held liable.

Competition authorities can impose on a company exploiting an AI-based technology that is considered an "essential facility" that it provide access to it, for example by granting licenses to operators –even competitors– under reasonable and non-discriminatory terms, but also by disclosing information (such as protocols and technical standards) required to enable interoperability between the technology in question and third-party tools. The solution adopted by the European Commission in the Microsoft decision of 2004, whereby Microsoft was required to disclose certain information necessary for the development of compatible products likely to integrate with Windows workgroup networks (without disclosing the source code), could thus be transposed to AI-based technologies considered to be essential.

AI can also be a way to strengthen the market power of a company holding a dominant position. While such strengthening is not prohibited per se, when AI is designed or configured by a company in such a way as to favor its own position (*self-preferencing*) or disadvantage its competitors, the company exploiting this technology may be held liable for abusive practices. In this respect, the approach taken by the European Commission in the 2017 Google Shopping case (upheld for the most part by the General Court of the European Union), in which Google was sanctioned for artificially favoring (via the algorithms determining their display) its own price comparator on its general search engine to the detriment of those of its competitors, could also be transposed to AI-based technologies.

As a result, user companies must be vigilant when it comes to the design and configuration of their AI tools to avoid incurring risks under competition law.

Finally, another concern in terms of market power in relation to AI-based tools, and in particular generative AI technology, is the possession and use of large volumes of data required to develop and train the tools. Where access to data is essential for the very development of AI, under certain conditions databases may themselves constitute an "essential facility"[46].

AI and merger control

Merger control does not escape certain specific concerns associated with AI, whether when analyzing the impact of a transaction on competition or possible commitments offered by companies to remedy any competition concerns as the case may be.

> Competition authorities tend to pay particular attention to mergers involving, in whole or in part, AI technologies, which may constitute innovations or confer significant competitive advantages to their users. The same considerations apply to transactions involving operators holding large volumes of data that could be used to develop new technologies or services.

As the US Federal Trade Commission recently pointed out, competition authorities are concerned that certain companies might consolidate their market power through mergers and acquisitions in the field of generative AI. Operators could be tempted to take control of AI technologies in order, for example, to reserve said technologies for their own benefit while depriving their competitors access thereto, and in so doing, strengthen their position, complete their portfolio of technologies or even hinder the development of competing tools (*killer acquisition*).

Although in certain circumstances the operators concerned could remedy competition concerns by offering commitments (see some examples in the above-mentioned section "AI and market power") to avoid a prohibition of the planned transaction, designing remedies may be difficult in an area involving sophisticated and evolving technologies. For example, the European Commission prohibited Booking's takeover of eTraveli because not only did it consider that the commitments proposed by Booking were insufficient, but also that it would have been difficult to monitor them, in particular because Kayak's algorithm operates like a black box (i.e. algorithms that are difficult to interpret even if the source code is accessible).

46 See the joint study "Competition law and data", published in May 2016 by the Bundeskartellamt and the French Competition Authority.

2.4 BANKING AND FINANCE

Authors:
Stéphane Puel - *Partner*
Guillaume Goffin - *Partner*
Franck Guiader - *Head of Gide 255*
Matthieu Lucchesi - *Counsel*
Rudolf Efremov - *Associate*

For several years now, the banking and financial sector has been undergoing a major digitalization process, with the emergence of digital applications and the automation of certain tasks. The use of AI by players such as credit institutions, investment firms, portfolio management companies, etc., is part of this trend. It appears to be an ideal response to certain challenges facing this industry, such as the search for greater efficiency and expanded analytical capabilities in an increasingly complex economic and regulatory environment.

AI in the banking and financial sector presents specific challenges compared with the digitalization that has developed to date, particularly in terms of the systems' autonomy and the emergence of new risks. In this particularly regulated sector, these challenges raise specific legal questions relating to the impact of AI on compliance with technology-neutral regulations.

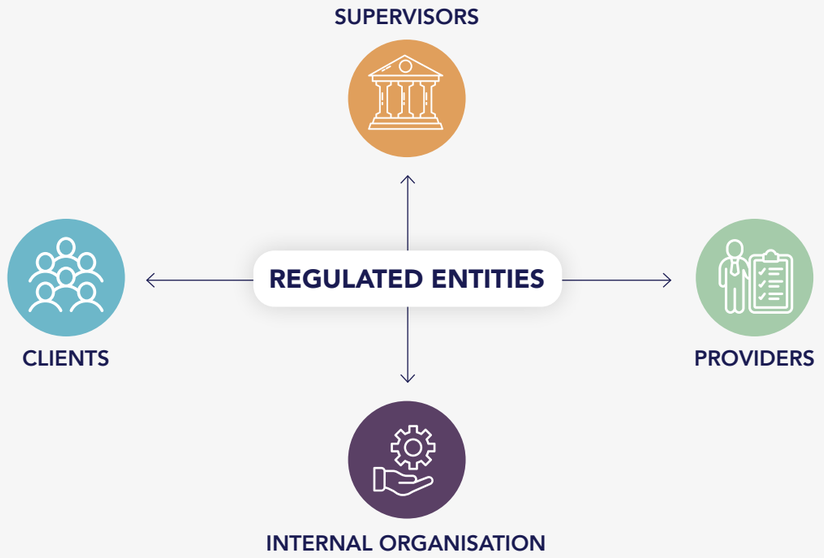
These challenges appear in all the implications that the regulated players may have, particularly in their relations with customers and external service providers, but also in their internal organization and in their links with the sectoral supervisory authorities.

What are the legal challenges of AI in customer relations?

In many cases of use of AI in the banking and financial sector, the ambition of the AI system is to improve the service provided to customers by regulated entities, for example for the provision of automated investment advice (or *robot-advice*), the execution of customer orders or the analysis of an individual's borrowing capacity.

AI then aims to improve the quality of the service provided, in particular through increased data processing power or faster handling of customer requests. AI systems can interact directly with customers on behalf of the regulated entity (e.g. *chatbots*); they also often support the regulated institution's teams to help them serve their customers better. The use of AI raises here the question of the ability of these systems to meet the obligations of regulated entities towards customers, the proof of a possible breach and, where applicable, the related liability.

AI IN THE BANKING AND FINANCIAL SECTOR
Global Legal Challenges



For example, when AI is used to provide clients with automated investment advice on financial instruments, the system must enable the firm to carry out the checks required by financial regulations, in particular that the proposed recommendation's suitability in the light of the client's characteristics[47]. The AI system must therefore be structured to integrate all the information that the regulations require to be retrieved from the client, and to process it in an auditable and clear manner. The *Autorité des marchés financiers* (French Financial Markets Authority - "**AMF**") has already indicated that it will carry out SPOT inspections in 2024 in the field of investment advice delivered on an automated basis to retail clients.

To this end, certain AI systems can be structured soas to increase transparency for clients with respect to the elements justifying the proposed recommendation. A study was carried out in 2023 by the Autorité de contrôle prudentiel et de résolution (French Prudential Supervision and Resolution Authority - "**ACPR**"), in partnership with Télécom Paris[48], on life insurance contracts (see section 2.4 p. 33), but its conclusions can probably be extended to the entire financial sector. According to this study, "explanations provided in the form of a conversation wrongly increase the users' trust in the incorrect proposals made by the robo-advisor"[49].

These conclusions highlight the key legal issues relating to AI for this type of use cases, in particular: (i) pre-contractual information and the contractual provisions binding the customer and the regulated entity to ensure that the customer is fully informed about the nature of the service provided and its scope, and to limit undue liability; and (ii) the explicability and calibration of AI tools to ensure that they meet the regulatory requirements to which the regulated entity is subject.

This is also a point of attention for ESMA, which has also published recommendations on this subject, stating that advisers must inform the client that the advice will be made on the basis of information provided by the client (without there necessarily being any human intervention in the process)[50].

As indicated in Section 1.2 p. 10, the future AI Act intends to impose a specific regime for high-risk AI systems. The use of an AI system to assess the creditworthiness of natural persons is considered high-risk. Credit institutions using such a system will have to ensure that they comply with the specific requirements set out in this new Act.

What are the legal challenges of AI in relations with service providers?

The introduction of AI in the banking and financial sector often require the regulated entities to rely on technical solutions provided by external service providers acting in different ways (infrastructure providers or service providers/subcontractors, etc.).

Depending on the nature of the regulated entity and its activities, banking and financial regulations generally lay down precise conditions under which these entities may entrust all or part of their tasks or underlying systems to third parties. The purpose of this framework is generally to ensure that they have control over external service providers and that a clear chain of responsibility is defined.

For AI use cases involving the outsourcing of essential services by regulated players, it will be essential to ensure compliance with this applicable framework. In this respect, one should keep in mind the specialization of AI players and the emergence of key leaders in this technology. Despite the leadership position of certain providers on the market, banking and financial players will have to ensure that they retain autonomy and the ability to supervise the providers in a way that is compatible with their regulatory obligations. Moreover, any such use of a third-party service provider should also be carried out in accordance with Regulation (EU) 2022/2554, known as "DORA", which comes into force in 2025.

What are the legal challenges of AI in the internal organization of regulated entities?

First and foremost, it seems essential for regulated entities to identify all the AI systems used within their organization. This mapping is the key to being able to supervise their operation according to the appropriate procedures.

In this respect, as indicated in section 1.2 p. 10, the future AI Act imposes a specific regime for AI systems, categorizing them according to the level of risk that the use case presents. For example, this list defines as high-risk the AI system used for certain human resources processing. Institutions will have to ensure that they precisely map the AI use cases in their organization and comply with the dedicated framework of the future AI Act according to the nature of the risks they present.

Second, in view of the applicable sectoral regulations, the implementation of AI systems within entities in the banking and financial sector requires, whatever the use case(s), the integration of these systems into the internal governance systems, the IT risk management system, and the permanent and periodic control systems.

> ***Internal governance must also include monitoring and control systems appropriate to the specific AI-related issues.***

In 2020, the ACPR emphasized the importance for the players under its jurisdiction to adopt "operational procedures (…) adjusted to the different activities performed, communicated, and periodically updated (…), to describe how the various levels of responsibility are assigned, the resources devoted to internal control mechanisms, the risk measurement, mitigation and monitoring systems implemented, and the organization of compliance monitoring"[51]. The internal control and risk management system must be adapted accordingly.

On this point, some regulated entities already have to take IT risk into account, in accordance with the provisions set out in the Order of November 3, 2014, as well as the notice published by the ACPR on this subject and the EBA's guidelines. The DORA Regulation also imposes cybersecurity and operational resilience requirements (including obligations to adopt a strategy to manage these risks, map risks and carry out stress tests).

Finally, regulated entities are also subject to level two (permanent control) and level three (audit) internal control requirements. This implies integrating artificial intelligence tools into control plans and providing the teams in charge of these controls with the adequate resources and training be able to verify whether the artificial intelligence tools operate in compliance with the applicable regulations.

As noted in Section 1.2 p. 10, the future AI Act requires internal organization, including an appropriate risk management framework, for high-risk AI providers and users. Where the latter are subject to sector-specific requirements, such as many banking and financial players, the future AI Act enables existing internal control processes to be capitalized on, in order to meet some of the obligations introduced by the new Act. However, the future AI Act does not specify how it articulates with sector-specific legislations. The sectoral regulators will hopefully clarify this in their forthcoming doctrine.

47 See in particular: French Monetary and Financial Code, art. L.533-13.
48 Questioning the ability of feature-based explanations to empower non-experts in robo-advised financial decision-making, Astrid Bertrand, James R. Eagan, Winston Maxwell, June 12, 2023.
49 La motivation du conseil par les robo-advisors : vers un éclairage apporté aux clients?, ACPR Review, July 2023.
50 See ESMA, Guidance on certain aspects of the MiFID II matching requirements, ESMA35-43-3172, April 3, 2023.
51 Governance of artificial intelligence in Finance - Discussion document, ACPR, June 2020.

What are the legal challenges of AI in relations with regulators?

The European authorities, and French authorities in particular, have clearly identified the challenges of AI development for the banking and financial sector, both to use it themselves and to supervise its implementation by the entities they supervise.

The authorities are therefore attentive to the use cases that can be applied to their own activities.

- As an example, the Banque de France published a call for evidence on the uses and impact of generative AI on its activities and missions[52], the finalists of which were published in July 2023[53].
- As for the AMF, it recently published a study on the opportunities linked to the use of natural language processing to automatically analyze risk factors published by listed companies[54].
- The ACPR already uses AI tools as part of its supervisory missions. In a 2022 decision, the ACPR's Commission of Sanctions stated that the use of AI tools does not affect the legality of an inspection procedure, even though the AI tool increases the authority's analytical capabilities tenfold and the use of this tool was not disclosed to the entity inspected prior to the procedure. In the Commission's view, the use of this type of tool by the ACPR remains compatible with the supervisors' duty of loyalty, particularly where the supervised entity was not prevented from presenting its observations in its defence[55].
- The AMF identifies artificial intelligence as a major recent development in terms of innovation in the financial sector. It actively contributes to ongoing regulatory discussions on this subject at international and European levels. In particular, within the International Organization of Securities Commissions (IOSCO), it has led the work on the financial stability risks induced by artificial intelligence.

For the regulated players that the authorities supervise, the use of AI systems must remain compatible with the ability of banking and financial players to ensure ongoing compliance with the obligations applicable to them. Nor should it hinder the ability of their authorities to control them. In order to meet these requirements, AI systems must allow for the auditability of their operation, in particular through the transparency of their calibration and the traceability of the results they have produced.

More broadly, while the authorities regularly highlight the opportunities that AI presents for the sector, they also generally point out the potential associated risks. At the 2023 AMF-ACPR Fintech Forum, for example, the AMF recently reiterated that it would pay attention, in particular to the accuracy and reliability of certain AI models, their possible lack of transparency, as well as cybersecurity and personal data protection issues[56] (see section 2.2 p. 26).

As indicated in section 1.2 p. 10, the future AI Act provides for a specific supervisory mechanism, including a European level and a national level. At national level, local legislation will have to define the competent authorities on their territory. In France, responsibility for the future AI Act has not yet been assigned to a specific institution. In any case, this competence will have to be articulated with that of the sectoral authorities for banking and financial players. The future AI Act itself encourages this linkage to ensure the effectiveness of supervisory mechanisms *(Recital no. 80, future AI Act)*.

The integration of AI into the banking and finance industry has an impact on all the relationships between industry players and their stakeholders, whether customers, external service providers or supervisory authorities. It also forces them to adapt their internal organization to ensure compliance with their own regulatory framework. These impacts have their specific legal challenges, often related to a need for transparency and resilience and the definition of a clear chain of responsibility. The analysis and handling of these legal challenges are crucial to the ability of players such as credit institutions, investment firms and portfolio management companies to take full advantage of AI and the opportunities it offers.

52 Call for papers: What uses and impacts of generative AI on the activities and missions of the Banque de France?, Banque de France, May 25, 2023.
53 The Banque de France closes its Call for Papers on generative AI, Banque de France, July 12, 2023.
54 Automatic analysis of risk factors published by listed companies: a use case of natural language processing for the AMF, AMF, January 2023.
55 ACPR Commission des Sanctions, decision of December 1, 2022, procedure no. 2021-05.
56 Speech by Marie-Anne Barbat-Layani, AMF Chairman - AMF-ACPR Fintech Forum, 16 October 2023.

Artificial intelligence ◆ 2. Legal issues - Banking and finance

Focus on the asset management industry

Having been directly exposed to technology and data processing for several decades, asset management companies have naturally come to use AI as part of their modus operandi, and are also confronted with it indirectly through the many interactions they have with their partners who use it (data suppliers, distributors, custodians, etc.).

Subject to numerous regulatory obligations, the use of AI in asset management is part of a search for operational performance and the digitalization of investor processes and relationships. Initiatives driven by new competition in terms of innovative investment solutions (e.g. "crowdfunding", "tokenization" of real assets, "robo-advisers") should also encourage asset managers to look to AI for possible development and sources of optimization.

As a result, the asset management sector could see many opportunities for growth in AI, particularly through their increased capabilities in enhanced data processing, better risk identification, and easier handling of certain low value-added tasks.

For example, AI tools could help reduce the time spent processing news-related information, preparing investment funds' periodic communications, or drawing up initial recommendations for their clients.

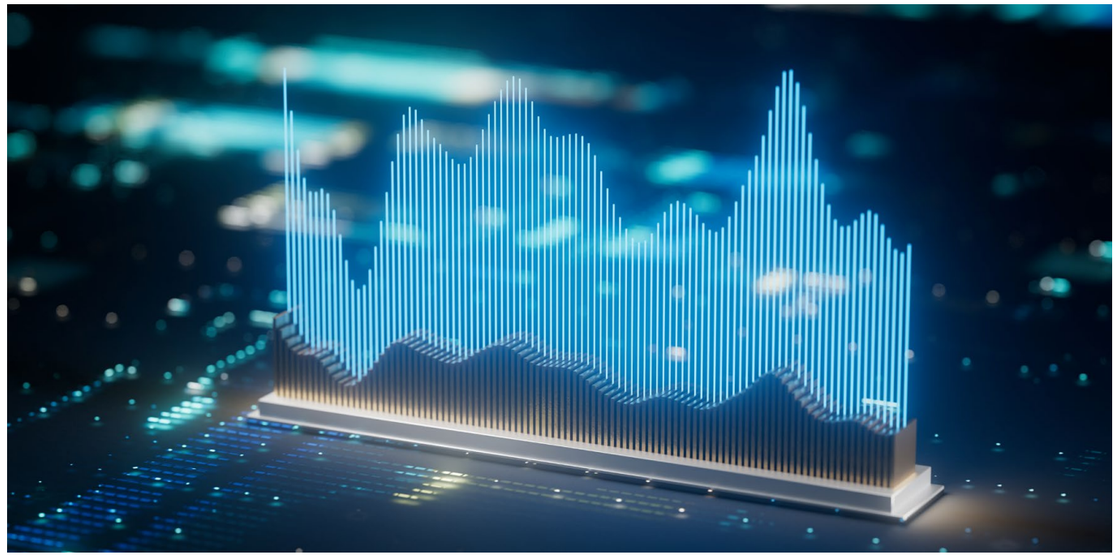
In terms of financial management, AI could also save a considerable amount of time in sorting out financial information, especially in quantitative management, where large volumes of data are used on a massive scale, and in thematic management, which is based on specialized areas of expertise where learning is gained by experience.

However, the legal issues behind the use of AI in asset management are numerous. Firstly, the programming of AI tools creates a significant risk of bias that could lead, for example, to a certain form of financial exclusion, as well as to errors of analysis, both for financial management and risk management. The latter risk is likely to put asset management companies in breach of their obligations to align their interests with those of their clients.

Secondly, AI tools –which can be complex– should not prevent asset managers from explaining investment decisions to their clients, and justifying the allocations they have made in a given market context over a given period.

The detection of unusual events and any form of risk identified by AI tools will also have to support the internal experts who bear this responsibility.

Finally, certain ESG issues will also have to be taken into account in terms of responsible AI, where certain uses could lead, for instance, to a disproportionate energy footprint. More generally, management companies will need to know how to use AI in compliance with their obligations, particularly in terms of cybersecurity and data use, all the while taking into account the information declared in their program of activities.



2.5 INSURANCE

Authors:
Richard Ghueldre - *Partner*
Constantin Beytout - *Associate*
Thomas Jardin - *Associate*

In light of the development of AI systems, the European Commission presented in April 2021 the Proposal for an AI Act aimed at providing a framework for the use of such solutions, notably in the insurance sector.

The future AI Act offers an opportunity to set out some initial thoughts, first on the increasing practical application of such solutions by the various insurance sector stakeholders and, secondly, on certain regulatory and prudential constraints attached to them.

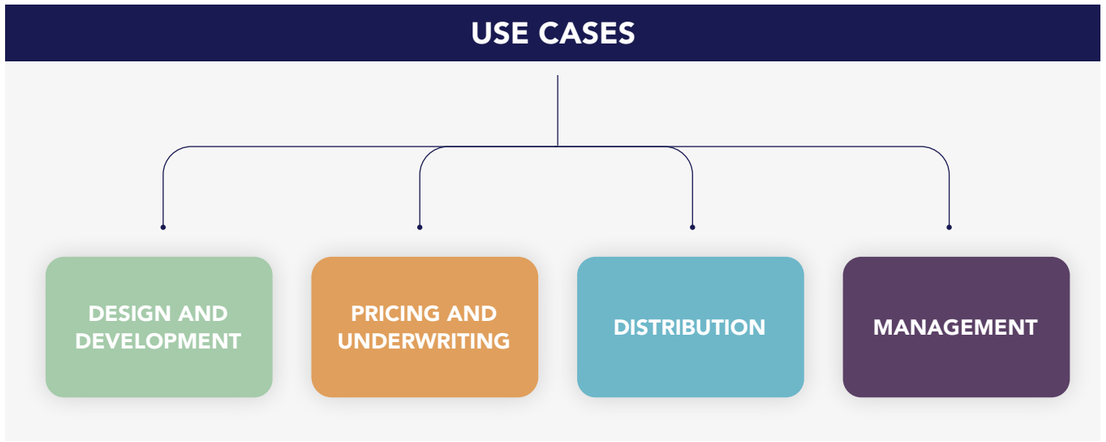
What areas of application for insurers and insurance intermediaries?

In view of the possibilities offered by AI systems, the European Insurance and Occupational Pensions Authority ("**EIOPA**") drew up, in a Report on AI Governance Principles published in June 2021, a list of AI use cases applicable throughout the insurance contract value chain.

For example:

- **with regard to product design and development**, AI makes it possible to analyze historical customer data, in particular based on their use of connected objects (vehicles, watches, etc.), to develop new products *(used-based insurance).*
  The collection and use of this data raises issues of personal data protection (see section 2.2 p. 26) and liability (see section 1.4 p. 19);
- **in terms of pricing and underwriting**, the growing amount of data available in the age of *Big Data* means that insurance products can be priced ever more precisely, taking into account all the particularities of each policyholder's personal situation.
  In this respect, the question arises as to how to maintain the principle of mutualization as a characteristic of the insurance transaction, or as to the persistence of the traditional informational imbalance that Article L.113-2 of the French Insurance Code aims to correct, by requiring that the policyholder precisely answer the questions asked by the insurer, notably in the risk declaration form.
  Consideration will also need to be given to whether or not the provisions applicable to intentional or unintentional misrepresentation on the part of the insured (see Articles L.113-8 and L.113-9 of the French Insurance Code) should be amended in the light of the information available to the insurer upon subscription;
- **In terms of distribution of insurance products**, one of the primary applications of AI systems is the use of chatbots.
  In this respect, as mentioned above (see section 2.4 p. 33), the ACPR and Télécom Paris conducted a study in June 2023 on these robo-advisors, which highlighted the fact that their use was not likely to eliminate any risk of breach of the duty to inform and advise that is incumbent on insurance distributors (see in particular Article L.522-5 of the French Insurance Code, applicable to capitalization and life insurance contracts).
  In this study, it was considered that the explanations provided in this context did not necessarily improve fictitious policyholders' understanding of the insurance proposal, and in fact sometimes wrongly increased their confidence, which was all the more detrimental in the event that the robo-advisor proposed a contract that did not necessarily meet the policyholder's demands and needs.
  Yet, as the European Commission pointed out in a 2019 communication: *"AI systems should support individuals in making better, more informed choices in accordance with their goals"*;
- **in terms of contract management**, AI systems could (i) improve claims management, notably by using image recognition to estimate damages, (ii) increase the effectiveness of the fight against fraud through better detection of anomalies and identification of fraud patterns, or (iii) facilitate the search for beneficiaries in the fight against escheated contracts through the analysis of a mass of documents, notably those available in open source.

More generally, the question of the legal status of designers/developers of AI systems designed to market or manage insurance contracts could also arise, particularly if they were considered to be involved in a distribution activity within the meaning of Article L.511-1 of the French Insurance Code.



What are the implications for governance and supervisory requirements?

EIOPA points out in its Report on AI Governance Principles that *"the toolset provided by AI to insurance companies presents risks that will require regulatory and supervisory oversight"*.

Therefore, in addition to general provisions applicable to AI users or providers, the future AI Act specifies more particularly as regards insurance undertakings that:

- they are subject to specific rules and requirements in terms of internal governance and risk management, which apply even when they make use of AI solutions.
  Accordingly, and in order to ensure the consistent application and implementation of the obligations arising from the future AI Act and European financial services regulations, including insurance regulations, the supervisory authorities in this sector should be responsible for monitoring and controlling the rules relating to AI use cases *(Recital no. 80, Proposal for an AI Act);*
- particular attention needs to be paid to the use of AI systems in relation to access and right to certain services.
  In particular, when these systems are used to determine whether services should be refused or reduced, they can affect people's livelihood and infringe their fundamental rights, such as the right to social protection, the principle of non-discrimination or the right to human dignity *(Recital no. 37, Proposal for an AI Act).*
  In this context, AI systems intended to be used to make or substantially influence decisions on the eligibility of natural persons for life or health insurance have been classified as "high risk" by amendment no. 723 adopted by the European Parliament on June 14, 2023 (see section 1.2 p. 10).

Thus, the use of AI entails that insurers adapt their system of governance, with Article L.354-1 of the French Insurance Code requiring this system to be subject to "regular internal review".

In particular, insurers' governance systems must take account of the impact of AI (i) both internally, in terms of the skills required of members of the board of directors or supervisory board, as well as of those in charge of key functions, and (ii) externally, in the context of the supervision of outsourced activities by insurers and the ACPR.

(i) While recalling the principle of proportionality, EIOPA invites insurance companies to clearly define in their internal policies the various roles and responsibilities of the staff involved in AI processes, and lays down certain governance principles in this respect:

- regarding board members, EIOPA specifies that they bear the ultimate responsibility for the use of AI in the company, and that they must have a sufficient understanding of how AI is used in their respective organizations and of the potential risks involved.
  The board of directors or supervisory board, as the case may be, must be regularly informed to enable it to understand the deployment and use of AI, particularly for AI use cases that are significant given their potential impact;
- concerning key function managers, EIOPA specifies, for example, that:
  - the compliance function must monitor the catalog of AI tools deployed in the company and ensure that they meet the new regulations;
  - the internal audit function must assess both the quality and effectiveness of algorithms and of the governance system, and implement appropriate controls.

(ii) As the ACPR pointed out in a discussion paper in June 2020, financial institutions use various types of third-party service providers to develop their AI: design and development can be entrusted to an external company, and the hosting and operation of AI systems can be outsourced to a traditional hosting provider or a cloud service provider.

In this respect, the ACPR stresses that the implementation of outsourcing requires provision for the reversibility of outsourced AI solutions, and must be preceded by an *ex ante* risk analysis. In addition, the insurer must be able to access the source code and models, and offer the same guarantee to the supervisor in order to enable an inspection covering systems, software code and data.

The ACPR could thus qualify, in certain hypotheses, the outsourcing of AI solutions as the outsourcing of an important or critical operational activity, within the meaning of Articles L.354-3 and R.354-7 of the French Insurance Code, which require prior notification of the ACPR via a dedicated form (see Instruction 2020-I-09, recently amended to include outsourcing to a cloud service provider).

In this case, both the insurer and the ACPR will have effective access to all information relating to outsourced functions and activities, including the possibility of on-site inspections on the service provider's premises (see Article 274 4. of the Delegated Regulation supplementing Solvency II Directive).

In anticipation of the entry into force of this new cross-functional regulation, the challenge for insurance companies is therefore to seize the opportunities offered by AI systems, while making their governance system evolve in compliance with a new regulatory framework, and under the control of supervisory authorities.

2.6 MERGERS AND ACQUISITIONS

Authors:
Louis Oudot de Dainville - *Partner*
Ghizlen Sari-Ali - *Counsel*
Pierre-Antoine Degrolard - *Counsel*

AI is forcing its way into every aspect of our professional and personal lives, and the economic fabric is not spared, regardless of the sector of activity. Companies specializing in AI, and in particular generative AI, are thus increasingly attractive targets for investors. In France, this noticeable trend since 2020 has increased during 2023.

As an example, Mistral AI, OpenAI's French rival, just recently raised 385 million euros less than 6 months after raising an amount of 105 million euros, which was already a record for a French start-up. This second round of financing valued the French start-up, created in May 2023 and specialized in generative artificial intelligence, at almost 2 billion dollars.

However, investing in a company specialized in AI requires a purchaser to bear in mind certain specific points. Notably, AI within the context of a M&A transaction requires an in-depth legal analysis in order to identify potential risks that should be taken into account during the drafting and negotiation of the contractual documentation relating to the transaction.

Identification of specific risks relating to AI

The conduct of a legal due diligence on a target company specialized in AI is essential, even if this may seem difficult given that the AI tool is often derived from a set of data and models that absorb and analyze a significant amount of information. The due diligence will make it possible to legally assess the risks and constraints relating to the model and its objectives, notably in terms of compliance with applicable regulations, certain elements of which are currently being determined through the future AI Act.

Intellectual property rights

Intellectual property rights are critical for companies active in the AI field. The main issues are relating to the protection of AI innovation (intellectual property, trade secrets, etc.), but also the protection of results generated by AI and the legality of the use of training data (see section 2.1 p. 23).

AI contracts

The due diligence phase will also reveal which contracts are the most important for the target's business, such as licenses, service contracts, maintenance contracts, development contracts, etc., as well as the types of customers that the target caters to (private companies, BtoC, public entities, etc.).

Purchasers should pay particular attention to the way clauses relating to change of control, duration, termination, price, liability or quality of services are drafted in these AI contracts.

Points to bear in mind for the drafting of the contractual documentation

> ***As AI raises specific risks, it seems necessary to adapt the provisions of share purchase agreements in order to adequately cover AI-related risks.***

Regulatory aspects

The transfer of AI technology ownership is increasingly subject to a careful examination by regulatory authorities, notably in terms of foreign investment control and merger control.

Control of foreign investment in France

The rules governing foreign investment in France, which require prior authorization from the Minister of the Economy for certain foreign investment transactions in so-called sensitive activities, have steadily increased their scope with successive reforms, to such an extent that they are now omnipresent in M&A transactions.

Since April 1, 2020, AI has entered the scope of "sensitive" activities, with regulations focusing more particularly on any research & development activity relating to AI and intended to be implemented in another sensitive activity (e.g. development of an AI solution intended for military purposes). As a result, a foreign investor planning to take a significant stake[57] in a French entity developing an AI solution could be required to obtain prior authorization from the Minister, where applicable, subject to certain conditions.

Determining how sensitive the target's activity is in the field of new technologies, and notably AI, is particularly complex and will have to be based on a wide range of indicators, some of which are the result of casuistry skillfully maintained by the Ministry: types of customers, specificity or dangerousness of the product, military or civilian applications *(end-use)*, substitutability of the product on the French market, but also the national, EU or international economic and geopolitical context, the presence of a French "*gold nugget*", etc.
Given the importance of AI in the political and economic debate, both nationally and internationally, and the major challenges that its development, protection and supervision represent, AI-related activities should be at the heart of the system relating to foreign investment control in France in the coming years.

In the context of a M&A transaction, this regulatory control must be anticipated in order to reflect these constraints in the legal documentation (conditions precedent, cooperation, specific covenants, etc.) and to adapt the transaction's timetable accordingly. Regulations provide for two possible options: either the investor or the target may request prior examination from the Ministry (a kind of ruling) in order to determine whether the target's activity falls within the scope of sensitive activities (the administration has 2 months to provide its analysis), or the investor may submit a request for authorization of the considered transaction (authorization being obtained or refused at the end of a review phase, which may last, theoretically, between 30 and 75 business days).

Finally, it should be noted that the control has recently been extended to transactions relating to change of control of foreign entities' French branches, so that an entirely foreign transaction could be subject to foreign investment control if the target has a presence in France. This will undoubtedly have an impact on European or international groups operating in the AI sector.

Antitrust

As soon as the operators involved in a M&A transaction exceed certain thresholds (turnover and/or market share), the transaction must be notified to the relevant competition authorities responsible for ensuring the protection of effective competition.

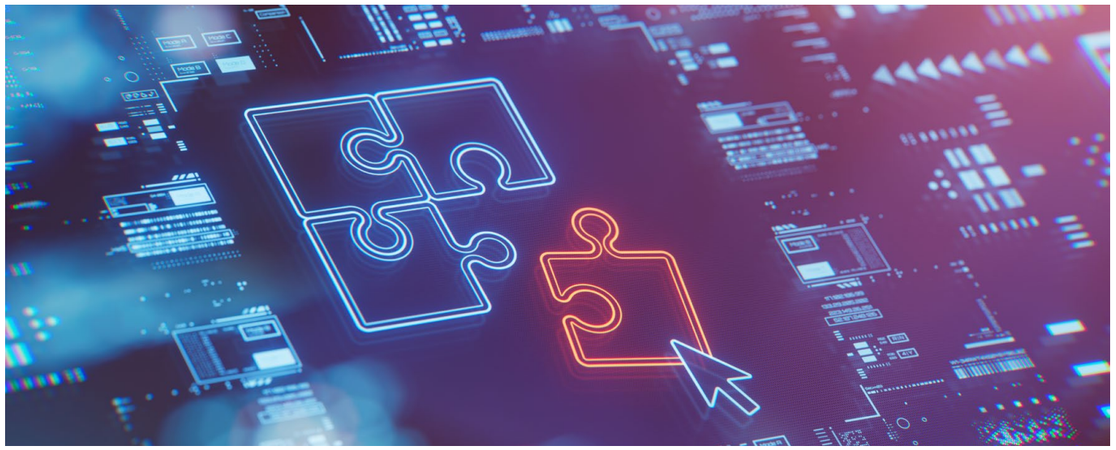
In an economic landscape unsettled by this new AI technology, the particular attention that competition authorities should give to merger transactions in this sector should be anticipated (see section 2.3 p. 30).

Representations and warranties

There is some debate as to whether AI-specific representations and warranties are necessary, as some consider that these risks can be covered by more global warranties notably relating to material contracts, intellectual property, information technology, data protection, cybersecurity and compliance.

For transactions where AI is of strategic importance for the target company, AI-specific representations and warranties should be negotiated in order to provide the purchaser with the necessary comfort on the legal compliance of the tools and products developed and/or distributed by the target.

In addition, specific indemnities could also be provided for, where appropriate, in order to cover, in particular, any third-party claims relating to an unauthorized use of datasets to train AI algorithms, in addition to the usual representations and warranties mechanism.



On another note, in the event that the transaction would be completed following the signature of the share purchase agreement, it could be considered during the interim period to restrict the target company's ability to substantially amend, without the purchaser's consent (unless the amendment is required by applicable law), (i) the nature of the data used by the target, (ii) the conditions relating to the development and/or use of the AI tools, and (iii) the target company's data confidentiality and security policies.

Transition Service Agreements (TSA)

Depending on the relationships between the seller and the target company, a transition service agreement could be put in place in order to ensure business continuity, in particular by maintaining the provision of AI services and existing contracts (notably licenses), where applicable, during a transition period.

The drafting and negotiation of a transition service agreement between the seller and the purchaser must pay particular attention to AI-related aspects. In particular, the parties will need to identify the transitional AI-related services required to continue the business, and agree on a corresponding price (the determination of which may be complicated in practice).

Focus on asset deals

In the context of business transfers (as opposed to share transfers considered above), purchasers will also need to ensure that the assets covered by the transfer agreement include all intellectual property rights on the AI tool, as well as all rights to sell and use this tool and its results, including all technology, software, algorithms, models and data necessary for the operation and further development of the AI tools owned and/or used within the scope of the business transferred.

In this respect, the provision of representations and warranties may be considered. Finally, particular attention should be paid to assignment clauses in this type of transaction, as well as to the consequences of a counterpart's refusal to transfer the rights (subcontracting, TSA, etc.).

57 Acquisition of control, acquisition of a branch of activity or crossing of the threshold of 25% of the target's voting rights (threshold reduced to 10% of the voting rights if the target is listed on a regulated market).

2.7 ARBITRATION

Authors:
Astrid Westphalen - *Counsel*
Sacha Willaume - *Counsel*
Zoé Can Koray - *Associate*

Despite a study carried out in 2021 by Queen Mary University that showed some reluctance on the part of litigants to use artificial intelligence (AI) in arbitration – the principal method of dispute resolution in international commercial transactions –, its increased use now appears undeniable. Such reality begs the question of how AI is likely to affect the conduct of arbitral proceedings and the role of those involved, particularly arbitrators, in the near future.

As a preliminary point, it should be noted that the future AI Act provides that "AI systems intended to assist judicial authorities [...] in researching and interpreting facts and the law, and in applying the law to a concrete set of facts or used in a similar way in alternative dispute resolution" qualify as "high-risk AI systems" *(Annex III and Recital no. 40 of the future AI Act)* and are subject as such to strict compliance and transparency requirements. By assumption, such a definition should include arbitration. It is therefore reasonable to assume that arbitrations with a connection with the European Union, for example given the location of the headquarters, will be subject to the future AI Act. The applicability of this regulation to a given arbitration will ultimately require a case-by-case analysis based on the circumstances of each procedure and on the way in which AI is likely to be used, if at all.

Notwithstanding the potential impact of the future AI Act, it is worth noting that the use of AI in arbitration has been the subject of a relatively limited regulatory framework so far, mostly in the form of soft law through guidelines and recommendations.

By way of example, the Council of Europe's European Commission for the Efficiency of Justice (CEPEJ) adopted the European Ethical Charter on the use of artificial intelligence in judicial systems in December 2018. The Charter identifies several essential principles applicable in relation to AI and the conduct of justice (respect for fundamental rights, non-discrimination, quality and security, transparency, neutrality and intellectual integrity, user control). While this Charter is not specifically aimed at arbitration, it is notably addressed to private parties and could therefore serve as a useful guide in arbitration matters.

More specifically, on August 31, 2023, the *Silicon Valley Arbitration and Mediation Centre (SVAMC)* published draft guidelines on the Use of Artificial Intelligence in International Arbitration. The draft provides recommendations on the uses, limits and risks of AI applications, the protection of confidentiality, the disclosure of the use of AI, the duties of due skill and care in the use of AI, the respect for the integrity of the proceedings and evidence, non-delegation of decision-making responsibilities and respect for the rights of the defence.

Without attempting an exhaustive examination of these issues, the purpose of this note is to set out some of the challenges that the use of AI is likely to pose in the arbitration process, whether in relation to the selection of arbitrators, the administration of evidence, the arbitrator's jurisdictional mission or predictive justice.

Can AI be a reliable tool for the selection of arbitrators?

One of the significant advantages of arbitration over state justice is the parties' freedom to choose an independent and impartial arbitrator to resolve their dispute. The arbitrator's independence and impartiality are fundamental principles of French law, as is the case in many other legal systems. This is codified in Article 1456 of the French Code of Civil Procedure (*Code de procédure civile* - "**CPC**"), and any breaches of this provision may result in the setting aside of an arbitral award.

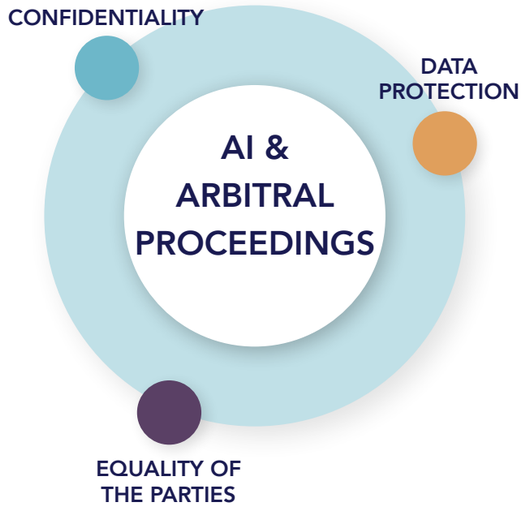
AI is likely to play an important role in the detection of conflicts of interest in the context of selecting arbitrators and more generally throughout the arbitration process. Tools such as Arbitrator Intelligence collect information on arbitrators worldwide and use artificial intelligence to recommend arbitrator profiles to the parties based on the selected criteria. Similarly, *Jus Mundi* offers a tool called *Conflict Checker*, which uses a database of arbitrators, counsel, experts and tribunal secretaries to trace existing and past relationships between them and identify possible conflicts of interest in a given arbitration. In addition, these tools can contribute to promoting diversity among arbitrators.

Nevertheless, these tools also give rise to certain risks. Depending on the data provided, they may reproduce certain biases or apply discriminatory choices. As such, it is essential that these applications be capable of transparently showing users the information on which they are basing choices and identifying the "correct" arbitrator in each case.

What are the challenges associated with the use of AI in the conduct of arbitral proceedings?

AI tools offer a multitude of potential uses by litigants, in particular facilitating document review (which is often time-consuming in arbitration), including analyzing the pleadings and exhibits of the opposing party, producing chronologies or converting interview notes into witness statements. Some document analysis platforms, such as *Relativity*, have developed AI tools for *e-discovery*. In this context, the use of AI is consistent with the obligation on parties and arbitrators to conduct arbitral proceedings efficiently and in a timely manner, as required under numerous arbitration laws and rules.[58]

Nevertheless, these opportunities also raise a number of procedural concerns.



Firstly, downloading documents exchanged in the context of arbitral proceedings onto AI models without anonymization entails significant risks with regard to the obligation of confidentiality that frequently binds the parties, arbitrators and arbitral institutions, particularly in commercial arbitration. Indeed, AI models are trained on massive datasets and have the ability to "remember" previously used information. AI may therefore expose the parties and arbitrators to the risk of breach of confidentiality, particularly in the event of a cyber-attack. In addition, if documents contain personal information, sharing them could also constitute a breach of the General Data Protection Regulation (GDPR). Therefore, the use of AI in arbitration requires the ability to identify where the data provided is hosted and, more generally, ensuring that access to data uploaded onto the AI tool remains sufficiently secure.
Secondly, the use of AI during arbitration, and in particular in the taking of evidence, is likely to be in contradiction with the guiding principles of arbitration proceedings, and in particular the principle of equality of the parties, which the arbitral tribunal must observe and must ensure is observed, subject to the annulment of the award. A party's use of an AI tool to make its case or defend itself more effectively could be perceived as an undue procedural advantage likely to violate the principle of equality[59]. It is conceivable that an arbitrator would accept the use of AI provided access is shared between the parties. However, this will not always be easy to implement in case of major discrepancies between their financial resources or even their aptitude to use this technology. In this respect, Article 9(2)(g) of the IBA Rules of Evidence in International Arbitration 2020, which allows the arbitrator to exclude certain evidence for "considerations of procedural economy, proportionality, fairness or equality of the Parties that the Arbitral Tribunal determines to be compelling," could serve as a useful procedural safeguard, where these Rules apply, in the event of improper use of AI by a party.

Be that as it may, it is advisable that arbitrators and parties address this subject at the outset of arbitral proceedings to determine whether the parties consent to the use of AI, and if so, under what conditions and with what guarantees.

58 See, for example, Article 1464(2) of the CPC: "The parties and the arbitrators act with diligence and loyalty in the conduct of proceedings." (in French: "Les parties et les arbitres agissent avec célérité et loyauté dans la conduite de la procédure."); see also the ICC Arbitration Rules, Article 22(1).
59 See, for instance, Article 1510 of the CPC: "Regardless of the procedure chosen, the arbitral tribunal guarantees the equality of the parties and complies with due process." (in French: "Quelle que soit la procédure choisie, le tribunal arbitral garantit l'égalité des parties et respecte le principe de la contradiction"); see also the UNCITRAL Model Law on International Commercial Arbitration of 2006, Article 18.

Is AI compatible with the arbitrators' jurisdictional mission?

Beyond the conduct of arbitral proceedings, the use of AI by arbitrators at the stage of drafting the arbitral award also raises questions.

Rendering an arbitral award –that is, a judicial decision with *res judicata effect*– constitutes the core of the arbitrators' jurisdictional mission and their main duty, namely to dispose of the dispute submitted to them. An arbitrator's duty to render an award implies that delegating this task to a third party is prohibited. Non-compliance exposes the award to the risk of being set aside.

One of the benefits of AI is to facilitate the arbitrator's task of drafting the award. Some tools, for example, may generate a summary of the parties' positions or of the proceedings to date, which may then be incorporated in the draft award. This is comparable to the work often performed by the secretaries of arbitral tribunals today. The use of AI in this context will undoubtedly result in a more rapid drafting of awards and hence faster dispute resolution, possibly at a lower cost. In this way, AI could help the arbitrator comply with its duty to act expeditiously.

AI will undoubtedly go further and it is reasonable to imagine that it will soon be able to propose reasoned decisions based on the information provided in the case file, and notably the parties' written submissions. Does this not create a risk of delegating the arbitrator's decision-making power? Even if an arbitrator retains the option of disregarding the proposal or amending it to their liking, it cannot be ruled out that AI interference in the arbitrator's decision-making process could potentially influence –or even mislead– them the event of a hallucination by the AI tool, for example in the calculation of the compensation awarded to a party. In any event, the arbitrators' wish to use AI to assist them in the elaboration of their award should only be considered if the parties expressly agree thereto.

In the longer term, the question arises as to whether the arbitrator could be entirely replaced by a robot-arbitrator. While this scenario may look like science fiction, the exponential development of AI should lead us to consider it seriously, even if some scientists doubt the feasibility of modelling the act of adjudication. The use of robot-arbitrators gives rise to a number of ethical concerns, particularly as regards their ability to make just and equitable decisions. More generally, the use of a robot-arbitrator raises questions as to how we can control

Artificial intelligence ◆ 2. Legal issues - Arbitration

not only its independence and impartiality, but also the transparency of its reasoning, and thus avoiding the "black box" effect of AI.

Without delving into this complex debate, it remains that such a revolution does not seem legally possible under French law for a number of reasons. To mention just a few, in domestic arbitration, Article 1450 of the CPC provides that "the task of arbitrator may only be carried out by a natural person enjoying the full exercise of his/her rights", a criterion that also appears in other legislation. Similarly, a domestic arbitration award must include, subject to nullity, the name(s) of the arbitrator(s) who issued it and their signature(s) (CPC, Art. 1481 and 1492 6°). How can this requirement be applied to a robot-arbitrator? In addition, case law considers that the relationship between the arbitrator and the parties is contractual and that the arbitrator may accordingly incur liability. However, this legal conception of the arbitrator is incompatible with the idea of an arbitrator-robot, which, unless the legislator decides otherwise, would have no legal personality and would therefore be unable to enter into a contract, let alone be held liable in the event of default.

In any event, assuming this hypothesis were possible, an award made in France by a robot-arbitrator might not be recognized in other countries, which would continue to apply criteria similar to those of current French law. Article V(2)(b) of the New York Convention of June 10, 1958, which is in force in 172 countries, allows a signatory State to refuse to recognize an award on its territory if it "*would be contrary to the public policy of that country*", and notably to its procedural public policy.

What is the role of predictive analysis in arbitration?

Predictive justice tools enable massive analysis of data based on decisions rendered in order to predict the outcome of given litigation. The law is thus used as a mathematical tool to quantify the chances of success or legal uncertainty. However, certain features specific to arbitration complicate the use of predictive analysis.

Indeed, the confidentiality of arbitration, especially commercial arbitration, limits the number of accessible awards and consequently the accuracy of prediction. It should nevertheless be noted that an increasing number of awards have been published in anonymized form in recent years.

Moreover, beyond the debate on the very existence of arbitral case law, the unique nature of each arbitration procedure makes it difficult to model the computer data required to implement a "predictive" tool. In addition to the inherent complexity of certain cases, it is particularly laborious to compare awards, since they will be radically different if they have been made in domestic or international arbitration, by one or more arbitrators, in law or in equity, under one national law rather than another, and depending on whether or not the practices of a sector or industry have been taken into account. Any procedural incidents and the procedural approach of a party may also influence arbitral decisions, which, in any event, benefit from greater discretionary powers than national courts.

These observations ought to be qualified with regard to sports arbitration and investment arbitration. Investment arbitration awards –and more particularly those made under the aegis of the International Center for Settlement of Investment Disputes (ICSID)– are often published. The issues faced by arbitrators are more recurrent (for example, the definition of investor, the notion of investment or the calculation of compensation awarded to the latter). Decisions on interim measures in investment arbitration could also be the subject of predictive analysis in order to identify patterns in terms of the criteria used and the types of measures granted, and possibly revealing the existence of a body of case law.

Even if the parties may fear the influence of these tools on the arbitrator's decision, predictive analysis could also encourage them to find a non-contentious outcome to their dispute or to settle certain pending proceedings. These tools, as offered by certain legal tech firms, may also be of interest to third-party funders that may more accurately assess the probability of success of an arbitral procedure.

2.8 EMPLOYMENT

Author:
David Jonin - *Partner*

The advent and development of artificial intelligence promises to send significant shockwaves through the labor world as we know it. Not merely a tool aimed at facilitating the fulfilment of certain tasks, artificial intelligence will likely revolutionize a considerable number of jobs, and may even replace some of them. As for the International Labor Organization (ILO), it believes artificial intelligence will "accompany" workers rather than replace them.

The future AI Act identifies as high-risk AI systems deployed in the fields of employment, labor force management and access to self-employment. For the authors of the AI Act, AI systems can significantly impact the affected workers' career prospects, livelihood and rights, and can lead to serious violations of fundamental rights *(Recital no. 36 of the future AI Act)*. In this respect, the future AI Act will set forth special protection around such AI systems, whereby the launch or start-up of such systems will be subject to a certain number of obligations (see section 1.2, p. 10).

More specifically, this will concern AI systems used as tools to assist in the recruitment or selection of individuals (circulation of job ads, screening of job applications, evaluation of candidates during interviews or tests, etc.), as well as to make promotion and dismissal decisions with regard to the performance of employment contracts, whether this involves the assignment of duties or the monitoring and evaluation of individuals' performance and behavior within the scope of these relationships.

> ***At first glance, the use of artificial intelligence in companies in support of a recruitment and staff management policy presents certain obvious opportunities. However, it also raises different questions, which will require that employers anticipate the possible effects thereof as well as the upstream involvement of the staff representative bodies in compliance with their consultative capacity.***

Use of AI by the employer

To what situations can an employer apply artificial intelligence?

As far as recruitment is concerned, artificial intelligence can provide employers with effective tools to promote parity and the fight against hiring discrimination. This aspect has triggered a discussion on algorithmic biases and the employer's liability in case of "algorithmic discrimination". Indeed, although the use of artificial intelligence provides greater objectivity, the first analyses of the CNIL (*Commission nationale de l'informatique et des libertés* - French Data Protection Authority) have revealed that algorithms are likely to replicate societal biases. This can mainly be explained by the fact that the databases that feed the algorithms may bear traces of social inequalities (e.g., an algorithm can reproduce a sexist bias based on the observed wage gap between men and women).

In case of suspected discrimination following the use of artificial intelligence, in light of current substantive law, the employer will most likely be deemed liable. Indeed, the latter must be able to prove that all decisions that are made rest on objective and non-discriminatory elements. Thus, if factual elements point to suspected discrimination in certain algorithmic decisions, it will always fall on the employer to prove that the decision made was justified by objective elements devoid of any sort of discrimination. This means that the employer will have to provide an explanation on how the algorithm works. Given that the employer cannot limit its liability to the mere execution of its obligations, it must apply caution and precise methodology when entrusting staff management decisions to AI.

This also raises the question of algorithmic staff management, beyond the recruitment process. Staff-related data homogenization software packages ("*Entreprise Resource Planning*" - *ERP*) already exist and are meant to simplify the work of human resources. To this can be added artificial intelligence software providing algorithmic management solutions or forward-looking human resources management solutions (aka, people analytics), which for example can focus on targeting high-potential candidates, managing careers and career development or even predicting potential work-related accident risks. Artificial intelligence could even be used to assist the employer with the assignment of tasks and performance reviews.

In view of such possibilities, the protection of worker rights must be placed in the forefront and must imperatively be addressed by the employer. The legal framework around artificial intelligence is still under preparation and a European directive could be adopted to compensate for the lack of specific regulations in this respect in the labor world. Indeed, on December 6, 2022, the European Trade Union Confederation ("**ETUC**") adopted a resolution calling for an EU directive on algorithmic systems at work. According to the ETUC, the guiding principle of the new directive on algorithmic systems in the workplace "must be to preserve the dignity of workers and to counteract dehumanization at work". This framework would be built on the basis of Article 153 of the Treaty on the Functioning of the European Union (TFEU), which provides that the European Union shall support and complement the activities of the Member States in the labor field.

The role of staff representatives

To what extent should an employer's use of artificial intelligence be submitted to the information and consultation of staff representatives?

The aforementioned resolution of the European Trade Union Confederation asks that, where the employer chooses to make use of artificial intelligence, the future directive strengthen and enforce the trade unions' collective bargaining rights as well as the information, consultation and participation rights of staff representatives.

As a reminder, according to French legislation, the works council *(comité social et économique)*, comprised of elected staff representatives, must be informed and consulted –prior to implementation within the company– on automatic staff management processing and employee activity monitoring means or techniques. The works council must also be informed and consulted –prior to use– on the recruitment assistance methods or techniques.

In any case, the works council will also have to be consulted when new technologies, as well as any major development modifying health and safety conditions or working conditions, are implemented within the company, as set forth by Article L.2312-8 of the French Labor Code.

In 2018, the French Supreme Court (Cour de cassation) nevertheless ruled that the designation of an expert on the basis of Article L.2315-94 of the French Labor Code ["*the introduction of new technologies, any major development modifying health and safety conditions or working conditions*"] was not justified when the "intelligent device", the implementation of which within the company is contemplated, only has a minor impact on the direct working conditions of the employees, whose tasks are consequently made easier[60].

It must be underlined that, despite the employer's obligation to inform the elected works council members on the artificial intelligence tools put in place within the company, the technicity and opacity of certain systems makes it difficult for the employer to abide by its duty of transparency.

Collective negotiations

Does the implementation of AI mechanisms within the company fall within the scope of collective negotiations?

> ***The implementation of artificial intelligence mechanisms within the company should be added to the scope of the negotiations on Quality of life at work.***

Indeed, the introduction of artificial intelligence in the work environment can have an impact both on the physical and psychological hardship of work and on the content of work, or even on labor relations.

A European framework agreement dated June 22, 2020 on digitalization aims to "encourage, guide and assist employers, workers and their representatives in taking up the issue of digital transformation". In particular, this text identifies "artificial intelligence and the human in control principle" as a major stake that the national negotiators are invited to take into account.

The framework agreement underscores that it is necessary to allow staff representatives to handle data, consent, privacy and monitoring, to link data collection to a concrete and transparent goal, and to provide staff representatives with the means necessary to fulfill their missions.

60 Supreme Court, Labor Div., April 12, 2018, no. 16-27.866.

2.9 REAL ESTATE

Author:
Sébastien Lamy-Willing - *Associate - KM*

Policies aimed at reducing land use and combating climate change are a prime area for artificial intelligence, as they involve processing large volumes of data. AI could also help reduce the number of legal uncertainties involved in setting up and implementing real estate operations.

Use of AI to help manage land-use challenges

Among the areas likely to be affected by AI, urban planning holds a prominent position. At a time when land-use planning policies are being challenged by climate and environmental issues, AI is set to play a key role in a number of ways.

Indeed, it is capable of analyzing a massive amount of data, making fine-tuned and highly relevant territorial diagnoses, and carrying out modeling that make it possible to simulate several possible scenarios based on changes in exogenous factors such as demographic growth, rising temperatures, increasing scarcity of water resources, and so on.

Since AI is capable of highlighting trends and anticipating likely events, it could be used to help achieve the objectives set by the public authorities in terms of land conservation.

In France, for example, the legislator has set a target of "zero net artificialization" (ZNA) of land by 2050, with an intermediate target of halving the consumption of natural, agricultural and forest areas by 2031. This target of reducing land artificialization, which is gradually beginning to appear in the major regional planning documents that are the regional plans, must be incorporated into local urban planning documents (SCOT and PLU) by 2027/2028

> ***Under these conditions, AI will be able to facilitate the identification of areas with a high potential for renaturation, as well as those likely to contribute to regeneration operations, through the consolidation of urbanized areas or the rehabilitation of brownfield sites.***

AI algorithms could even make it easier to identify future brownfield sites, which could then be redeveloped. This predictive knowledge of the area would thus make it possible to incorporate reversibility possibilities into programs, as is already the case in certain regions on an experimental basis.

In the long term, this could involve the design of a forward-looking decision-making tool based on the prediction of trends (in climate, transport, de- or re-industrialization, the decline of certain commercial areas in favor of logistics warehouses, etc.), so that this can be anticipated in land-use planning policies.

Use of AI to combat climate change

AI can play an important role in the fight against climate change, whether at a regional level or at the level of a building (see section 2.10 p. 54). At least, that is the view of 87% of public and private sector leaders in charge of climate-related issues, according to a report by the "AI for the Planet Alliance", drawn up by Boston Consulting Group in 2022.

At a regional level, researchers are developing applications to offer planners solutions in terms of “smart cities”, i.e. an area equipped with technologies for automating network management processes (water, electricity, communications, heat) based on data collected by electronic sensors, so as to keep waste to a minimum.

AI may even offer functionalities that go far beyond the simple connected city. One example is the concept of "urban brains" hosted on digital platforms from which artificial intelligence is able to act on urban planning.

At the level of a building, the energy performance diagnoses and other measures aimed at reducing energy consumption set out in the various pieces of legislation (notably the French Tertiary Sector decree) do not currently enable operators to project the carbon trajectory of buildings they own so as to anticipate the environmental obsolescence of their asset portfolios.

This is why a European consortium developed the CRREM (Carbon Risk Real Estate Monitor), a tool designed to enable a projection of real estate assets on a trajectory compatible with the ambitions set out in the Paris Climate Agreement adopted during the COP 21. Here again, artificial intelligence is set to play a role. For example, a French start-up from the Ecole Polytechnique incubator has raised funds to develop a solution for decarbonizing buildings using AI, in order to speed up their compliance with regulatory standards.

Use of AI to set up complex real estate projects

Setting up complex real estate projects generally involves a high degree of uncertainty regarding the administrative authorizations to be sought. The provisional timetable for these projects, and therefore their feasibility, is itself dependent on the uncertainties that may exist regarding the authorizations to be obtained and their issuance, where applicable.

For instance, before applying for a building permit within the scope of a project, a prior environmental impact assessment is commonly required. Depending on the opinion issued by the environmental authority, the results of this assessment can potentially give rise to avoidance, reduction or offsetting measures, which would themselves require modifications to the project.

So, depending on the nature of the project, an impact assessment may be systematic or requested after a case-by-case examination. This second case also involves a high degree of uncertainty.

It is also not uncommon for large-scale projects to require an adaptation of planning regulations. Here again, depending on the nature of the changes to be made to the planning regulations, an environmental impact assessment of these changes may be required.

In addition, an environmental assessment necessarily gives rise to various public participation procedures, especially when it involves changes to town planning documents.

There may also be preventive archaeological issues, for which the procedure will depend on discoveries made on site, or environmental authorizations to be sought under the legislation on classified installations or the law on water, depending on the type of use that will be made of the site once the real estate project has been completed.

By collecting regional, regulatory and procedural data, AI could have a role to play here, on the one hand, to automatically predict the different scenarios and sub-scenarios likely to occur in the setting up of this type of project and, on the other, to evaluate the most likely scenario. The operator could then consider different development options to comparatively examine the resulting range of scenarios, generated automatically by a tool capable of editing not only text, but also timelines and other explanatory diagrams.

AI could also facilitate the task of the investigating departments, particularly when it comes to building permits, since checking that projects comply with planning regulations could be automated to a large extent, which would also speed up the time taken to issue authorizations.

In this respect, a French start-up developed an AI tool that can be used to "decode" planning regulations and facilitate the study of project feasibility, with in particular the creation of a virtual assistant *(chatbot)* designed to decipher PLUs (local urban planning plans).

Use of AI to implement complex real estate projects

Even if all the necessary authorizations for a real estate project have been obtained, they must still be final, i.e. they must be free from any appeal.

However, operators, and behind them their financial backers, categorically refuse to start work until an appeal against planning permission has been cleared, which very often leads them to settle with the applicant, sometimes paying them very large sums in return for withdrawing the appeal.

> ***AI could play a role here in predictive justice, so as to identify the applicant's chances of success in light of the arguments raised by the latter and to ensure, where appropriate, that a potential defect in legality can be rectified, so as to enable work to begin without waiting for the outcome, whether amicable or judicial, of an appeal.***

Insurance products could even be envisaged to cover the risk –identified and controlled by AI algorithms– of a building permit being cancelled once work has begun.

2.10 ENVIRONMENT

Author:
Jean-Nicolas Clément - *Partner*

Artificial intelligence and the protection of the environment have been making headlines far and wide. While the development of a potential connection between the two has thus far been limited, and while this new form of intelligence that is AI has already found numerous applications in a wide variety of fields, such as medicine, finance or video games, its use in the environmental sphere is lagging behind. This will certainly not come as a surprise, given the very –if not too– broad nature of environmental concern; after all, doesn't biodiversity cover the entire living world and its interactions? Not only that, but the inter-disciplinary nature of environmental issues is also a factor. Legal experts can vouch for this: environmental law does not come under any of the two cardinal categories of private law and public law. Quite naturally, the very broad characteristics of environmental law make it extremely difficult to formulate questions to be fed to AI and very often lead to answers that are far from having reached operational satisfaction.

Can any correlations be found between these two highly topical, but seemingly fundamentally opposite concepts? How can the incarnation of economic and technological development that is AI be reconciled with the protection of the environment? Could AI have a part to play in addressing environmental challenges? For some time now, these issues have sparked passionate debates. World organizations like the UN[61] and UNESCO[62], as well as the French government[63] and French[64] and foreign[65] companies, have been studying the question. Two main conclusions stand out: while the advent of AI is bringing noteworthy innovations to certain sectors of activity, its impact on the environment on the other hand raises certain concerns; nevertheless, AI might also be able to serve as a vector of innovative solutions for the protection of the environment.

Presently, when we think of the correlation between AI and the environment, we think of the strong impact that the development of AI has on the environment

Currently, when examining the correlation between the environment and AI, our view of the subject often tends to be shortsighted, as we only see its carbon footprint on the environment.

It is true that AI has a substantial environmental impact – whether it be during the design or implementation phase or when the equipment that supports it ceases to operate.

Therefore, like any computer program, AI 'lives' through electrical and electronic equipment, the manufacturing of which very often requires the need for precious metals that are rare resources (such as gold and lithium). The extraction of such resources can cause serious environmental damage (pollution, deforestation, etc.). According to researchers at the University of Massachusetts[66], training a single AI model "can emit nearly five times the lifetime emissions of the average American car (and that includes manufacture of the car itself)".

Likewise, data centers that feed and support AI take up considerable square footage and their operation can leave a significant environmental footprint, notably due to its highly energy intensive nature. AI requires high computing power, directly entailing accrued power draw and cooling needs –a problem that is all the more serious in the context of the difficult sharing of water resources already under pressure.

Lastly, while it is true that today AI appears as a model of innovation, like any technology –and even more so, those stemming from the digital revolution–, AI evolves in the ever looming shadow of obsolescence. The rapid pace of technological evolution in the field of AI means that models already in place quickly become obsolete, and anything that is not the highest-performing model usually ends up as waste. It is well known that waste management, and in particular waste electrical and electronic equipment, is a major environmental issue.

These problems are real, but simply observing them does not suffice for a complete analysis. Indeed, once a problem is identified, it is precisely the role of environmental law to reflect on how to eliminate, reduce and possibly compensate for the damage or problem caused, by applying the principles of prevention and reduction at source. In this respect, various approaches can already be envisaged, and even adopted, to eliminate or limit the impact of AI on the environment. It would thus be possible to design optimized AI algorithms requiring less energy, and therefore being less harmful to the environment. Likewise, in order to meet the energy needs of AI, the use of renewable energy sources should be the preferred choice (e.g. via solar panels installed directly on and around data centers). Lastly, with regard to the production of waste electrical and electronic equipment, it is imperative that we rethink the obsolete equipment recycling chain. These points did not escape the attention of the legal drafters of the future AI Act, who recall the requirements of a fundamental right to a high level of environmental protection. Hence, the Commission will be responsible for requesting a publication from the European Standards Organizations (ESO), with a view to improving the performance of AI systems in terms of reducing their consumption of energy and other resources. Furthermore, providers of general-purpose AI systems, which feed on large quantities of data and therefore tend to be energy intensive, will be required to disclose their energy consumption (see section 1.2, p. 10).

AI, a vector of innovative solutions for the protection of the environment

Today, when it comes to AI, the spotlight mostly highlights the negative effects. The future however –and when it comes to technological progress, the future is often just around the corner... – may shine a brighter light on the positive role that AI may play with respect to environmental protection. Indeed, AI may turn out to be a powerful ally for the protection of the environment, as noted in the Reasons for and objectives of the Proposal for a Regulation on AI: "*By improving prediction, optimizing operations and resource allocation, and personalizing service delivery, the use of artificial intelligence can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy. Such action is especially needed in high-impact sectors, including climate change, environment and health, […].*"

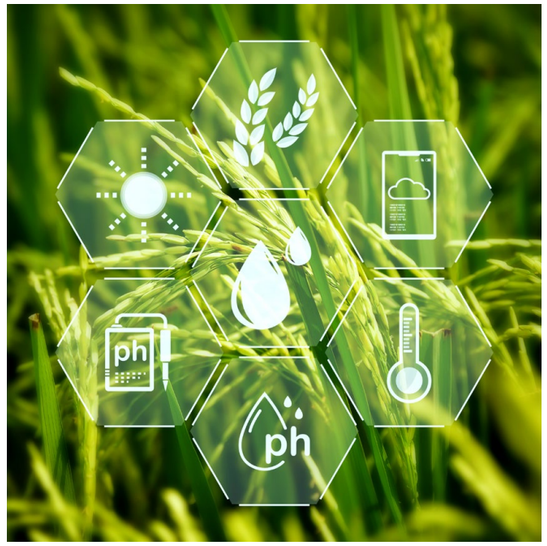
61 ONU info, "L'intelligence artificielle, une alliée pour le climat", November 4, 2023.
62 UNESCO, "IA pour la planète : mettre en évidence les innovations en matière d'IA pour accélérer leur effet", February 25, 2021. Last updated on April 20, 2023.
63 Entreprises.gouv.fr, "L'intelligence artificielle au cœur de la transition écologique des transports". Updated on March 1, 2023.
64 SUEZ Group, "Artificial intelligence serving the environment", April 7, 2022.
65 IBM, with the creation of the IBM Environmental Intelligence Suite, a SaaS platform that makes it possible to monitor and forecast weather and climate events in order to be better prepared.
66 As discussed by the MIT Technology Review website in an article dated June 6, 2019 on AI.

AI systems are and will increasingly be deployed to monitor biodiversity, combat pollution, predict natural disasters and optimize the use of natural resources. In fact, just as AI can reason and learn as if simulating human thought, it will be able to recreate climate and biodiversity models, and enable anticipatory analysis of changes linked to modifications and interactions of complex variables.

Hence, **as regards biodiversity monitoring**, AI can analyze satellite images and photographs to track the movement of certain animal species, monitor changes in natural habitats and identify protected species. The company Open Studio launched the "Mellia" project, which allows beekeepers to have a connected hive using AI to remotely monitor the bees' living conditions[67].

As for the optimization of water management, SUEZ, in collaboration with Microsoft, has created a platform called Co-DAI, which "*centralizes and accelerates its artificial intelligence innovation policy*"[68]. This platform contributed to the "*Sewer Ball*" innovation: a "*smart solution*" for inspecting wastewater networks and identifying issues, through the use of a small ball inserted into the water distribution pipeline network[69]. This "ball" can detect water leaks and anticipate their exact location.

AI systems are also used to manage waste and the recycling process. **AI-powered robots can sort waste more efficiently and improve recycling rates**. A noteworthy example is the association "*The Ocean Cleanup*"[70], which has set out to develop and scale AI technologies aimed at ridding the world's oceans of plastic waste. The plastic collected by the robots is then recycled.



As regards natural disasters, AI also has a part to play. AI algorithms can gather and analyze vast quantities of data (meteorological, geological, rainfall, etc.) to anticipate and prevent natural disasters. For instance, AI could provide predictive models based on this data, to predict hurricanes, floods and earthquakes. An AI-based action plan has been launched by the UN Secretary General to ensure the protection and safety of people –by the end of 2027– from dangerous weather, water and climate events, through early warning systems[71].

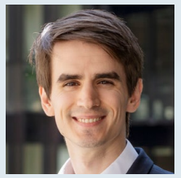
Lastly, **in the energy sector,** AI maximizes the efficiency of energy use, particularly renewable energies. Predictive algorithms would anticipate the energy produced by solar panels or wind turbines, enabling these sources to be better integrated into power grids. AI could also be used to optimize energy consumption in buildings, industry and transport networks. By way of example, the French Ministry of Economy, Finance, and Industrial and Digital Sovereignty wants to place AI at the heart of transportation's ecological transition[72].

While it remains imperative to balance the technological advances enabled by AI with ethical and environmental responsibility, it is undeniable that AI has a key role to play in helping mankind meet the challenge of environmental protection and sustainable development.

67 Open Studio, "Mellia, notre ruche connectée grâce à l'IoT et à l'IA".
68 SUEZ Group, "Artificial intelligence serving the environment", April 7, 2022.
69 Ibid.
70 The Ocean Clean Up website.
71 ONU info, "L'intelligence artificielle, une alliée pour le climat", November 4, 2023.
72 Entreprises.gouv.fr, "L'intelligence artificielle au cœur de la transition écologique des transports". Updated on March 1, 2023.

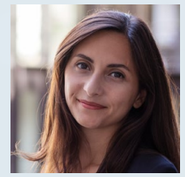
CONTACTS

THIERRY BONNEAU
thierry.bonneau@gide.com
+33 (0)1 40 75 60 22
Senior Counsel
Banking & Finance



RUDOLF EFREMOV
rudolf.efremov@gide.com
+33 (0)1 40 75 99 81
Associate
Banking & Finance

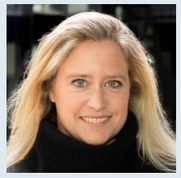
SÉBASTIEN LAMY-WILLING
sebastien.lamy-willing@gide.com
+33 (0)1 40 75 36 46
Associate - KM
Real Estate Transactions
& Financing



GHIZLEN SARI-ALI
ghizlen.sari-ali@gide.com
+33 (0)1 40 75 36 56
Counsel
Mergers & Acquisitions

ZOÉ CAN KORAY
zoe.koray@gide.com
+33 (0)1 40 75 61 92
Associate
Dispute Resolution

RICHARD GHUELDRE
ghueldre@gide.com
+33 (0)1 40 75 22 55
Partner
Insurance, Industrial risk
& Transport



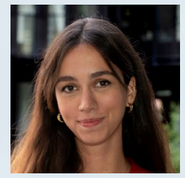
EMILIE LEYGONIE
emilie.leygonie@gide.com
+33 (0)1 40 75 61 56
Associate
KM & Documentation
Manager

MICHEL SERVOZ
michel.servoz@gide.com
+32 2 231 11 40
Consultant
Competition
& International Trade

LAURA CASTEX
castex@gide.com
+33 (0)1 40 75 94 15
Partner
Competition
& International Trade

GUILLAUME GOFFIN
goffin@gide.com
+33 (0)1 40 75 29 02
Partner
Banking & Finance

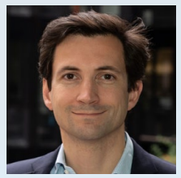
MATTHIEU LUCCHESI
matthieu.lucchesi@gide.com
+33 (0)1 40 75 99 57
Counsel
Banking & Finance
Innovation & Fintech



SOFIA VUKOVIC
sofia.vukovic@gide.com
+33 (0)1 40 75 36 48
Associate
Competition
& International Trade

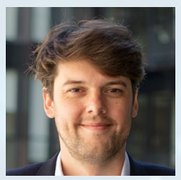
JEAN-NICOLAS CLÉMENT
jean-nicolas.clement@gide.com
+33 (0)1 40 75 22 44
Partner
Public Law, Energy & Environment

FRANCK GUIADER
franck.guiader@gide.com
+33 (0)1 40 75 44 98
Head of Gide 255
Innovation & Fintech



LOUIS OUDOT DE DAINVILLE
louis.oudot-de-dainville@gide.com
+33 (0)1 40 75 35 27
Partner
Mergers & Acquisitions

ASTRID WESTPHALEN
astrid.westphalen@gide.com
+33 (0)1 40 75 61 43
Counsel
Dispute Resolution



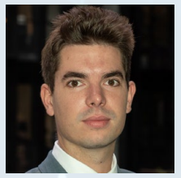
PIERRE-ANTOINE DEGROLARD
pierre-antoine.degrolard@gide.com
+44 (0) 20 7382-5593
Counsel
Mergers & Acquisitions

JULIEN GUINOT-DELÉRY
guinot@gide.com
+33 (0)1 40 75 99 94
Partner
Intellectual property,
Telecommunications,
Media & Technology

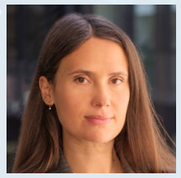
AURÉLIE PACAUD
aurelie.pacaud@gide.com
+33 (0)1 40 75 29 37
Counsel
Intellectual property,
Telecommunications,
Media & Technology

SACHA WILLAUME
sacha.willaume@gide.com
+33 (0)1 40 75 22 38
Counsel
Dispute Resolution

THIERRY DOR
dor@gide.com
+33 (0)1 40 75 29 46
Partner
Intellectual property,
Telecommunications,
Media & Technology



THOMAS JARDIN
thomas.jardin@gide.com
+33 (0)1 40 75 94 22
Associate
Insurance, Industrial risk
& Transport



MARIE-ANGE POZZO DI BORGO
pozzodiborgo@gide.com
+33 (0)1 40 75 94 73
Counsel
Intellectual property,
Telecommunications,
Media & Technology

PHILIPPE DUPICHOT
dupichot@gide.com
+33 (0)1 40 75 29 87
Senior Counsel
Head of Gide's
Scientific Council

DAVID JONIN
jonin@gide.com
+33 (0)1 40 75 36 88
Partner
Employment Law

STÉPHANE PUEL
puel@gide.com
+33 (0)1 40 75 29 69
Partner
Banking & Finance

gide.com

1ST EDITION MARCH 2024

This publication does not pretend to cover all legal issues relating to artificial intelligence. It does not contain legal advice or opinions. The information provided is limited to delivering thoughts on the legal implications of AI in certain sectors, based on ongoing discussions at the time of publication regarding the future European AI Act, and remains subject to the final text that will be adopted.

Photo credits: Istock, Unsplash

GIDE
GIDE LOYRETTE NOUEL