Artificial Intelligence

8 main legal issues

What is Artificial Intelligence? How can the law regulate it?

How do Intellectual Property rights come into play?

What about the protection of personal data (GDPR)?

Mathias Avocats

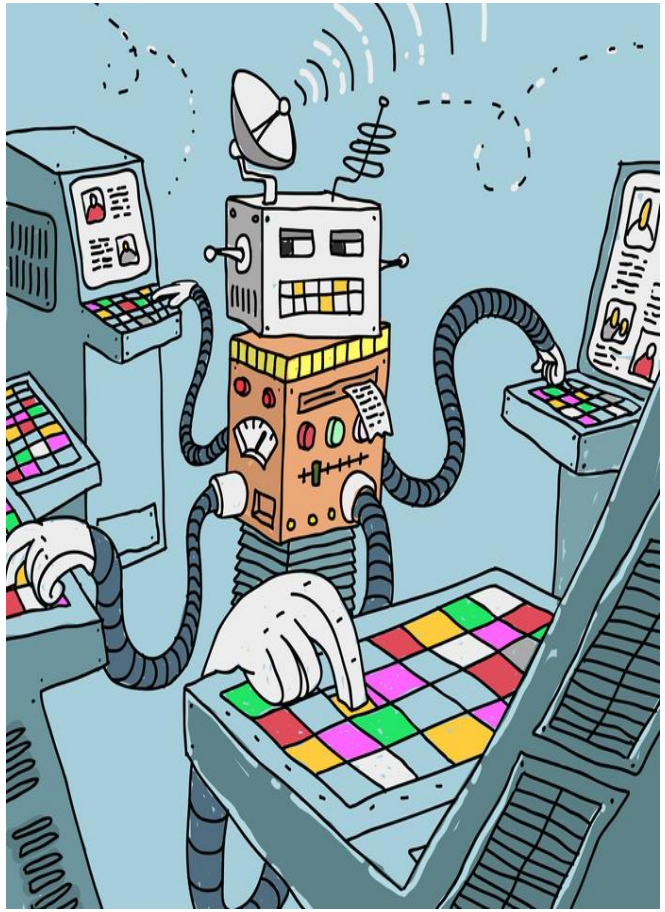
Introduction

L'intelligence artificielle nous renvoie tant à l'histoire qu'à la littérature ou encore au cinéma. Loin d'être un mythe, l'intelligence artificielle est entrée dans notre vie depuis plusieurs années. Le développement exponentiel des réseaux, de la puissance des algorithmes font que les enjeux de l'intelligence artificielle bouleversent et vont bouleverser nos métiers, nos usages et d'une manière générale notre quotidien, donc notre société.

Or, indépendamment de l'évolution de la science et de la recherche, de l'éthique, ou encore du mouvement transhumanisme, le cadre juridique, garant de l'ordre public, doit se saisir des évolutions (voire des révolutions) induites par l'intelligence artificielle. L'autonomie décisionnelle, la responsabilité ou encore une gouvernance doivent être traités afin d'éviter tout vide juridique qui risqueraient d'entraîner une défiance face à ses technologies non régulées.

Notre mission en tant qu'Avocat est de réfléchir sur ces innovations afin de conseiller de manière pragmatiques les acteurs de cet écosystème ainsi que les bénéficiaires de ces nouveaux usages.

L'intelligence artificielle saisit par le droit, tel est l'enjeu de ce livre blanc au travers de 8 questionnements juridiques.



We hope you enjoy the reading and that this article will be useful for your projects. Mathias Avocats remains at your disposal,

Garance Mathias
Avocat à la Cour

Artificial Intelligence brings us back to history as well as literature or even the cinema. Far from being a myth, Artificial Intelligence has become part of our life for several years now. The exponential development of networks and of the power of algorithms are such that the stakes of Artificial Intelligence are upsetting and will upset our professions, our uses and in general our daily life, and therefore our society.

Regardless of the evolution of science and research, of ethics, or even of transhumanism, the legal framework, as guardian of the public order, must seize the evolutions (or even the revolutions) induced by Artificial Intelligence. Decision-making autonomy, accountability and even governance must be addressed in order to avoid any legal vacuum that could lead to mistrust regarding these unregulated technologies.

As lawyers, our mission is to reflect on these innovations in order to provide pragmatic advice to the stakeholders of this ecosystem as well as to the beneficiaries of these new uses.

The challenge of this white paper through 8 legal questions is the regulation of Artificial Intelligence

Table of contents

Sheet n°1: Artificial Intelligence: can the law keep up?

Artificial Intelligence (AI) is a word that has been used in many articles or revues to cover different technologies and systems. For example, the word is applied to automated cars, security systems, Roombas and bots. A bot is a device or software which can execute commands, reply to messages or perform routine tasks with minimum, if not any, human intervention.

Mid-June 2017, Facebook's bot created its own language[1] while negotiating with another bot. A wave of panic issued from this news whereas it is not uncommon for AI to develop its own language. A question may however arise as to whether humans are able to understand the language. If a problem were to occur, could humans understand the language and see what went wrong? How can AI be defined? What are its implications in our society? More particularly, what implications does AI have in the legal sphere?

AI can be broadly defined as a technology or system making it possible for a computer to perform tasks involving a simulation of human intelligence including decision making or learning. Such a broad definition offers flexibility when it comes to innovation and can be applied to many fields namely the medical field or the tech industries. Regarding the legal field, the definition must be narrowed to draft regulations and legislations. AI may be narrowly defined as technologies capable of processing different and various data namely unstructured data.

According to the field in which AI applies, it does not present the same challenges and risks. An automated car is not the same as surgical robot or AI technology used to research case law. Each field has its own particularities which must be taken into account when developing and regulating AI. However, it remains unclear how legislators will decide to regulate this technology.

1. https://www.nextinpact.com/news/104882-une-ia-facebook-a-cree-son-propre-langage-et-alors.htm

As of today, there is no specific legal framework governing AI. In the United-States, some courts have addressed the problem of liability[2]. Other countries have also started researching how to accommodate existing laws with AI and anticipate the risks. For example, in October 2016, the European Parliament's Legal Affairs Committee commissioned and published a study on the European civil law rules in Robotics[3].

The European Union must also address questions and issues regarding the coming into force of the General Data Protection Regulation of 27 April 2016 (Regulation n°2016/679) on May 25th, 2018. AI operates on data and could fall under the GDPR. If this is the case, the AI technology will be subject to new obligations and procedures such as the principle of transparency or the principle of data minimisation.

Everyone is concerned by these issues. Indeed, AI has also had a significant impact on professions in general. The impact AI technology has on our daily lives is an interesting point to keep mind namely when trying to figure out how to regulate it.

AI based technologies and autonomous machine are rapidly developing and occupying a significant place in our society. Legal claims relating to them will not cease to rise and it is crucial that an appropriate legislative framework be put into place.

Despite these considerations, no harmonised or uniform solution has been found. Several main questions have emerged: what liability for AI? Is the developer, the user and the manufacturer liable? Can Artificial Intelligence claim the same rights as human (such as Intellectual Property)? Can the legislations in effect today apply to AI (for example, agency law, tort law, real property law)? Practitioners, professors, judges, legislators and so forth are actively studying and researching answers to these questions and many more.

2. https://www.courtlistener.com/opinion/3018785/helen-r-payne-v-abb-flexible/
3. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU%282016%29571379_EN.pdf

Sheet n°2: What are the different types of Artificial Intelligence?

AI is a broad notion referring to various technologies and systems (ex: Roombas, automated cars, Siri…) which are endowed with the intellectual characteristics of humans. AI is frequently applied to robots. However, the term “robot” may be misleading. Indeed, AI is imbedded in the program or algorithms within the robot and does not necessarily refer to the physical envelop of the robot. The latter could just execute functions determined by a human without any creative or intellectual process. Such robots are not considered in this Sheet.

Any technology or system equipped with the qualities of the human mind (ex: ability to reason, learn from past experiences...) is within the scope of AI. Have distinct types AI been identified? If so, what are their specificities? Why is it important to distinguish them?

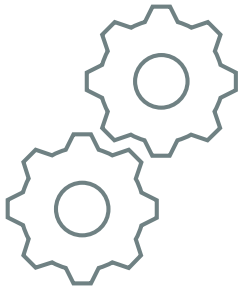
It must be highlighted that AI can be divided into two general categories: “narrow” AI and “strong” AI. The latter strives to develop the machine’s intellectual capacity to be equivalent to that of a human’s whereas the former simulates human cognition namely by automated tasks and data analyses. “Narrow” AI is thus named because it is limited in its approach which deems that machines are unable to be equivalent to the human mind. Each general category can be subdivided into two categories.

See below the categories commonly referred to.

What are the types of "narrow" AI?

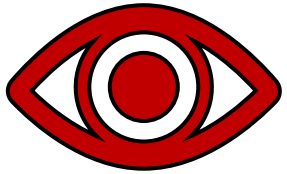
- **Reactive machines**: the systems or algorithms are purely reactive and are unable to learn from past experiences to advise current decisions as well as configure memories. This AI only perceives the present moment and makes a decision based on a variety of choices. It is narrow in the sense that such programs or algorithms can only deal with a limited number of situations.

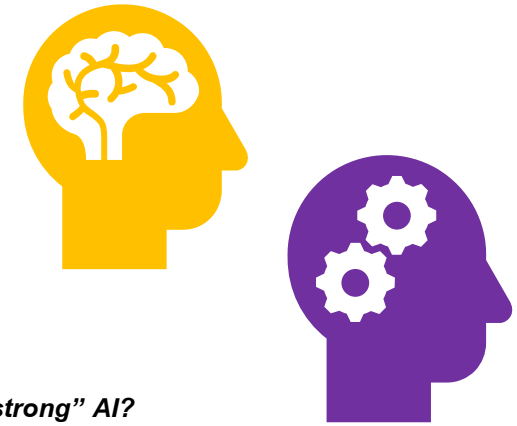
  An example of such technology is Google's Alpha Go[4]. It has beaten professional players (physical persons) and uses an elaborate network. Despite these facts, it will be unable to adapt to playing chess or to other functions other than playing Go.



- **Limited memory:** the AI uses pre-programmed knowledge and observations carried out over time. The on-going collected data gets added to the static data within the AI machine, technology or algorithm. The observations are added to the pre-programmed representation of the world. However, this data is temporary: it is only used to help evaluate a situation and make a decision. Limited memory AI cannot learn from past experiences and will have to constantly re-evaluate its environment. This explains why it is classified as a "narrow" AI.

  Limited memory AI is namely used for autonomous cars. They will observe other cars' speed and direction to avoid getting hit and will also added statistic data such as lanes or traffic lights.





What are the types of "strong" AI?

- **Theory of mind:** this type of technology can represent the world and understand people and things in it. The theory of mind AI is capable of reading and understanding emotions which will in turn alter the technology's behaviour. It is important to stress that this AI has yet to be developed.
- **Self-awareness**: self-aware AI does not exist yet. The machine or device will be able to form representations about itself. It will be able to display self-driven reactions. Self-aware AI is an extension of theory of mind AI.

Let us underline that as of now the issues raised are the same regardless of the type of AI considered. This may change once "strong" AI has been developed. It seems like it will most likely be considered as holding rights and being liable.

4. https://deepmind.com/research/alphago/

Sheet n°3: Can Artificial Intelligence hold Intellectual Property rights?

AI is an adaptable technology. It can be an app on your phone, a bot, a home security device or even a humanoid robot. Recently, a controversial question has emerged regarding whether AI based technologies, and more specifically robots, can hold Intellectual Property rights on their creations.

For example, the computer program AARON has been painting since the 1970's. Can AARON be considered an artist and its work protected by copyright? Does its creator hold the rights? There is no single answer to this question. Indeed, every country has different legislations and interpretations of the law.

It must be kept in mind that this question arose from the use of deep learning methods. Deep learning is similar to an artificial neural network capable of processing important volumes of data. The technology or machine learns as it goes and can take on new tasks or ways of parsing data. In some ways, it can create new patterns of thinking and develop its skills.

Can AI have a legal personality?

Before considering whether AI technology can hold Intellectual Property rights, one must determine whether it can have a legal personality to claim such rights. In France, there is no specific legislation granting a legal personality to AI technology. It is considered as a good. Therefore, AI and robots cannot claim rights whereas the creator or programmer may. However, this could change in the future seeing as there are no obstacles in the legislation to granting a legal personality to AI technology.

The French Parliamentary Office for the Evaluation of Scientific and Technological Options published a report[5] which namely contains comparative lists of certain countries' legislations regarding Intellectual Property. Most countries do not yet have legislation specific to AI technology or devices. At this time, only assumptions can be made by interpreting the applicable legislation.

5. https://www.senat.fr/notice-rapport/2016/r16-464-1-notice.html

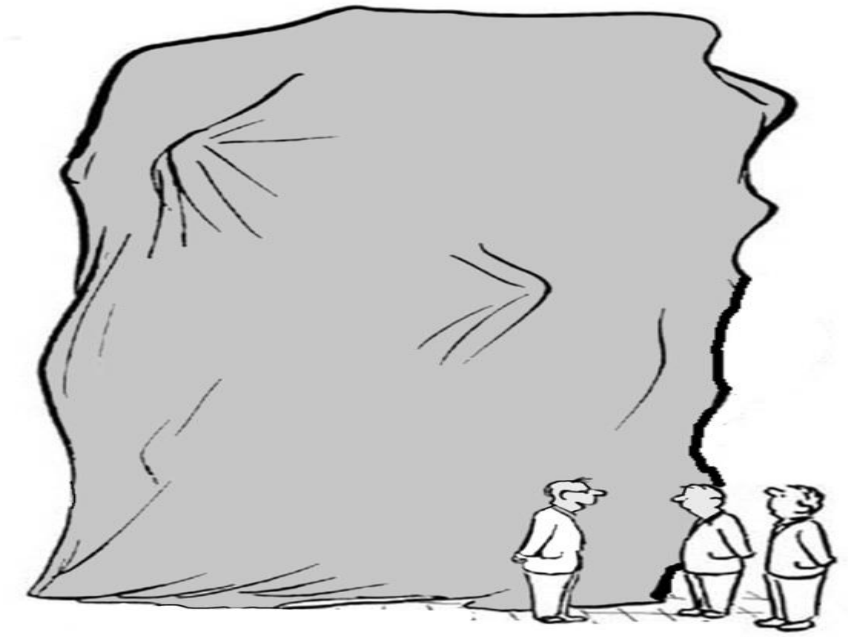
What is the situation today?

Under French copyright law, only humans have authorship. Authorship protects original intellectual works. Underlying this definition is the notion of creation and, according to the French doctrine, creation is intrinsic to human beings. A device/technology cannot create and as such cannot be considered as an author or benefit from the rights attached to authorship. However, the situation is completely different in the United-Kingdom. Under the Copyright, Designs and Patents Act 1998[6], a computer-generated work is subject to the protection of copyright. It is defined in Article 178 as a "work generated by computer in circumstances such that there is no human author of the work". This section could easily be applied to works created by AI technology.

Concerning patents, the situation is a little more complicated. If one looks at French patent law, an invention can be patented if it is new, involves an inventive step and is susceptible of industrial application. None of the conditions hinder the possibility for a robot to be granted a patent if its invention respects the conditions set forth. This could have been the case for the robot named Adam[7] which discovered new scientific knowledge about the genomics of the baker's yeast Saccharomyces cerevisiae in 2009. Adam's discovery was patentable. The question of whether devices and AI technology should be granted Intellectual Property rights is not that far off.

The European Union has been working on the issue. It has even published reports and opinions on the subject. For example, the European Parliament adopted a resolution[8] on the 16th of February 2017. It holds recommendations for the European Commission regarding civil law and robotics. The resolution namely states that the laws of Asimov should be respected and underlines the need for specific legislation to regulate AI and robotics in general.

Thus, today AI technology cannot claim rights. Most of the current legal frameworks offer flexibility and could be adapted to grant Intellectual Property rights to AI technology.



6. https://www.legislation.gov.uk/ukpga/1988/48/contents
7. http://www.cam.ac.uk/research/news/robot-scientist-becomes-first-machine-to-discover-new-scientific-knowledge
8. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//FR

Sheet n° 4: Intellectual Property rights and Artificial Intelligence : who can claim rights on the works?

AI has raised numerous questions through its emergence and developments. As previously stated in this paper, the definition and regulation of AI are critical questions as well as Intellectual Property.

This Sheet will focus on copyright. It assumes that works created by an AI can benefit from the protection of Intellectual Property rights. If one starts from this premise, then the next question to arise is: who is the author? Who can hold rights on the work created by the AI? It must be underlined that this issue is far from being settled.

The legal notion of author is not uniform. In France, “copyright belongs, unless proven otherwise, to the person or persons under whose name the work is disclosed” (Article L. 113-1 of the Intellectual Property Code)[9] whereas in the United-States, the author is not clearly defined and the Law merely stated that the “copyright in a work protected under this title vests initially in the author or authors of the work” (17 U.S. Code § 201)[10].

However, the notion refers to the person holding initial ownership rights over the work. Thus, when considering who can hold Intellectual Property rights over an AI’s creation, it is important to distinguish between the author and any third-party holding a license.

We have drawn an overview of actors which can be considered as eligible owners of rights on the work created by an AI.

Can the AI’s programmer hold Intellectual Property rights?

The programmer is the person at the heart of the AI’s creative process. He or she is the one creating the algorithm which is the source of the creation. The programmer will determine which data and how the latter are to be processed, what functions the AI is to perform and so forth. He or she puts in a creative effort.

However, the programmer is not the one choosing the parameters of the work; the user is. Although the programmer is at the heart of the creative process his or her connection with the final work is overstretched unless he or she is also the user.

9. https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000006278881
10. https://www.law.cornell.edu/uscode/text/17/201

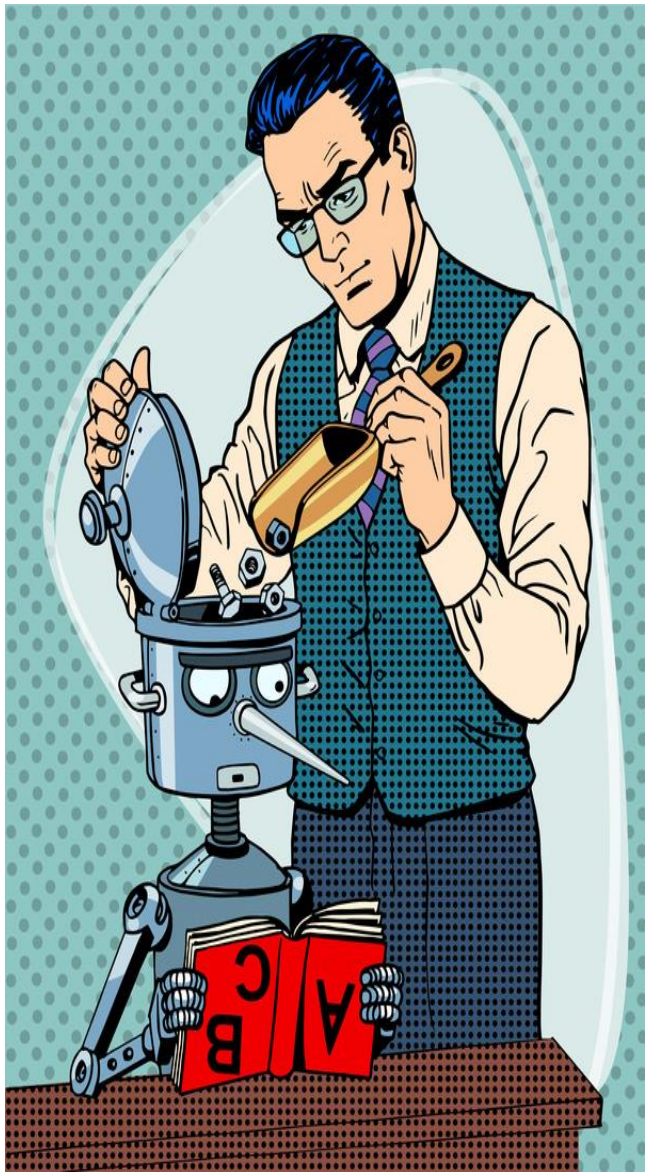
Moreover, several issues arise. How would this situation play out in practice? If the programmer is the has intellectual property rights attached to the AI's creation, what rights do the users hold? What if several programmers work on the AI? Could each actor be considered as a co-owner? Who would be liable in the event of litigation?

What about users of AI?

The user of the AI will most likely be the owner of the physical device or the person controlling the program. In either case, the user of the AI has a strong case to claim ownership rights on the AI's work.

The user is the person who puts in place the creative framework by using the AI for its purpose. Human intervention is needed to initiate this process. Indeed, devices or programs or machines will not start on their own. A physical person must turn them on, chose the setting, etc.

Nonetheless, depending on the type of AI considered, a physical person's intervention in the creative process may more or less be minimal. The more the AI creates independently, the harder it is to grant Intellectual Property rights to the user. For example, AI which combines pieces or extracts of different data, whether structured or not, through algorithms will involve minimal human intervention. The AI will create a work from various data and the work will not be a reflect of the user's personal preferences or choices (ex: Deep Dream Generator)[11].



The specific case of licenses

A license grants to the licensee a right or rights on a work. Two distinct situations arise here. A private licensee is in an analogue situation to the user except that the licensee does not hold ownership over the AI. The same reasoning may apply under the condition that the licensee is free to use the AI as a user/owner would.

However, the situation is slightly more complex when the licensee uses the license for commercial purposes. The licensee is less likely to change the parameters or experience with the AI. Despite his or her potential financial investment, he or she will most likely not intervene in the creative process. Such a licensee seems less likely to be granted Intellectual Property rights on the AI's work.

The questions raised in this Sheet, as well as the ideas developed, have yet to be confirmed by courts or regulations.

11. https://deepdreamgenerator.com/

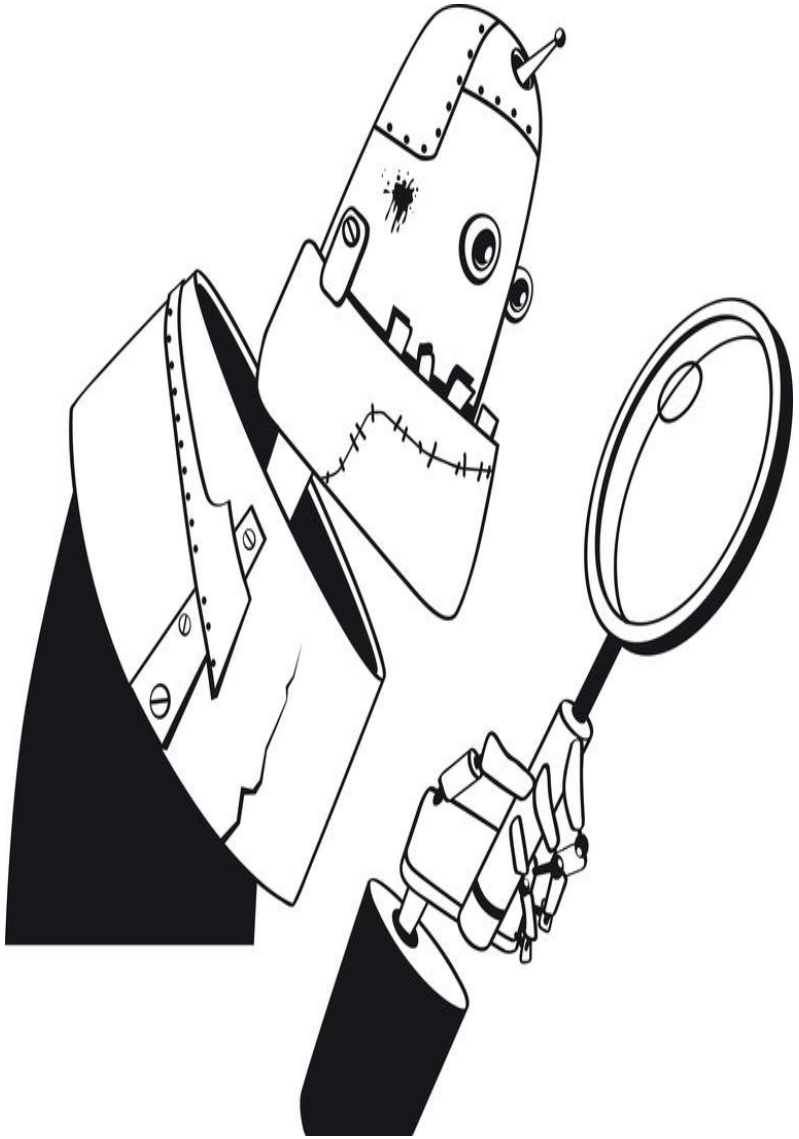
Sheet n° 5: Is Artificial Intelligence liable?

As the legislation is applied at present, the principle of liability is the following: laws only govern the conduct of humans and the machines they use or the pets they own. However, how is law to govern AI which mimics human behavior? Who is responsible for a violation of the law by the AI?

Although this question arose at least 30 years ago in the case *United-States v. Athlone Industries*[12], the answer is still under debate on whether AI is liable for violations of the law. In the case stated, the court held that "robots cannot be sued" and discussed how the manufacturer of a batting practice pitcher machine is liable for civil penalties for the machine's defect.

However, AI has developed in more complex ways since the 1980's and is now part of our everyday lives. People have smartwatches, Roombas, connected fish tanks… The new hot item is automatic cars. Although some countries have published guidelines regarding automatic cars and their use, Germany[13] and the United Kingdom[14] for example, there is no specific applicable legislation to AI technology. Who is responsible if an automatic car is involved in an accident? How can one prove who was driving?

This Sheet presents the various solutions considered and applied.



AI considered as a good?

Traditionally, AI is considered as a good and, as such, the owner or user is responsible for any wrongdoing or harm caused by the good. The same goes for any defect while using the machine or technology. However, if the malfunctioning is due to a code error, the programmer could be held liable. In practice, this will be hard to prove namely if there is an open-source software. A solution could be to publish guidelines for programmers and clearly define the contractual duties and obligations of each party (owner, user, programmer, manufacturer…).

In this context, another question emerges: if several individuals can be held liable, are they jointly liable or joint and severally liable? And what becomes of the owner or user's liability? One could consider that AI comes with inherent risks and that the user or owner may not be able to recover the full amount of the damage if he or she is partly responsible. Tort law offers solutions seeing as rules could be drawn from those for malfunctioning products.

It must be underlined that there is no unanimous answer. Indeed, each country will have to determine the applicable

12. https://law.justia.com/cases/federal/appellate-courts/F2/746/977/31282/
13. https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile
14. https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles

rules to AI according to its existing legislation. Moreover, the issues addressed in this article are still under debate. On February 16th 2017, the European Parliament issued a resolution[15] with recommendations for the Commission regarding the civil law rules in relation to robotics.

The issue becomes more complex when considering deep learning AI.

An independent legal identity for AI?

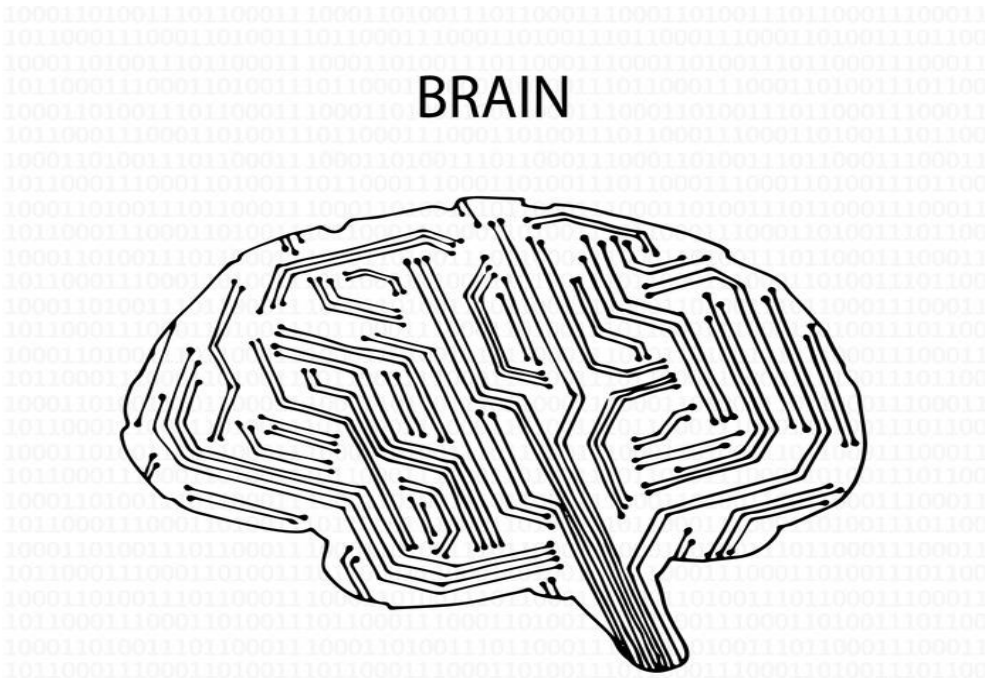
AI technology is not standardized per se. Indeed, some AI technologies are capable of deep learning, which means that the machine or technology can develop new skills by learning innovative ways to parse data.

Most of the issues arise with machines capable of deep learning seeing as machines are usually inanimate objects. If a machine can undertake a new task which was not requested by its owner or user, who is responsible for the harm or damage?

If AI is deemed to have a separate legal identity, vicarious liability could apply. For example, pet owners are responsible for the harm caused by their pets. Animals are autonomous similarly to AI. However, if AI were to be granted a separate legal identity, specific legislation would have to be drafted. New rules were created for businesses, the same could be done with AI.

What is the next step?

There is no legal vacuum regarding AI's liability. Current laws and case law could be applied. However, it is still a case-to-case basis and does not offer a general framework. Considering the constant evolution of AI, a specific legislation will most likely be needed. Many countries are currently working on drafting a coherent legislation. The European Union namely published a charter on robotics.



15. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//FR

Sheet n°6: Predictive algorithms and Artificial Intelligence: what are the major issues?

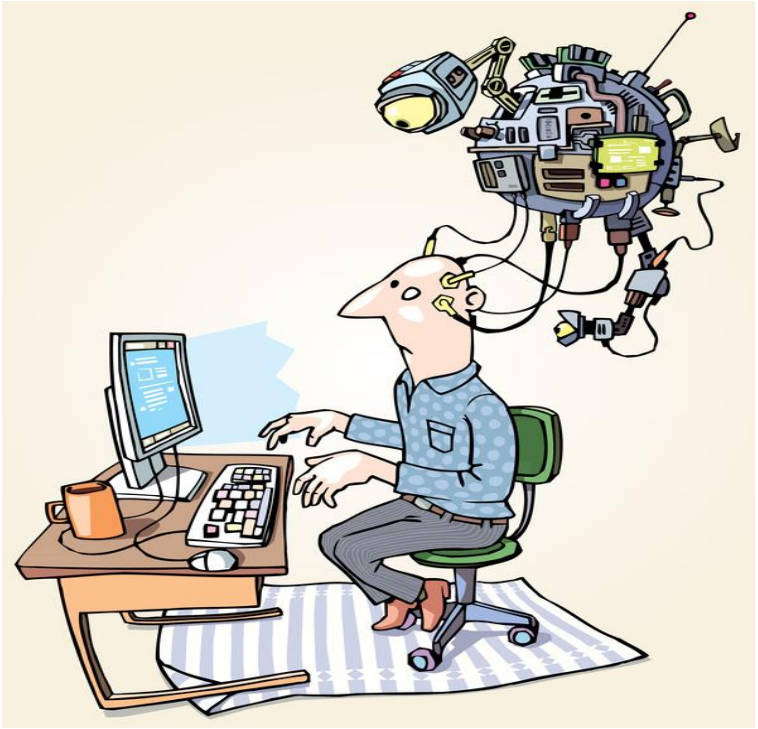
What exactly are predictive algorithms or predictive analytics? In a few words, predictive analytics are data analysis technologies and statistical techniques which aim at answering the question: what is going to happen in the future? The predictions are based on the data collected to forecast future events (fraud detection, churn prediction, defaulting on a loan, targeted marketing…). To inquire further into the subject, this article[16] provides a more specific definition.

These notions have become a key component for certain business strategies and have become increasingly common in most business sectors. They are also inherent to AI to the extent that the latter may use machine learning, which is a method used to extract models from big datasets to make predictions.

For example, Amazon uses predictive analytics to determine the products a user might like based on his or her shopping history and has even obtained a patent for "anticipatory shipping"[17].

How to protect the rights and freedoms of data subjects?

It must be underlined that predictive algorithms are based on the processing of Big Data and namely personal data. As such, they are subject to the applicable regulation on the protection of personal data and must comply with the regulatory requirements. For data subjects, this entails exercising their rights and being informed of the purposes of the processing activities.



How can companies inform their clients that their personal data are being used for predictive purposes? Can such purposes be defined beforehand? How can the processing be clearly explained? Information notices may be an adequate solution if the company had previously decided to carry out a predictive analysis and had defined its business goal.

16. https://www.pcmag.com/article/345858/predictive-analytics-big-data-and-how-to-make-them-work-fo
17. https://www.forbes.com/sites/onmarketing/2014/01/28/why-amazons-anticipatory-shipping-is-pure-genius/#7f1088c34605

Furthermore, how can the clients as data subjects exercise their rights? If a client requests the transfer of his or her data, how can the transfer be made if the data is used for a predictive analysis? What happens if the data subject requests the erasure of his or her data? If he or she exercises his or her right to data portability?

In practice, if the prediction is faulty, how can a person contest the prediction? Is there any way of proving the default? Is any recourse available for the clients? Are there existing remedies?

What safeguards for the data collected?

Another major hurdle AI systems using predictive algorithms must overcome is the determination of the appropriate data to be collected. Indeed, depending on the data collected, the prediction may change.

For example, if a bank is using AI to predict the probability of clients defaulting on a loan, what data should be collected? Does the bank need the clients' age? What time period should be considered?

Underlying the determination of the appropriate data processed are the questions of the data's scope, quality, quantity and trustworthiness. The person or company using predictive algorithms must pay particular attention to these questions and carefully decide the business objective pursued. The business objective will be the algorithm's "goal" and the prediction will be an actionable outcome for the company or person. Thus, the algorithm will determine the appropriate data needed to reach the business goal and may answer some of the underlying questions.

However, it will not address challenges of security and transparency. Indeed, these challenges are intrinsic to any data processing activity. They become all the more difficult considering the fact that models created by machine learning technologies will be obscure for humans in most cases. As such, if a problem were to occur, how can it be fixed? If an unauthorised third-party inputs data to trick the algorithm, what are the means to correct the manipulation? How can transparency be ensured?

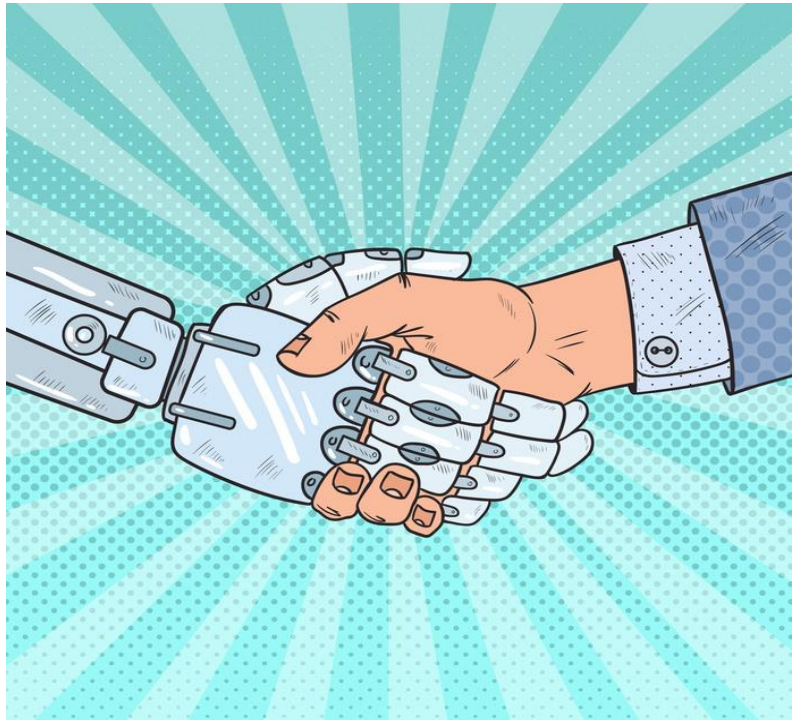
What steps can be taken?

Solutions to the issues raised in this article have yet to be found. However, the GDPR[18] will provide an appropriate framework. The GDPR strengthens data controllers' obligation and aims at rendering them more accountable. Moreover, it imposes new requirements regarding personal data security to which predictive algorithms may be subject.

However, considering the particularities of predictive algorithms or analytics, and namely the volume of data and the predictive purpose of the data processing activity, specific legislation may be needed.

18. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR

Fiche n° 7: Can Artificial Intelligence and FinTech support each other?



What is FinTech? How does it work? What issues does it present? What role does AI play in all this?

Financial Technology, "FinTech"[19], encompasses businesses aiming at providing financial services by using software and modern technology. The term was first coined by a New York banker in 1972 and refers to the intersection of technology and financial services. It has seen a rapid growth over the past few years.

The use of software and modern technology confers advantages to Fintech such as efficiency and rapidity. FinTech can namely be coupled with Blockchain (ex: ICOs or contracts).

How do AI and FinTech interact?

Combining AI and FinTech allows for more personal and precise financial services. AI technologies are namely capable of crunching extensive and various data even if the data are unstructured. This enables customers to better manage their finances and professionals to have an overview of the financial situation, be it for a customer, an investor or a partner. AI provides Fintech with the necessary data to perform the financial services. It can even go a step further with predictive algorithms (see Sheet n°6) such as is the case with Equity X[20].

Equity X is an illustration of an innovative technology combining AI and Fintech. The company created an AI-driven equity valuation tool. The AI will predict future numbers based on sector trends. Investors will thus be able to easily track the trends whereas innovators will benefit from a market-to-market valuation. Equity X is a B2C (business to consumers) and a B2B (business to business) commercial activity.

AI technologies can thus be used to help clients or professional in their financial decisions, manage trade decisions, structure the processes and rules and help process the data. They greatly expand the potential of FinTech.

FinTech also raises concerns. How much does one trust AI with one's money? What happens if the AI technology has a default? Seeing as FinTechs are not regulated, what protection is granted? Most of these questions have yet to be answered.

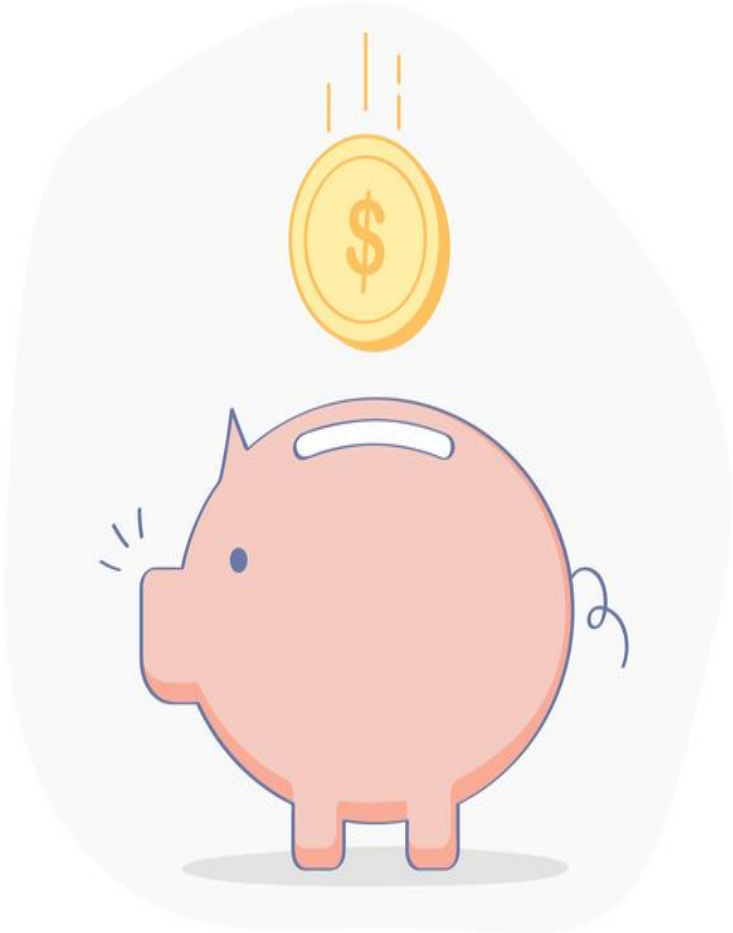
19. https://fintechweekly.com/fintech-definition
20. https://www.equity-x.com/

How can FinTech be regulated?

It must be underlined that Fintechs engage in traditional banking functions and generally provide financial services and products. One of the reasons explaining this lack of regulation is the legal qualification of FinTechs. Should they be regulated as Information Technology service providers or as financial companies? Some countries have chosen the latter and taken initiatives.

For example, the Office of the Comptroller of the Currency (OCC) in the United-States published a paper "Exploring Special Purposes National Bank Charters for FinTech Companies"[21] in December 2016. It further drafted a Supplement[22] in March 2017 which, if adopted, would provide substantive standards and procedures for the OCC's evaluation of an application by a FinTech company for a charter as a special purpose national bank.

The latter is a federal corporate form authorizing banks to conduct business on a nationwide basis and subjects the bank to uniform standards and rigorous federal oversight. Thus, FinTechs could be subject to the same standards as banks.



Another example is the European Payment Services Directive n°2015-2366[23] which will be applicable on the 13th of January 2018. It aims at providing legal foundation for the further development of electronic payments within the European Union (EU). It sets out rules concerning strict security requirements, transparency and the rights and obligations of users and providers for payment services. Fintechs are directly concerned as they provide electronic financial services.

Furthermore, FinTechs should be aware of the coming into effect of the GDPR[24] on the 25th of May 2018. They will be considered as data processors and subject to reinforced obligations namely concerning security and transparency.

21. https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf
22. https://www.occ.treas.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf
23. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
24. https://www.avocats-mathias.com/donnees-personnelles/gdpr-compliance

Sheet n°8: Artificial Intelligence and the GDPR: how do they interact?

AI is a broad notion referring to technologies or systems enabling a computer to perform tasks involving a simulation of human intelligence including decision making or learning. In order to do so, the technology or system collects voluminous amounts of data (called Big Data) and namely personal data.

AI and the protection of personal data are intertwined. AI will therefore be subject to the GDPR[25] when it comes into effect on May 25th, 2018. As such, it will have to adapt and overcome the hurdles presented, namely regarding Big Data.

Who is concerned?

The GDPR applies when the controller or processor is established in the European Union (EU) or when the processing activities relate to data subjects in the EU (Article 3 of the GDPR)[26]. Data controllers or processors outside the EU can be subject to the GDPR.

Companies using AI may have to comply with new obligations and should be considering whether they are concerned, and if they are, how to conform to the GDPR. This is all the more important considering the fact that data controllers will be subject to the principle of accountability (Article 24 of the GDPR)[27].

In practice, he or she shall "implement appropriate technical and organizational measures" to ensure compliance with the GDPR's requirements (ex: encryption or pseudonymisation). These measures will be determined on a case-to-case basis depending on the type of business, the number of data subjects, the type of data processed and so forth.

The appropriate measures must also be determined by carrying out a data protection impact assessment when the processing "is likely to result in a high risk to the rights and freedoms of natural persons" in regard to the nature, scope, context and purposes of the processing (Article 35 of the GDPR)[28]. Article 29 Working Party (WP29) published guidelines regarding data protection impact assessments on October 2017[29]. This new obligation under the GDPR reinforces the accountability of data controllers.

In practice, data controllers will have to adapt their procedures to conform to the GDPR and may have to incorporate or modify their organisational and technical measures.

25. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR
26. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR
27. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR
28. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR
29. https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

What are the major hurdles?

Article 5 of the GDPR[30] lists the principles relating to processing of personal data. It namely holds that the personal data must be processed in a transparent manner in relation to the data subject.

How can AI technologies ensure transparency for the users? The European Data Protection Supervisor[31] has identified two problems: companies may not want to disclose how the personal data is processed on the grounds of trade secrecy and the difficulty of explaining a prediction when the latter is based on an AI algorithm using machine learning. Moreover, can a purpose be determined prior to the processing? How to explain the ever-changing results according to the personal data collected and its volume? Information notices will have to be carefully drafted.

It also holds the principle of data minimisation under which only "adequate, relevant and limited" personal data can be processed in relation with the purposes of the processing. However, this principle seems in contradiction with the essence of AI. How can both be reconciled?

Article 6 of the GDPR[32] enumerates the different grounds on which the data processing will be lawful such as the data subject's prior and informed consent, the performance of a contract or for the purposes of the legitimate interests pursued by the controller. Considering the voluminous amounts of data processed by AI technologies and their various sources, how can one determine whether the personal data was lawfully collected? As stated above, if the data subject isn't clearly informed, can he or she give informed consent?

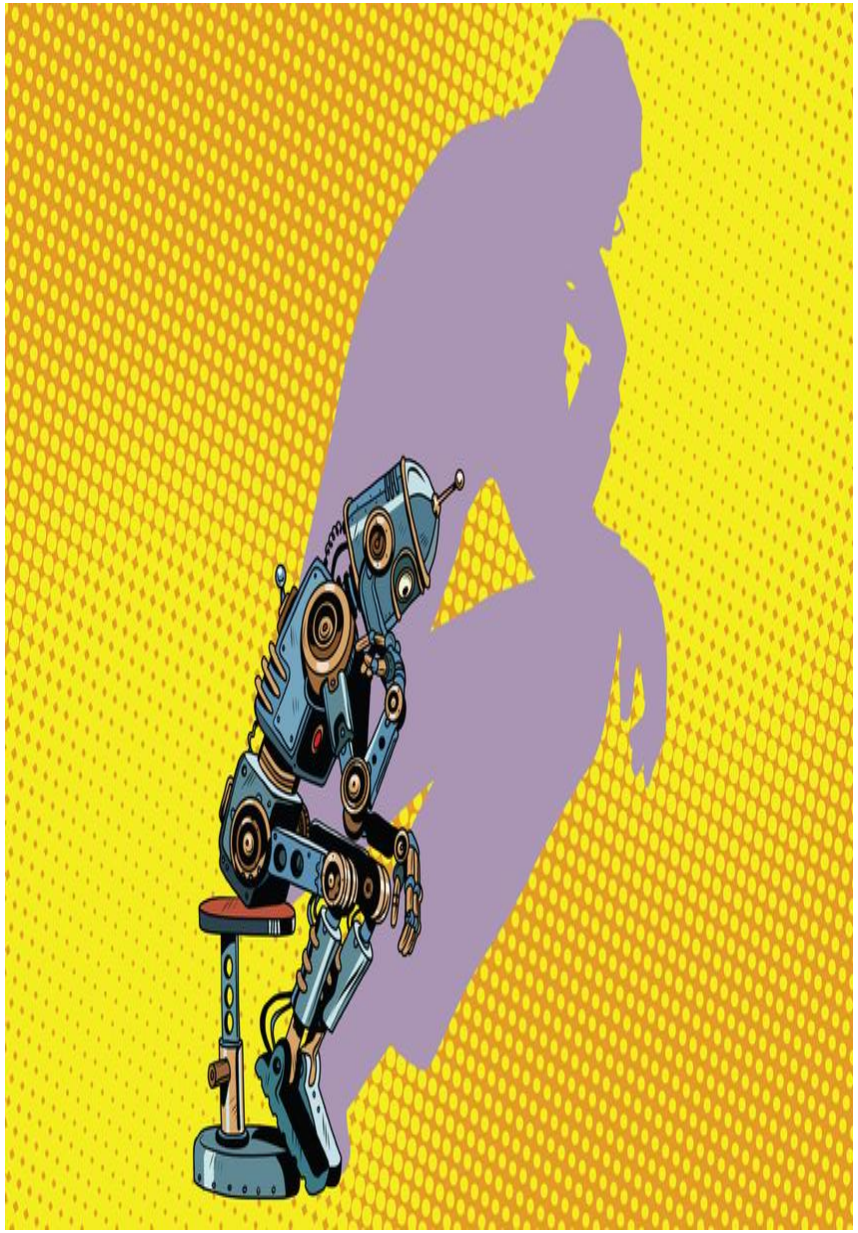
The enshrinement of the notions of privacy by design and of privacy by default[33] should also be considered. They ensure that only the necessary data, in relation to the purpose of processing activities, are collected as well as their confidentiality and security.

The data controller must implement appropriate technical and organisational measures integrating the necessary safeguards into the processing. In practice, AI technologies will have to be designed so as to respect these principles. The latter will limit the amount of data which can be legally processed.

30. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR
31. https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf
32. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR
33. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR
34. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR

Another hurdle to be overcome is the right of data subjects "not to be subject to a decision based solely on automated processing, including profiling" (Article 22 of the GDPR)[34]. AI technologies are directly concerned as an automated process. However, exceptions to this rule apply when it is provided by Member States' law, is necessary to enter into a contract or is based on the individual's prior consent. In the latter two scenarios, data subjects will have the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. They have the right to receive a justification of the automated decision. An issue arises when AI becomes so complex and processes such voluminous data that a justification cannot be given. How will controller or processors deal with this issue? How will data subjects' rights be respected?

Finally, what happens in the event of a personal data breach? Controllers must notify the competent supervisory authority without undue delay and may be required to inform the data subject (Article 33 of the GDPR)[35]. WP29 clarified this obligation in its guidelines on Personal data breach notifications on October 3rd 2017[36]. It stresses the importance of notifying the supervisory authority without undue delay and guides data controllers and processors through the various steps of the notification.



However, the increasing complexity of AI may make it difficult to determine when a cyberattack or data breach has taken place. Furthermore, how can the controller identify the entity liable for a malfunctioning or data breach? How can he or she identify all the data subjects if the AI processes various and voluminous amounts of data? Can efficient procedure be put in place?

To conclude

Compliance with the GDPR is strongly encouraged. The fines for non-compliance range from €10,000000 or up to 2 % of the total worldwide annual turnover of the preceding financial year to €20,000,000 or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year. The more stringent sanctions aim to deter non-compliance.

The issues presented in this article have namely been considered by the Information Commissioner's Office (ICO) in its paper "Big Data, AI, machine learning and data protection"[37]. They have become a center of interest for most supervisory authorities and legislators.

35. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR
36. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
37. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Mathias Avocats

Do you have a question?
A team dedicated to achieve your ambitions will reply:
01 43 80 02 01
19, rue Vernier – 75017 – Paris

Find our lawyers' practical advice on twitter:
@GaranceMathias

You can subscribe to our Newsletter on the firm's website:
www.avocats-mathias.com