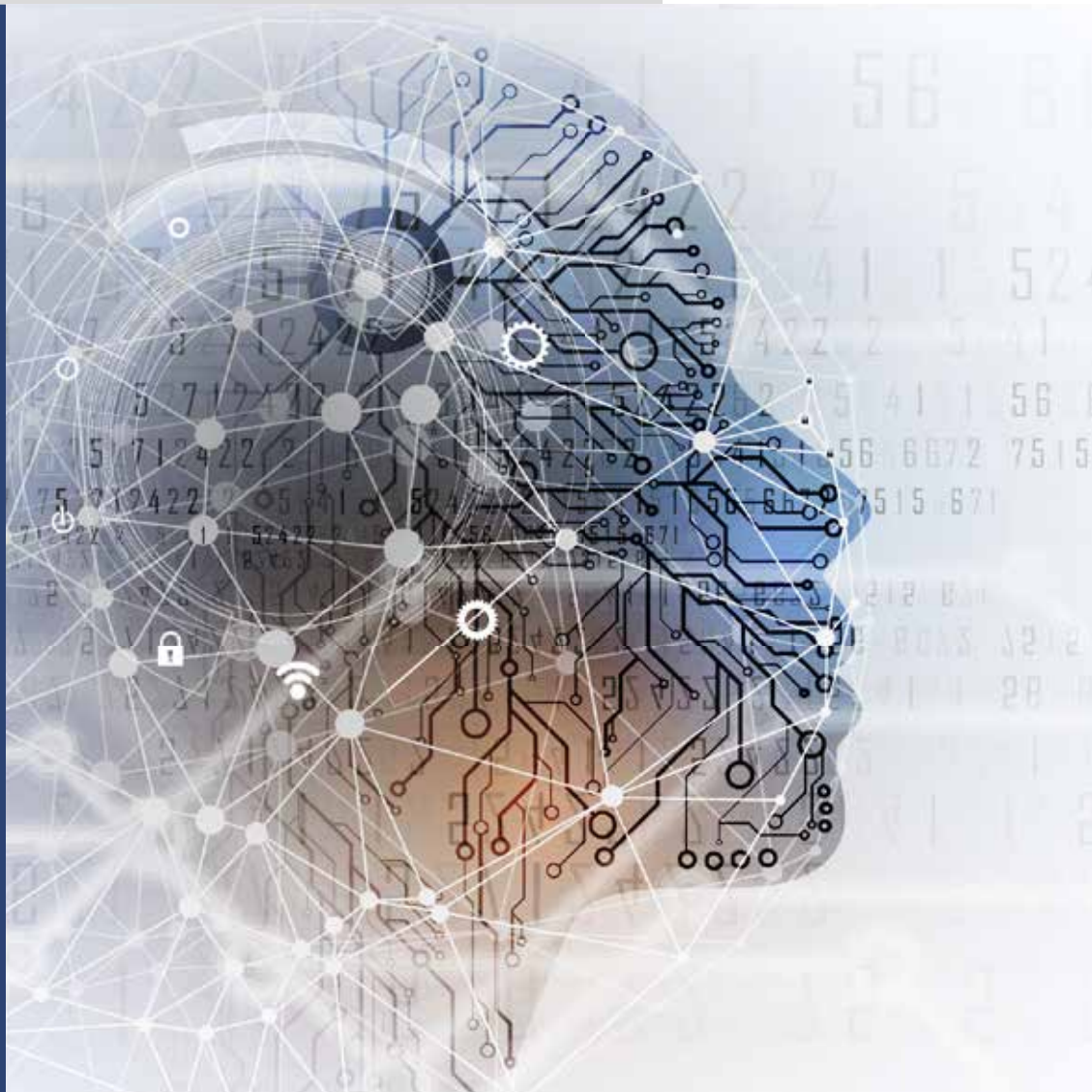
Council of Bars and Law Societies of Europe
The voice of European Lawyers

Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE CONSIDERATIONS ON THE LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE

2020



Contents

Executive Summary

With this paper, the CCBE sets out a number of considerations about the various legal aspects arising out of the use of AI in the following areas which most directly concern the legal profession:

A. Artificial intelligence and human rights

Virtually all human rights can be affected by the use of AI systems. In this paper, the following have been addressed in particular:

- The **right to a fair trial** due to, among others, the inherent lack of transparency in the way AI operates.
- The **right to freedom of expression** due to increased scrutiny and control of the way people express themselves.
- The **right to freedom of assembly and association** when AI is used to identify participants of assemblies or protests.
- The **right to life** in the context of smart weapons and algorithmically operated drones.
- **The right to privacy and data protection** due to the very nature of AI and how it functions by processing, working and combining data.

In this regard, there is a need for extensive discussion to determine whether **new legal frameworks** may be needed to codify the principles and requirements governing the use of AI, in conjunction with voluntary **ethics codes** committing AI developers to act responsibly. Putting AI systems under **independent and expert scrutiny**, **duly informing persons** impacted by the use of an AI system and ensuring the **availability of remedies** for these persons already appear as appropriate recommendations.

B. The use of AI by courts

A fundamental debate is needed to critically assess what role, if any, AI tools should play in our justice systems. Increasing access to justice by reducing the cost of judicial proceedings through the use of AI tools may sound like a desirable outcome, but there is little value in increasing access to justice if the quality of justice is undermined in doing so. Therefore, **AI tools must be properly adapted to the justice environment**, taking into account the principles and procedural architecture underpinning judicial proceedings.

To this end, the following main issues should be considered by Courts:

- Possibility for all parties involved to **identify** the use of AI in a case
- **Non-delegation** of the judge's decision-making power
- Possibility to **verify** the data input and reasoning of the AI tool
- The possibility to discuss and **contest AI outcomes**
- Compliance with **GDPR** principles
- The **neutrality and objectivity** of AI tools used by the judicial system should be guaranteed and verifiable.

C. The use of AI in criminal justice systems

Some of the police forces' work in the **prevention of crimes** – including all forms of technical surveillance such as **intercepting, collecting and analysing data** (text, audio or video) and **analysis of physical evidence** (DNA samples, cybercrime, witness statements, …) – can potentially be technically supported by the use of AI. This also gives rise to various issues; for example, inherent **bias** in tools used for predicting crime or assessing the risk of re-offending and tools like **facial recognition technology** being inaccurate at identifying people of different races. Such forms of discrimination pose a threat to civil rights. Additionally, the use of AI in the field of **digital forensic work** and **re-offence risk assessment** faces challenges, given that the specific ways the algorithms work is usually not disclosed to the persons affected by the result of their use. This leaves the defendant unable to challenge the predictions made by the algorithms. Another concern relates to the **inequality of arms** that may arise between the more advanced capabilities which prosecutors may have at their disposal and the more limited resources lawyers may have.

D. Liability issues

The notion of "**fault**" and "**liability**" might struggle to find its place in this new environment as an AI system may cause damage as a consequence of its **own autonomous** actions determined by data and algorithms, without any "defect" in the traditional sense. In this regard, issues regarding the **burden of proof, strict liability and product liability** will all need to be reconsidered to a certain extent. In order to avoid a **responsibility gap**, the most reasonable way forward in civil liability might be, at least for the time being, that **strict liability** (with reconsidered defences and statutory exceptions) and **liability based on fault** should continue to coexist.

E. The impact of AI on legal practice

Just like many other aspects of our society, lawyers and law firms are also affected by the increase of the amount of data generated. In that regard, the use of AI in the field of lawyer´s work is, as of today, more or less limited to research tools, simplification of data analytics and, in some jurisdictions, predicting possible court decisions. Several branches can be highlighted:

- Tools facilitating the **analysis of legislation, case-law and literature**
- Tools facilitating the process of carrying out **due diligence of contracts and documents, and compliance reviews**
- **e-Discovery** solutions (automated identification of relevant documents, and technology assisted review)
- **Document automation** facilitating lawyers to create legal documents in a shorter timeframe

Several previous CCBE guidelines emphasise the need for lawyers to make conscious and responsible use of these new technologies in order to carry out their activities in the best possible way, protecting the relationship of trust between the lawyer and the client and compliance with current regulations. From these points of view, the most obvious principles to respect in the use of AI tools concern: the **duty of competence**, the **duty to inform the client**, **maintaining lawyers' independence** in terms of defence and advice, the **duty to preserve professional secrecy/legal professional privilege** and the obligation to protect the confidentiality of clients' data. This also requires a thorough assessment of the **training needs** lawyers have as it regards AI.

Next steps

The findings of this paper clearly indicate the need for the CCBE and its membership to continue monitoring the impact of the use of AI in the legal and justice area. Given lawyers' dual role, on the one hand with their active role in the judicial system and, on the other, as legal service providers, they have a unique role to play when it comes to the further development and deployment of AI tools, especially in those areas where access to justice and due process are at stake.

Therefore, and also taking into account the upcoming policy developments on AI at the EU and Council of Europe level, the CCBE may wish further to articulate its views on aspects of the use of AI on the basis of further studies and reflections by its respective committees and working groups.

Introduction

"Robots of the world! The power of man has fallen!
A new world has arisen: the Rule of the Robots! March!"
Karel Čapek, Rossum's Universal Robots

"Artificial Intelligence" (AI) is about to infiltrate many aspects of people's daily lives. The recent rise of so-called machine learning algorithms has triggered a fundamental discussion on the role technology should play in our societies and the ethical considerations that need to be taken into account when they increasingly impact the lives of citizens.

In the legal services and justice environment, legal tech start-ups have emerged throughout Europe and have brought, or are planning to bring, a range of tools on the market promising to facilitate legal practitioners with legal analysis, reduction of repetitive and time-consuming tasks, speeding up judicial processes, or even assisting judges in decision-making. Likewise, AI tools for policing purposes have emerged and started to play an important role in criminal justice systems.

The use of such technologies raises many questions and constitutes a real challenge for both judicial institutions and lawyers.

Both the EU institutions and the Council of Europe have over the last couple of years undertaken various initiatives to assess the impact of AI in different domains. For example, the European Commission's High-Level Expert Group on AI was established which published 'Ethics Guidelines for trustworthy AI' and the Council of Europe European Commission for the Efficiency of Justice (CEPEJ) has adopted an ethical charter on the use of AI in judicial systems and their environment. Following a range of other policy papers and studies, commitments have been made also to establish some kind of a legislative framework codifying certain principles and requirements which need to be respected in the development and deployment of AI tools. The European Commission President, Ursula von der Leyen, announced that she will put forward legislative proposals for a coordinated European approach on the human and ethical implications of AI within her first 100 days in office. Furthermore, the Committee of Ministers of the Council of Europe set up an Ad Hoc Committee on Artificial Intelligence which will examine the feasibility of a legal framework for the development, design and application of AI based on the Council of Europe's standards on human rights, democracy and the rule of law.

As lawyers play an important role to ensure access to justice, defence of the rule of law and protection of democratic values, they seem to have a particular role to play when it comes to the further development and deployment of AI tools, especially in those areas where access to justice and due process are at stake. In the near future, the CCBE may therefore wish to comment on and respond to consultations concerning upcoming policy developments on AI at the EU and Council of Europe level.

Hence, the objective of this paper is to assist the CCBE's member bars and law societies to make a detailed and informed response to such developments and consultations by informing them about the various legal aspects arising out of the use of AI in those areas which most directly concern the legal profession. Instead of providing prescriptive recommendations on how to tackle the issues raised, the paper identifies and explains the imminent challenges and sets out a number of high-level principles which are reflective of the values of democracy and the rule of law, and against which the use of AI can be further evaluated taking into account specific applications and circumstances. As such, this paper also serves as a basis for the various CCBE

committees to further reflect and devise policies and recommendations in specific areas, so far as relevant and necessary.

For the purpose of this paper, the term "AI" is used to describe automated systems based on machine learning algorithms. These algorithms allow the system to analyse its own experiences and make corrections for improved future performance, as opposed to automated systems based upon algorithms without any learning capabilities.

Following an introductory part explaining what complex algorithms and Artificial Intelligence are, the paper sets out the various legal aspects arising out of the use of AI by courts and in criminal justice systems, AI's relation to human rights and liability, as well as its overall impact on legal practice.

1. What are complex algorithms and "Artificial Intelligence"?

1.1. INTRODUCTION

"Artificial Intelligence" (AI) is a term which is frequently used but often misunderstood. It tends to conjure up images of intelligent, decision-making systems – either the humanoid Robots of popular imagination or at least intelligent computer systems capable of substituting for human agency. Such systems are, certainly, included within the category of AI, but so too are other, less sophisticated systems.

Indeed, as a term, "AI" is so broad and imprecise as to be of limited utility in analysing ethical and legal issues arising from its use. A measure of that imprecision is that the phrase "Artificial Intelligence" is defined in the Oxford English Dictionary not as a process, but as a field of study: "[T]he study of how to produce machines that have some of the qualities that the human mind has, such as the ability to understand language, recognize pictures, solve problems, and learn." However, as the phrase is now more commonly employed, it describes various processes carried out by computers.

Whether a program is run by a general-purpose programmable computer or it performs the functions of a narrowly specialised device, like an automatic door-opening sensor, the use of algorithms is at the heart of all computer processes.

An **algorithm** is a process or set of rules to be followed in calculations or other problem-solving operations. Such algorithms are represented by a structured series of logical steps, each capable of being answered unambiguously, and the structure of which can be visually represented by means of a flow chart.

The use of algorithms pre-dates the invention of computers. Algorithms have been used by mathematicians for millennia, but it is only with the invention of machines capable of processing algorithms – that is to say, computers – that they have come to be an inevitable influence in all areas of our lives. Some algorithms, although not intrinsic threats to our fundamental rights and freedoms, can still provoke legal issues. For example, if a door-opening sensor malfunctions as a person is passing through the doorway, the door might close on him and cause an injury. Other algorithms, such as a sophisticated system sifting through, and making decisions about, job applications, can affect human rights. Some may even be capable of impinging upon the rule of law and other democratic principles.

Clearly, the all-pervasive nature and increasing sophistication of computer algorithms requires a careful and consistent response from the CCBE to the multiple issues which may arise from their use.

Therefore, when analysing the legal issues arising from the use of computer systems, it is helpful to draw a distinction between cases involving "dumb" algorithms and those where the algorithms operate in a more complex and opaque fashion.

As helpful as these distinctions can be, it is detrimental to become obsessed with what is essentially a definition game. When defining the expression "AI", some people would include any algorithm processed by a machine, whether a programmable computer or a door-opening chip, while others would restrict its use to more complex algorithms. There may even be discrepancies within either group as to which programs do or do not qualify as "AI".

There have been attempts to define "AI" in the more restrictive sense. Thus, a definition of the process of AI is set out in ISO Standard 2382:2015: "the capability of a functional unit to perform functions that are generally associated with human intelligence such as reasoning and learning." However, the ISO standard tends to suggest a degree of precision which an AI system may not possess in reality.

The most common approach of defining AI systems is commonly based on the reproduction of abilities usually

attributable to humans in their learning and decision-making roles. Such definitions can be found in several relevant papers[1] by the bodies of the Council of Europe or of the EU Commission. Thus, the definition of AI usually includes the ability to learn, i.e. to perceive data (be it analogue or digital data) and to analyse them, and to provide outcome – whether in the form of recommendations, decisions or controls – as abilities that distinguish AI from other less evolved algorithms.

However imprecise and unhelpful the phrase "AI" may be, its almost-universal use makes it difficult to avoid. Further, a universally accepted definition which might more accurately distinguish amongst the different types of "AI" has yet to be established. In view of the upcoming policy developments at the EU and Council of Europe level, it is understood that the CCBE in the near future may wish to comment on and respond to consultations concerning so-called "AI" as the concept continues to expand.

In order to assist the CCBE and its committees to make a detailed and informed response to such developments and consultations, it is intended now to suggest a practical sub-division of the amorphous concept of "AI".

1.2. SUB-DIVISIONS OF AI

AI may be sub-divided into the categories such as simple algorithms, weak AI and strong AI.

A **simple algorithm** is, in effect, a normal, conventional computer program with which we are all familiar. It runs on a computer or device which has been programmed by a human to run a particular algorithm or set of algorithms. Though conceptually simple, it can, in its construction and operation, be quite complex, not because the technology is complex, but because the algorithms are complex. Simple algorithms have been with us for millennia, and, in machine form certainly for decades, if not centuries (in the form of Babbages's Difference Engine, designed in the 1820s).

Weak AI, by contrast, is a system which involves an element similar to an autonomy. Typically, a "weak AI" system is created using some "learning" algorithms. These algorithms carry out an automated optimization process (similar to an analysis) based on previous examples and this makes further and further corrections possible to the prediction model used up to the best possible results achievable with that given algorithm. "Learning" here is an iteration of adjusting parameters in the complex algorithms, based on examples, on expected correct values. On a sufficiently large set of proper examples and the use of appropriate algorithms, this learning can, in many domains of use, result in useful and reusable optimizations, which may appear as a (weak) AI to everyday users. Weak AI is a relatively recent phenomenon (used as a term since 1959), but is increasing in importance, especially due to the breakthroughs in deep learning methods since 2010.

Strong AI is a system which genuinely thinks for itself in the same way as a human being would do (whether it has a sense of self-identity is a philosophical, rather than a technical question). Strong AI is currently the stuff of science fiction. It does not yet exist, and it is not clear when it will materialise, if ever. This will therefore not be addressed in this paper.

The different classes of AI are best explained by reference to several examples: lifts, traffic lights, Google Go, Google Go Zero and the cancer diagnosis software that is currently available.

Conventional computer programs consist of a structured series of logical steps, each able to be answered in a "yes" or "no" format. The structure of these steps can be visually represented by a flow chart. One example is a lift, which is typically controlled by a series of algorithms determining where and in what sequence the lift is to stop based upon inputs from the "up", "down", and "floor" buttons by persons outside or inside the lift, as well as an input "telling" the lift where it is at present. Another example is a set of traffic lights controlled by inputs from detector strips under the road surface, "cross" buttons operated by pedestrians and sometimes a timer. Most persons would not regard such systems as possessing AI. More broadly, marketers and salesman are very eager to assign more sophisticated "dumb" systems as he category of AI.

On the other hand, a "weak" AI system is written using algorithms which enable the computer to "learn" from itself and make decisions which would appear autonomous to most observers. These systems, in fact, are based on machine learning mechanisms. For example, Google's AlphaGo[2] program (like earlier chess-playing programs), is programmed in such a way that the system can be "educated" with a dataset (in this case a dataset of previous Go games) enabling the system to internally derive appropriate responses to moves made by its opponent. The

1 For example:
Council of Europe, Commissioner for Human Rights: Unboxing Artificial Intelligence: 10 steps to protect Human Rights (https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64);
High-Level Expert Group on AI: ETHICS GUIDELINES FOR TRUSTWORTHY AI (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419);
High-Level Expert Group on AI: a definition of AI: main capabilities and disciplines (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651).

2 AlphaGo is a computer program that plays the board game Go.

larger and more reliable the dataset, the better the outcome. The next generation of such systems is typified by the AlphaZero[3]. Instead of being educated by a dataset, AlphaZero systems are programmed with the basic rules of the game and then set to play against itself until it became adept at playing. It is, in effect, a self-educating system. Modern cancer diagnosis software is likewise trained on datasets and from its own experience. The result is that it is significantly better at detecting early-onset cancers than humans are. However, a fault of such systems is that their internal "reasoning" processes tend to be very complex and impenetrable for many, therefore even its programmers may be unable to explain how they achieve their outcomes without incurring extra costs. This is commonly referred to as the "Black Box" phenomenon.

The essential difference between simple algorithms and weak AI systems is that the former follows a precise step of logical rules (algorithms) to achieve a goal, and it will always perform in the same way, without possibility for feedback-based improvement. Thus, simple algorithm systems will perform in the way in which they were explicitly programmed. This type of system presents fewer issues of legal liability than the weak behaviour of machine-based learning systems (weak AI). This is due to weak AI's technical capacity to "learn" from their experience. That is, with time, the system that is able to improve the way it carries out a certain task, in a way that was not explicitly programmed by a human. Therefore, it would be more difficult to identify the responsible party and understand the issue, should the system malfunction. Many (but not all) machine learning systems may be described only stochastically, which is to say by reference to their outputs. In such cases, the ability to describe, and even reverse engineer, such a trained behaviour (i.e. explain which input caused the trained behaviour) is an area of intense research. Such systems may be readily amenable to the application of existing legal principles and solutions.

In the narrow sense, AI systems may sometimes call for novel analyses and solutions. For example, there may be hidden biases or identification errors in the datasets which are used to educate the relevant system. In some states in the United States, there are AI systems that analyse the likelihood of an alleged offender committing offences if the offender is released on bail. These systems can determine whether bail will be granted. However, such systems have been accused of discriminating against particular sections of society, not because of any inherent weakness in the algorithms, but because the dataset used to educate the system contained a hidden bias. It cannot be assumed that the system will "reason" in the manner that a human might reason. Similarly, Google developed an AI photo recognition system capable of distinguishing between photographs of dogs and wolves. It proved to be remarkably accurate, until it was shown photographs of dogs and of wolves respectively against a neutral background. At that point the system effectively broke down. This outcome displayed that the system had trained itself to distinguish between dogs and wolves not on the basis of the respective physical characteristics of the animals, but on whether the background of the photograph showed a wild or a domestic setting.

1.3. ADDITIONAL CONSIDERATIONS

1.3.1. The writing of software:

When considering software creation, the average person may invoke the image of an individual developer or team of developers writing software from scratch. However, this is rarely the case. It is essential to understand that these systems (especially those using open source software, whether individual programs, or entire platforms such as the Android operating system) are often built in a way that make it nearly impossible to identify a single developer or group of developers.

The original software is likely to have undergone multiple modifications at many hands. Sometimes the number of people working on a piece of software can reach well into the hundreds. The licensing model, for example with the GPL family of licences, may be such that it is unlikely to be possible to identify the writers of the software, and, so far as it is possible to do so, they may reside in a multiplicity of different jurisdictions. Furthermore, a developer who has contributed code to an Open Source programme may be unaware at the time of his/ her contribution that the direction of the program might be subsequently changed and find itself incorporated as an underlying element or module in the code of an "AI" system.

This circumstance should be borne in mind when discussing issues such as legal liability.

1.3.2. Autonomy of Devices

The autonomous nature of AI systems can give rise to uncertainty. Not even experts in the AI field can necessarily be able to foresee the "decisions" made by an AI system, or to explain the process by which those decisions were

3 AlphaZero is a computer program developed by artificial intelligence research company DeepMind to master the games of chess, shogi and go.

made. Compared to non-AI systems and traditional purely mechanical products, AI systems may have inherent in them a high degree of unpredictability.

It is also relevant to bear in mind that a machine learning system which is, or appears to be as an autonomous system, might not reside on a single autonomous device or, if it does, may nonetheless require interconnectivity with external sensors or other autonomous devices to work properly or, indeed, require constant interconnectivity with a remote server.

For example, communication between autonomous vehicles may allow automated driving systems in a number of vehicles to cooperate with each other or with traffic control systems to optimise traffic flow and minimise the risk of accidents.

Furthermore, the tasks requiring to be performed by autonomous devices, including self-driving vehicles, are highly complex.

1.4. CONCLUSION

The following can be taken from the above discussion:

Care should be taken when using the expression "AI", as it can have many meanings. For this reason, this paper uses the expression "AI" to describe automated systems based on machine learning algorithms. These algorithms allow the system to analyse its own experiences and make corrections for improved future performance, as opposed to automated systems based upon conventional (even if complex) algorithms which are programmed by a human to run an algorithm that is not designed to improve based on a set of algorithms on a computer or other device. As so-called strong AI does not yet exist in reality, this paper does not further discuss "strong AI" except where flagging possible future issues.

Since the term "AI" is exceptionally broad in its scope, consultations and discussions can often fail to distinguish between systems built on conventional algorithms and systems built on machine learning. Technically these two types of systems are fundamentally different. Sometimes those differences may be irrelevant to the matter under discussion but, on many occasions, a proper understanding of the technical differences between the two types may be critical to undertaking a proper analysis of a legal problem and forming a reasoned and informed response. There may be cases where there is a good reason for a different response in the case of conventional algorithms than in the case of a machine learning.

The relevant technical considerations in any given matter may extend beyond the question of what is meant by a reference to "AI" but also considerations of the manner of the creation of the relevant software, selection and compilation of datasets used for educating the system and the extent to which any given system would be self-contained or depend upon other components or systems for its effective operation.

Therefore, in approaching all of these matters, it is critical to have a clear understanding of the technical nature of the systems potentially involved and how such systems might affect the legal profession.

2. Human rights and AI

2.1. INTRODUCTION

Historical analysis shows that the concept of human rights as we perceive it today has been developing for centuries, if not millennia. Some consider human rights to be the modern Ten Commandments,[4] but the oldest written source of these fundamental laws can be traced back even further than the times of Moses and the Ten Commandments.

Based on archaeological research, the Code of Hammurabi can be traced to the 18th century B.C. Obviously, the code includes rules abandoned by modern law regarding things such as slavery. Further, the punishments set out in the code (examples of "eye for an eye" principles can be found throughout the text) appear rather harsh compared to modern penal systems. However, the code also presents some of the earliest examples of the right to freedom of speech, the presumption of innocence, the right to present evidence, and the right to a fair trial.[5]

The concept of Human Rights was anticipated in such important national legal texts as the Magna Carta and the Bill of Rights from England, the Claim of Right in Scotland, the Constitution and Bill of rights of the U.S., and the French Declaration on the Rights of Man and Citizen. It was not until the mid-20th century that the concept of human rights and fundamental freedoms as we know it today was internationally recognized, first, in the Universal Declaration of Human Rights,[6] followed in the pan-European perspective by the Convention for the Protection of Human Rights and Fundamental Freedoms[7] and more recently by the Charter of Fundamental Rights of the European Union.[8] Today, human rights are often considered to be the basis of civilisation's behaviour and function.

2.2. INFLUENCE OF AI ON HUMAN RIGHTS

AI has the capability to influence humans and their lives. Many examples can be found throughout this paper – from the example of self-driving vehicles and the use of AI to support the provision of a court decision, to analysis of early stages of cancer. Even today, in many fields, AI systems can provide better results and productivity than humans could ever achieve, which is why humans develop AI in the first place. However, without proper precautions, the use of AI may impact human rights, which is why it is so important that AI tools are always properly assessed at the early stages of their development in order to minimise the risk of adverse impact.

Throughout this paper, various issues which arise from the use of AI in connection with certain human rights will be outlined further. However, one must keep in mind that virtually all human rights can be affected by the use of AI systems.

The **right to a fair trial** is the basis of the discussion in Chapter 3 and 4 of this paper. While issues pertaining to the use of AI in court and in criminal proceedings will be identified below, it is worth mentioning that some consider a right to a natural judge to be part of the right to a fair trial. Potential bias of the data sets which AI uses to learn is also a clear example of an issue affecting the fairness of a trial. AI systems do not understand the entire context of our complex societies. Their input data is their only context for them and if the data provided to train AI is incomplete or include (even non-intentional) bias, then the output of AI can be expected to be incomplete and biased as well. Also, at the current development stage, AI systems often lack transparency in their conclusions. They lack explainability, i.e. the ability to explain both the technical processes of an AI system and the related

4 Walter J. Harrelson, The Ten Commandments & Human Rights, Mercer University Press, 1997

5 Paul Gordon Lauren, The foundations of Justice and Human Right in early legal texts and thought (available at http://www.corteidh.or.cr/tablas/13523.pdf)

6 https://www.un.org/en/universal-declaration-human-rights/

7 https://echr.coe.int/Documents/Convention_ENG.pdf

8 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

human decisions (e.g. application areas of a system).[9] Therefore, humans do not understand or have doubts regarding how they reach conclusions. These conclusions can be harmless in ordinary use, but when used before a court, the conclusions may interfere with the fairness of the proceedings.

The right to freedom of expression and information may be affected as well – AI will allow for more scrutiny and control of the way in which people can express themselves both online and offline. While positive uses can be seen when fighting against hate speech and fake news,[10] the line between the beneficial use of AI and its misuse appears to be tenuous.

Similarly, the **right to freedom of assembly and association** comes into consideration when using AI to identify participants of assemblies, protests or of any other large gathering. While useful in some situations to protect public order, such tools can easily be misused against political opponents. Systems capable of automated recognition of individuals (face or movement recognition) and analysis of their behaviour are already available. It may well be that these tools will influence the participation of people in assemblies, thus tempering the right to freedom of assembly and association.

The right to life in the context of smart weapons and algorithmically operated drones, will also be affected by AI. The right to protection against discrimination can be engaged when employers use AI to automate parts of employee recruiting processes. Even today, systems capable of pre-selection of workplace candidates are available.

In our digital age, the amount of data humans provide about themselves is enormous. Whether it is metadata or content data, they provide many details of their personal lives or details that are just generally private. AI lives on data and its ability to work with the data and combine them is immense.[11] The **right to privacy and data protection** is therefore clearly at stake.

Democratic principles and the rule of law are closely linked to human rights as they complement each other. When noting the right to privacy, gathering of information from people's social networks profiles on their political views[12] and then (mis)using them to affect voting preferences and elections, not only tampers with the right to privacy, but also may be considered as an interference with one of the principles of democratic society and has a direct impact on public order.

2.3. GENERAL CONSIDERATIONS

Some of the possible ways available to address the issues connected to the use of AI systems will be discussed in more detail in the following sections. In general and based on currently available recommendations[13] in this field, it should be noted that thorough assessments of the effect of AI systems on various human rights, democratic principles and the rule of law seems to be one of the measures which may be used to prevent unwanted conflicts with these rights, principles and rules. Such assessments should be implemented as soon as practical, even at the early development stage by evaluating the potential impact AI systems may have on human rights throughout their entire life cycle.

It may also be appropriate to put AI systems under independent and expert scrutiny, especially when public use is intended. Making the output of such scrutiny publicly available will likely increase the trustworthiness of AI systems. Opening AI systems for scrutiny by any stakeholder may increase their trustworthiness even more; however, this will not be possible without proportionate interferences with trade secrets and other IP rights of AI developers.

For the sake of transparency and in order to enable individuals to defend their rights, it seems appropriate that the persons impacted by the use of an AI system should be duly informed that AI is being used and that data concerning him or her matter may be considered by an automated system. This corresponds with the current data protection principles, which in general must be followed when using AI, as must also any other applicable legal standards.

As is common elsewhere, ensuring the availability of remedies will likely be the appropriate measure to address cases of misuse of AI systems or damage caused by them.

It needs to be considered whether the currently available legal frameworks are adequate or need to be adapted in order to ensure that AI systems are used in compliance with human rights. Possibly, some new legal frameworks may need to be established to codify certain principles and requirements in conjunction with voluntary ethics

9 High-Level Expert Group on AI: Ethics Guidelines For Trustworthy AI (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419)
10 https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf
11 https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4
12 https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal
13 Council of Europe, Commissioner for Human Rights: Unboxing Artificial Intelligence: 10 steps to protect Human Rights (https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64)

codes committing AI developers to act responsibly. Since technology (including AI) is extra-national, where the need for a legal framework which is not limited to one jurisdiction can be supported, the development of such a framework would arguably be desirable and would seem to be in line with current developments.[14]

14 See the Council of Europe activities in this field and its Ad Hoc Committee on Artificial Intelligence that has been established on 11 September 2019 to assess the need for such legal framework: https://www.coe.int/en/web/artificial-intelligence/-/the-council-of-europe-established-an-ad-hoc-committee-on-artificial-intelligence-cahai.

3. The use of AI by courts

3.1. INTRODUCTION

In the field of justice, there are strong incentives for using AI. Public authorities have already identified the budgetary benefits that could be obtained by replacing some judicial staff with automated systems. The possible use of automated systems in judicial decision-making processes by enabling programmable and predictable judicial outcomes also brings a lot of significant challenges and risks to fair trial rights and the delivery of justice. In democratic regimes, its introduction may also be justified by the desire to broaden the supply of justice, to make it more accessible, faster and less costly. For those categories of people for whom the use of justice remains an inaccessible luxury, the possibility of having their case adjudicated with the help of a machine can be considered as progress. Certain categories of litigants, group litigation managers, are certainly ready, as soon as the reliability of the programs is sufficient, to promote their use for accounting purposes.

The potential use of AI as a decision-making tool could also enable judges to make more consistent and higher-quality judgments more quickly, rationally and efficiently. Such a use within the judiciary is already mentioned in the European Parliament's resolution of 12 February 2019 for "A comprehensive European industrial policy on AI and robotics"[15].There is, therefore, no doubt that AI will be used in the field of justice.

This raises the question of the conditions for such a use.

The aim must therefore be to continue the work initiated by the CEPEJ which has set out general principles. It is essential to extend such work by thinking about concrete applications of AI. There is a question of formulating concrete proposals that can be used as guidelines for operational decisions. In this sense, the CCBE's concerns are similar to those expressed by the European Commission's High-Level Expert Group on AI. When we look at the different possible uses of AI in the judicial process, we immediately see that its introduction within court systems could undermine many of the foundations on which justice is based. In consequence, it would be desirable map out how AI might be used in different justice architectures, to verify in each case how the AI fits into these different architectures, and to measure its effects on these architectures. (see below part 3.3).

3.2. THE NEED FOR AN ETHICAL FRAMEWORK REGARDING THE USE OF AI BY COURTS

The need to define an ethical framework for the use of AI goes beyond the field of justice alone. The European Commission has set up a group of 52 experts (the **High-Level Expert Group on AI**) which has published Ethics Guidelines for Trustworthy Artificial Intelligence[16].

Meanwhile, the CEPEJ has adopted an "**ethical charter on the use of AI in judicial systems and their environment**"[17] which also includes an "in-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data."

The CCBE supports such initiatives and remains convinced of the importance to keep monitoring the implementation of these principles and to possibly expand them in light of new technological developments and

15 European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics, Recital W: "Whereas further development and increased use of automated and algorithmic decision-making undoubtedly has an impact on the choices that an individual (such as a businessperson or an internet user) and an administrative, judicial or other public authority make in reaching a final decision of a consumer, business or authoritative nature; whereas safeguards and the possibility of human control and verification need to be built in to the process of automated and algorithmic decision-making", available here: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html.

16 See https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

17 See the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment as adopted by the CEPEJ during its plenary assembly on 3-4 December 2018, and is available online at: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

circumstances.

However, ethical reflection alone will not be sufficient to assess the impact of the use of automated tools on the judicial system. **Therefore, it is necessary to continue this analysis in order to identify effective operational principles that can govern, in practice, the use of automated tools.**

This is a difficult task because it is very hard to measure the impact of systems whose uses are not yet fixed and whose capacities are not exactly known. Although it is, of course, necessary to be aware of these limitations, a systematic examination of the different stages of criminal and civil legal processes should, nevertheless, make it possible to identify the services that could be provided at each stage of the judicial process by automatic systems. It will be useful to try to imagine the tools that could be used in the future based on knowledge of the current capabilities of computing systems, which remain limited.

This may include the use of such systems in administrative case management, witness hearings, oral hearings, the trial itself, sentencing or the enforcement of judgements in both civil, and, particularly, criminal matters. It will also be necessary to consider the automated systems and databases that may be available to prosecutors.

For example, the CEPEJ Charter also includes a list of possible uses of AI and offers a classification of these uses which range from those that are encouraged, to those that should only be considered with the most "extreme reservations". When reading the CEPEJ report, it appears that even the uses to be encouraged are likely to upset the balance of the trial. This is the case, for example, of the "valorisation of jurisprudential heritage", which allows the judge to dialogue in natural language with an AI. This situation can already lead to decisions in which it becomes difficult to distinguish between what has been decided by humans and what has been decided by the machine. For instance, the simple fact that the AI tool selects, from among the existing precedents, those decisions from which the judge should be guided in order to make his/her decision, should lead to questions about the conditions under which such a selection by the machine can occur. Any search engine designer must trade-off between the level of precision (to avoid polluting responses with multiple false positives) and the recall rate (the ability to identify all relevant documents in the database). It is, therefore. very likely that this leads to problems even though, on the surface, AI seems to be only an improvement. It is because of these possible misuses that a framework for the deployment of such applications, especially in the judicial area, must be established very carefully.

Therefore, these applications must be reconciled with the fundamental principles that govern the judicial process and guarantee a fair trial: equality of arms, impartiality, adversarial procedures, etc.

Even if the temptation to sacrifice all for efficiency may be present, these fundamental rights have to remain guaranteed to all litigants. For this reason, it is necessary to ensure in all cases that fundamental rights and their exercise are not compromised when using automatic systems.

3.3. IDENTIFICATION OF POSSIBLE USES OF AI IN COURT SYSTEMS

The CCBE has tried to map out possible uses of AI systems in the different stages of a legal proceeding. The following areas have been identified which could be impacted and for which certain principles need to be taken into account[18]:

Use of AI by Courts					
Stages	**Management of cases**	**Pre-trial**	**Trial**	**Judges' deliberation/ decision-making**	**Post sentencing**
(Potential) AI applications	- Case management system - Electronic communications - Digital platforms accessible for lawyers/clients - Automatic monitoring of procedures - Automatic system for monitoring procedural delays - Automatic system for completing procedural formalities - Automatic decisions on the progress of the case - Queue management - Automatic sorting of appeals	- Plea-bargaining: Prosecutor's databases	- Use of videoconference - Automated transcription / automated translation - Automated presentation of file's document on screens during hearings - Case management (in a situation of complex cases) - Use of emotional AI (detection of emotions, etc....)	- Case law tools - Prediction technology - Legal researches and analysis / autonomous researches - Scoring of risks / assessment of the suspect (probability of recidivism) - Automated judgments (decision trees) - Writing assistance tools and drafting judgments - Decision making systems - Intelligence assistant systems (identification of patterns, analysis of data...)	- Scoring of risks / probability of recidivism / parole opportunities
Main principles and issues to be taken into account					
Principles	- Adversarial proceedings - Rule of law, due process, security - No restriction of access to justice - Equality of arms - Transparency of decision-making - Access to data by lawyers	- Adversarial proceedings - Equality of arms - Access to data by lawyers - Data protection and compatibility with fundamental rights	- Adversarial proceedings - Fair trial - Transparency - Neutrality (in profiling) - No use of emotional AI when videos are used during a trial	- Adversarial proceedings - Fair trial - Transparency about use of AI by judge - Transparency of decision-making process - Algorithms and accountability - Liability if errors occur - Access to evidence - Right to request for a human intervention (judge)	- Adversarial proceedings - Fair trial - Transparency of decision-making process - Algorithms and accountability - Right to appeal

The above table shows that one can imagine using AI tools:

- In the management or follow-up of files.
- During hearings, either in the trial or pre-trial phase (e.g. negotiation with the Public Prosecutor's Office concerning plea-bargaining; or assessment tools to calculate a defendant's probability of recidivism, allowing prosecutors more strategically to determine sentence lengths, and parole opportunities etc).
- To facilitate the judge's decision-making (the deliberation phase).
- In the follow-up of the execution of decisions.

Furthermore, AI tools might also be deployed for the evaluation of the functioning of courts and judges. The use of algorithms is likely to allow a very detailed and sophisticated monitoring of the judicial activity of each court and even each judge. This raises questions as to whether, and, if so, to what extent, the use of these tools is appropriate or desirable. For example, these tools could be open to abuse by being employed not merely to manage court business more efficiently, but also to evaluate the "performance" of judges, including analysis of supposed biases in their behavioural patterns.

3.4. MAIN CONCERNS WITH THE USE OF AI TOOLS BY COURTS

When considering the various steps in judicial processes, it should be possible to verify the likely effects of AI on the very architecture of the judicial system.

One of the main characteristics of the current decision-making process of courts is that the judge (single judge or a panel of judges) relies on the input given by the parties. They are the ones who provide the judge with the material for their decision: facts, evidence, arguments, case law, etc. This is also referred to as the principal of

18 The sole purpose of this table is to indicate the possible uses of AI tools in the different stages of a legal proceeding. Much debate is still needed to critically assess what role, if any, AI tools should play in justice systems. As such, the list does not constitute any endorsement of the use of these tools in courts.

adversarial proceedings, i.e. that in a court case both parties to a criminal or civil trial must be heard and provided the opportunity to have knowledge of and comment on all evidence presented or observations filed with a view of influencing the court's decision.

It may also occur that the judge, under the conditions defined by the judicial systems that provide for this possibility, solicits the technical expertise of an expert not included in the list of parties. In such a case, the work provided by the expert will be introduced into the debate so that the parties can discuss its quality and relevance before the judge before he/she has made his/her decision.

It is a fundamental principle that all the elements on which judges will base their decision are debated by the parties in an adversarial manner. One of the conditions of a fair trial is that the judge decides on the documents and arguments presented to him/her by the parties. Each party must have had the opportunity, prior to the deliberation, to read and discuss the opposing party's documents and arguments. The subject matter of the judge's decision is found in the evidence provided by the parties and previously discussed before the judge.

The use of AI tools by courts could therefore brutally unbalance the current mechanisms, especially if it were accepted that the judge could access it alone, during the deliberation process.

The current general architecture of a trial is explained by the need to ensure compliance with a number of principles and to produce decisions whose main characteristics are as follows:

- Decisions are made by the judge him/herself, to whom society has delegated the power to judge.
- Decisions are made following an adversarial process, and the judge decides in the light of the arguments and evidence provided by the parties.
- Decisions are rendered by an impartial judge.
- Decisions are reasoned and contain explanations that make it possible to understand which legal provisions and precedents can justify them.

With the introduction of AI tools, there are multiple disadvantages that can be noted:

- The use of data and elements that have not been the subject of an adversarial debate.
- The exploitation of conclusions (even partial ones) that have not been obtained through the reasoning of the judge, which leads to the transfer of part of the decision-making power.
- The lack of transparency of the process, since it becomes impossible to know what should be attributed to the judge and what comes from a machine.
- Lack of level playing field (equality of arms). For example, if the prosecution office has advanced capacities to analyse huge data sets which the defence does not possess, the defendant is placed at a significant disadvantage.
- The undermining of the principle of impartiality due to the impossibility of neutralising and knowing the biases of the system designers.
- Breach of the principle of explicability, because of the existence of results that are beyond human reasoning and cannot be traced. This could also lead to poorly justified and motivated Court decisions, thus limiting the right of defence.

There is also raised the interesting question of whether there might emerge different judicial architectures from the one which we know today, especially if it is acknowledged that, in certain areas, it may become possible to entrust the settlement of a dispute to a machine. In this context, the identification of the different possible architectures would allow us to identify possible developments in the judicial system and, once again, to identify models compatible with respect for the fundamental rights of justiciable rights.

This verification is also made difficult by the simple fact that automatic tools will be developed outside the judicial system. This is an unprecedented situation because in the classic conception of legal processes, the only element which is outside the parties themselves is the judge. Automated systems must attract even more careful consideration because digital tools can in no way be considered as neutral objects or actors. The machine which follows the steps of an algorithm to achieve a result obeys instructions. There is no guarantee that this process will be fair or impartial, and referring to the concept of ethics by design may not be enough. The fairness of software can also be a mathematically inaccessible objective. The U.S. *Loomis* case[19], which ended in the Supreme Court of the State of Wisconsin, illustrates this phenomenon. In this case, an algorithm assessing an offender's chances of reoffending was used to help determine the appropriate sentence and as a result, serious questions about the influence of machines on the functioning of justice first appeared. The decision of the Court, which upheld the

19 Loomis v. Wisconsin, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017).

use of a proprietary automated system, the purpose of which was to assess the probability of an accused person offending if released on bail, has been the subject of much criticism. This was due in particular to the bias in the responses provided by the system and also to the poor quality and unreliability of its results.

Similar questions may arise about the data accessed, or on which the machine is based. The use of "black boxes" could also undermine another structural principle of the process: the explicability of the solution which it delivers. The requirement for a motivated judgment which sets out the reasons for the decision seems difficult to reconcile with the functioning of certain software applications.

These different parameters could be taken into account in the drafting of CCBE recommendations that would complement the general ethical principles already identified, in particular by the CEPEJ, on which it should be possible to rely. The CCBE and its members could thus be provided with a robust and operational reference framework, which would make it possible to evaluate the deployment of AI tools in the judicial system, with the objective to ensure that fair trial rules are respected.

3.5. AI ADAPTED TO THE JUSTICE ENVIRONMENT

There has been demonstrated in 3.4 above the potential impact of AI tools on court systems and how this could undermine principles guaranteed or ensured by the current architecture of legal proceedings. It is therefore important that AI tools are properly adapted to the justice environment, taking into account the principles and procedural architecture underpinning judicial proceedings.

The introduction and use of AI in the judicial system need to be thoroughly controlled to ensure that AI tools are effectively able to improve the functioning of the judiciary and facilitate access to the law and to justice.

Therefore, the definition and adoption of principles governing the use of AI should precede the implementation of AI tools by the judicial system. In this context, the principles established by the CEPEJ's Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment can be helpful. Moreover, the principles ideally should be transposed into operational rules (defined in advance) that will ensure that the introduction of AI tools into the judicial system would not undermine the rules of a fair trial, the rights of the defence, the adversarial principle and the independence of the judge.

To this end, the following main issues should be considered:

- **The possibility to identify the use of AI**: all parties involved in a judicial process should always be able to identify, within a judicial decision, the elements resulting from the implementation of an AI tool. There should be a strict separation between data or results from the operation of an AI system and other data in the dispute.
- **Non-delegation of the judge's decision-making power**: the role of AI tools should be defined in such a way that the use of the tools does not interfere with the judge's decision-making power. Under no circumstances should the judge delegate all or part of his/her decision-making power to an AI tool. AI tools should neither limit nor regulate the judge's decision-making power, for example in the context of the making of an automated decision. When the judge´s decision is (partially) based on the elements resulting from the implementation of an AI tool, it should be properly justified and explained in the judgement.
- **Possibility to verify the data input and reasoning of the AI tool**: in cases where the decision is likely to be based, in whole or in part, on the data or outcomes provided by an AI tool, the parties and/or their lawyers should be given the opportunity to access that tool and assess its characteristics, the data used and the relevance of the outcomes it provides. As a result, "Learning software" should only be used to the extent that it would still be possible to verify how the machine achieved the proposed result and to distinguish the elements resulting from the use of AI from the judge's personal reflection.
- **The possibility of discussing and contesting AI outcomes**: the parties should have the opportunity to discuss in an adversarial manner the data and conclusions deriving from an automated system. Therefore, the deployment of AI should always be carried out outside the deliberation phase and with a reasonable time for discussion by the parties.
- **Compliance with GDPR principles**: even outside the scope of application of the GDPR, the principles of automated decision making as set forth in Articles (2) (f) and Art. 22 GDPR should be taken into account. Hence, no decision of a court, public prosecutors' office or other body of the law enforcement and judicial systems should be based solely on automated processing, unless the conditions described in Art. 22 (2) GDPR are present. Any party subject to such processing, be it a natural person or a legal entity, should be informed about the existence of any automated decision-making by a court, public prosecutors' office or other body of the law enforcement and judicial systems. They should be entitled to meaningful information about the logic involved, as well as the significance and the envisaged consequences of such automated decision.

- **The neutrality and objectivity of AI tools** used by the judicial system should be guaranteed and verifiable.

To ensure compliance with these issues, difficulties of several kinds must be overcome. Indeed, some of the difficulties may be related to the design and implementation phase of the AI tools, while others are the result of specific characteristics of the tool itself.

3.6. CONCLUSION

Much debate is still needed critically to assess what role, if any, AI tools should play in our justice systems. Change should be embraced where it improves or at least does not worsen the quality of our justice systems. However, fundamental rights and adherence to ethical standards that underpin institutions based on the rule of law, cannot be subordinated to mere efficiency gains or cost saving benefits, whether for court users or judicial authorities.

Increasing access to justice by reducing the cost of judicial proceedings may sound like a desirable outcome, but there is little value in increasing access to justice if the quality of justice is undermined in doing so.

4. The use of AI in criminal justice systems

4.1. OVERVIEW AI USE IN CRIMINAL LAW

The use of AI in criminal justice systems is today mainly happening in the field of work of the various police forces and law enforcement authorities. The main areas are:

1. Prevention of crimes (predictive AI use)
2. Gathering and analysis of evidence

The use of AI in the field of lawyers' work is at present largely limited to research tools, simplification of data analytics and, in some jurisdictions, predicting possible court decisions.

4.2. PREDICTIVE AI USE BY POLICE FORCES

The use of predictive AI tools is part of so called "Predictive Policing" and is used to visualise and analyse crime incident patterns in order to be able to make forecasts as to the locations at which there is a higher probability that criminal acts will be committed and where, thus, the allocation of police intervention (additional officers or closed-circuit television (cctv)) may have a positive impact. These algorithms mostly make an analysis of census demographics, areas of crime, likely offenders´ locations etc. In order for these predictive analyses to be as accurate as possible, several criminological theories are taken into account, such as the "repeat victimisation theory" (the theory that a recent victim is at a temporarily higher risk of repeat crime than non-victims) and the "routine activity theory" (the theory that crime involves three conditional elements: a likely offender, a suitable target and the absence of a capable guardian). Combining all of these elements, overviews on crime probabilities are created by algorithms.

For example, the Bavarian police have used a system called "GLADIS" (Geographisches Lage-, Analyse-, Darstellungs- und Informationssystem) since 2004. The system uses standard software for creating general overviews as a basis for strategic decisions. The overviews thus generated are designed as maps and include examinations of the types of crime occurring in certain areas, the exact spatial distribution of crime and the temporal distribution of crime.

Other algorithms are designed to evaluate inherent risks relating to certain people, especially repeat offenders. Several technological methods have been developed to calculate probabilities of crime being committed by individuals, by trying to calculate how likely it is for a certain person to commit an offence. Those algorithms are based on factors like economic status, gender, age, offending history, place of residence etc.

However, the practical use of these algorithms is widely criticised, as they also include nuisance crimes which are more frequent in low income neighbourhoods, many of which are populated minority ethnic groups. Such nuisance crimes draw more police into these neighbourhoods. As a consequence, police officers observe more of these often victimless crimes, which, in turn, makes these areas appear to be even more dangerous. This, again, causes more police to be drawn into these areas and so on. Predictive AI thereby becomes a self-fulfilling prophecy and instead of preventing serious crimes, it becomes a major factor in why, in the United States so many black and Hispanic adolescents from poor neighbourhoods are being sent to prison for taking drugs or committing other nuisance crimes[20].

20 For further insight into this topic, see Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, New York, Crown, 2016, page 84.

4.3. FACIAL RECOGNITION AND OTHER TECHNICAL SURVEILLANCE MEASURES

All forms of technical surveillance, especially intercepting, collecting and analysing data (text, audio or video), are unthinkable without the use of AI. This is especially true for the initiation of technical surveillance measures, which is often triggered by AI systems reacting to a wide range of indicators ranging from "unnormal" behaviour to "trigger words" in a communication.

However, this technology has serious flaws that endanger civil rights. For example, facial recognition technology has been proven in multiple studies to be inaccurate at identifying people of different races. Also, there are grave concerns that the trigger words which are used by national security agencies are not sufficiently refined and thus the phone conversations and email correspondence of millions of people are monitored without a legal basis.

Further, the widespread use of facial recognition may pose severe risks for an open and pluralistic society if not used proportionately with a proportionate intended aim such as ensuring public safety. In many situations, anonymity is the most important safeguard of freedom, and facial recognition techniques that cover major areas in the public space endanger this freedom. The more accurate they are and the more widespread their use, the more dangerous they become.

For a more detailed analysis of the fundamental rights challenges that are triggered by the use of facial recognition technology in the context of law enforcement, reference is made to the following study of the European Union Agency for Fundamental Rights (FRA): 'Facial recognition technology: fundamental rights considerations in the context of law enforcement'.[21]

4.4. USE OF AI FOR ANALYSIS OF EVIDENCE

AI is used to analyse physical evidence such as. DNA samples, and other evidence including witness statements, physical documents, patterns of crimes and tools used by the offender. These algorithms mainly match the data collected regarding the physical evidence against data collected in various databases, for example' DNA databases, firearms databases, bank account registers etc. The results found might be presented to a court by a forensic analyst as an expert witness.

This technology is deemed as sufficient proof in most jurisdictions and has been used to solve millions of crimes, however, it is not fail-safe. There is always the risk of inappropriate handling of the DNA collected at the crime scene, including the risk the crime scene may have been compromised by the introduction of DNA to it or the transferring of DNA to the victim, a weapon and other items., either by accident or on purpose.

4.5. CYBERCRIME

As cybercriminal activities are not possible without the use of (more or less sophisticated) AI, the police and/or prosecuting authorities use AI for detecting cybercriminal activities: the evidence gathering in cyberspace is done by AI; the mapping of financial transactions would not work without AI and the scanning of the dark web would not be possible without the use of AI. There are different forms of algorithms used by police and/or prosecuting authorities to analyse data, which analysis could lead to solving a cybercrime. These forms range from algorithms applying scientific methods to the recovery, analysis and interpretation of relevant digital materials. These methods are often referred to as "digital forensics", a term inspired by the real-life use of forensics in evidence analysis. The use of data in criminal investigations is not executed only by programmable computers, but by all types of digital devices. Solving cybercrimes with digital forensic methods can be quite complicated, given the fact that digital data is easily lost or destroyed and that there is no standard or consistent digital forensic methodology. The procedures mostly stem from the experiences of law enforcement, system administrators and hackers.

To ensure a safe procedure regarding the prevention and prosecution of cybercrimes, ENISA, the European Union Agency for Cybersecurity, was established in 2004. ENISA and EUROPOL, the EU Law Enforcement Agency, provide manuals and training courses for dealing with volatile, modifiable and easily destroyable data.

As mentioned in all fields of AI, the use of AI in forensic work faces the same challenges, given that the specific ways the algorithms work is usually not disclosed to the persons affected by the result of the use of algorithms. Additionally, due to the fact that there is a technological arms race going on with perpetrators trying to use sophisticated algorithms to mask their criminal activities, law enforcement authorities are struggling to keep up with these technologies. Thus, there is a high probability that the use by law enforcement bodies of AI tools may produce results that do not reflect the truth and can lead to innocent persons being convicted as a result of the authorities being misled by the actual perpetrator.

21 FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement, November 2019.

4.6. AI USE IN CRIMINAL COURTS

Despite the widespread use of AI in the pre-trial phase of criminal proceedings, the use of AI during the actual trial is still rather uncommon in Europe. Besides the use of video conferencing (which usually involves no AI), most criminal courts in Europe do not use any kind of AI during the trial. This comes about because most European jurisdictions have strict provisions that verdicts must be made solely by judges and/or jurors. Should these tools, however, be used in the future, the same types of concerns will arise that are already addressed in Chapter 3 of this paper.

4.7. USE OF AI BY LAWYERS AND DEFENCE COUNSELS

As discussed above, the primary field in which AI is employed in criminal proceedings is during investigation and the pre-trial phase. In most jurisdictions. lawyers do not participate in this phase, except for counselling, accompanying their clients to interviews, and filing motions to take evidence or appeals. The two largest areas in connection with criminal procedure where lawyers in Europe use AI are the use of algorithms for (legal) research and of algorithms for analysis and interpretation of trial relevant data.

Legal research tools are relatively sophisticated and are also affordable, especially those offered by legal publishers, who have included and embedded legal research tools in the databases they have been operating for the last few decades.

The use of algorithms for analysing trial relevant data, ranging from all kinds of digital data to physical documents or photos and witness statements is still developing. The two main problems which arise are that the data is gathered in various digital formats and the AI has to have the ability to identify the content of any evidence in any format. The more sophisticated algorithms which are able to do this are (at least at the moment) so expensive that they are out of the financial reach of most lawyers. This could create an inequality of arms between the more advanced capabilities which prosecutors may have at their disposal and the more limited resources lawyers may have. This places the defendant at a significant disadvantage.

4.8. USE OF AI IN RE-OFFENCE RISK ASSESSMENT

As described under 4.2, algorithms for predicting crimes are being used on a macro level by police forces on the one hand, and on the other hand, similar algorithms can be used on a micro level for predicting the probability of a person committing future offences. The police in Durham use an algorithm called Harm Assessment Risk Tool (HART) to divide offenders into three groups based on an assessment of whether the risk of the offender committing further offences within the next two years is low, moderate or high. Based on this assessment, the offenders forecasted as “Moderate Risk” – who are expected to offend, but not in a seriously violent manner – are admitted into “Checkpoint”, which is a programme to change the socio-cultural environment of these offenders, rather than putting them into jail.

The risks for such a use of AI are very similar to the risks described under 4.2. Because the methodology used to produce these assessments is usually not disclosed to the defendant, the defendant is unable to challenge the predictions made by the algorithms. Further, until it is possible to create AI which is free of bias, there is a risk that certain groups of individuals will be unfairly excluded from programmes from which they could otherwise benefit.

4.9. POSSIBLE PREDICTIONS CONCERNING THE USE OF AI IN THE CRIMINAL JUSTICE SECTOR

It is not likely that the development of complex algorithms used in the criminal justice sector will stop at this point. There are certain to be further advances and technological innovations which will contribute to an increased use of algorithms in all of these fields.

To see an example of how far the use of algorithms might reach in the future, one only needs to look at the experience in United States, where courts and correction departments use algorithms far more extensively than in Europe. The use of risk assessment tools in both pre-court and in-court processes is very common, with algorithms analysing the probability of someone showing up in court, machine learning controlling a convict’s home detention, automatic prison cell allocation based on the most compatible cellmates and many other tools all of which depend on algorithms.

In many instances, U.S. courts even let algorithms decide the sentencing of criminals. This is widely criticised because the offenders are not able to assess the operation of the algorithms. This lack of transparency is often due to the fact that private businesses write the algorithms; the government agencies only buy the systems, and often features are implemented in these systems that contain proprietary know-how of the developers which is subject to confidentiality obligations. As a result, only the developers and sometimes the purchasers have access to the decision process, but not the defence.

The Wisconsin Supreme Court, however, has ruled in the matter ***Loomis v. Wisconsin***, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017) that this limited insight into the result of the decision-making process is sufficient and that there is no requirement for further insight into the process. The case sought to challenge the State of Wisconsin's use of proprietary, closed-source risk assessment software in the sentencing of Eric Loomis to six years in prison. Loomis argued that using such predictive algorithms in sentencing violates the defendant's right to due process because it prevents the defendant from challenging the scientific validity and accuracy of such algorithms It was also alleged that the algorithm in question ("Correctional Offender Management Profiling for Alternative Sanctions" or COMPAS) violated due process rights by taking gender and race into account. Hearing this case would have given the US Supreme Court the opportunity to rule on whether it violates due process to sentence someone based on a risk-assessment algorithm whose workings are protected as a trade secret and thus not disclosed to the defendant. However, the US Supreme Court, to which the case was appealed, decided not to hear it, leaving the decision of the Wisconsin Supreme Court unchallenged.

Moreover, where there are no statutes that regulate the use of AI in criminal justice, this makes the processes even less transparent. In other instances, it is also an area of criticism that algorithmic decisions are often based on factors that seem racially or otherwise biased, for example, biases related to gender or the area in which the suspect lives Also, the reliability and accuracy of the algorithms are not guaranteed.

Some of these methods cannot yet be implemented in European jurisdictions due to statutes prohibiting such proceedings, and if they were to be implemented, it is likely that detailed regulations on the use of these features would be introduced concurrently. However, it cannot be ruled out that European countries will adapt to these changes and also expand their use of algorithm-based tools in their criminal justice systems.

4.10. CONCLUSION

Much debate is still needed to critically assess what role, if any, AI tools should play in our criminal justice systems. While preventing crimes from being committed, increasing the solving rate of crimes and improving the quality of criminal judgments are certainly goals which everyone will share, the risks of bias and discrimination against particular groups in our societies are high, and the threat of mass surveillance by AI systems poses a risk to open and pluralistic societies. Especially in the criminal justice system, fundamental rights and adherence to ethical standards are fundamental for preserving the rule of law. Therefore, AI systems should be introduced only when there are sufficient safeguards against any form of bias or discrimination. All measures of increased surveillance should be carefully balanced against the impact they may have on an open and pluralistic society.

5. Liability issues

5.1. INTRODUCTION

AI systems are increasingly coming into common use both as stand-alone systems – which can run-on general-purpose computers – and as part of more complex products. An example of the former is medical diagnosis software used to analyse CT scans for early signs of cancer and of the latter is self-driving vehicles.

It is likely that there inevitably will be errors and failures in the AI systems themselves or the more complex products and systems of which they form part. Such malfunctions may lead to either personal injury or economic loss. Such damage might arise from a programming error, but might, more likely, arise from the autonomous actions of the AI system itself. Further, even if there is no error or failure in the system itself, such products might be used in a dangerous way, giving rise to possible civil or criminal liability.

In any case, in order to protect users properly on the one hand, and to attempt to achieve some foreseeability for producers on the other hand, there is a need to make sure that a "responsibility gap" is avoided[22].

How should such issues be approached?

5.2. CIVIL LIABILITY

In approaching the question of the liability model for AI systems, some may be tempted to say that the law is already well-developed, especially regarding Product Liability as well as other liability regimes in force in the Member States, and all that is required in order to protect potential victims is to apply it. On the other hand, because AI is a new development, some may want to seek to reinvent the law of liability to deal with the issues it raises. In reality, a more nuanced approach, taking into consideration the new challenges brought by AI, may be called for. This approach should also consider the particular type of AI system concerned and the context in which it is likely to be used.

Plainly, a comprehensive analysis of all possible types of liability systems and issues which might arise lies outside the scope of this paper but some indications of the sorts of issues which might arise can still be given. For practical reasons this will be done particularly in light of the recently published report of the Expert Group on Liability and New Technologies set up by the European Commission[23] . It should be noted, however, that there is a large number of other studies[24] and policy documents[25] written in this regard that are also worth considering when analysing this subject in more detail.

If one looks to existing liability models, there are a few possible approaches to address the issue of civil liability in respect of AI[26]: 1) a liability system based on the concept of fault or 2) a strict liability system. Within these broad categories, there may be scope for differing approaches. For example, as regards the latter, the system could be either a pure strict liability regime - where there is liability whether or not there is a defect and where no defences

22 Nathalie Nevejans, Traité de droit et d'éthique de la robotique civile, 2017, p. 553 s.

23 European Commission: Report from the Expert Group on Liability and New Technologies – New Technologies Formation: Liability for Artificial Intelligence and other emerging digital technologies, December 2019.

24 Only to mention some studies, see, for example: Andrea Bertolini: Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules, (Law Innovation and Technology, 5(2), 2013, 214-247), 19 Mar 2014; Cédric Coulon: Du robot en droit de la responsabilité civile : à propos des dommages causés par les choses intelligentes, Responsabilité civile et assurances, étude 6, 2016; European Parliamentary Research Service: A common EU approach to liability rules and insurance for connected and autonomous vehicles, February 2018; European Parliamentary Research Service: Cost of non-Europe in robotics and artificial intelligence, June 2019.

25 As regards policy documents, see, for example: European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

26 See, for example, Herbert Zech: Liability for Autonomous Systems: Tackling Specific Risks of Modern IT (May 1, 2018). In: Sebastian Lohsse/Reiner Schulze/Dirk Staudenmayer (eds.): Liability for Artificial Intelligence and the Internet of Things, Nomos/Hart (2019).

to exclude or reduce liability are allowed - or a strict liability system which allows several defences, following the model of the Directive 85/374/EEC[27] (EU Product Liability Directive). Moreover, other liability regimes might be worth considering in the context of AI. For example, the report of the Expert Group mentions vicarious liability (liability arising from the actions of others) regarding autonomous technology. Furthermore, contractual liability or other compensation regimes could be applied in some digital ecosystems alongside or instead of tortious liability.[28]

Approaches seem to differ significantly as to the best regime to tackle this issue of liability in respect of AI. However, the most reasonable way, at least for the time being, might be that strict liability (with reconsidered defences and statutory exceptions) and liability based on fault should continue to coexist.

Regardless of the approach adopted, certain important changes will need to be made to EU and national liability regimes, considering issues such as the following:

First, the attribute of self-learning and autonomous decision-making in AI systems militates against the use of traditional legal reasoning based upon the concept of "foreseeability" as a basis of liability. In this context, an AI system may cause damage either as a result of a traditional "defect" for example in the software, but also as a consequence of its "own" actions determined by data and algorithms, without any "defect" in the traditional sense.[29] Thus, liability for damages cannot easily be attributed to "fault" on the part of a person (whether natural or legal) nor by the existence of a defect in a product, in the sense of a specific malfunction in that product. Under these conditions, one could say that liability for actions taken by an AI system should not necessarily be linked to the notion of fault (in its traditional sense) or a "defect" (in its traditional sense). It is noteworthy that the existing EU Product Liability Directive, although based on the existence of a "defect", defines "defect" not in the traditional sense, but in relation to outcome – i.e. "a product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account..." (Article 6(1)".

Second, there is the question of to whom liability might extend. That may be a challenging task given the opacity of AI systems and bearing in mind the multiplicity of persons potentially involved, possibly in multiple jurisdictions, and in the case of some persons, it may be without knowledge that their work would be subsequently utilised in an AI system. There are several possibilities of identifying different actors to whom liability could be attributed. For example, the Expert Group's recent report suggests: the *operator's* and the *producer's* strict liability; or the *operator's* and the *producer's* duties of care in case of fault liability.[30] The introduction of the notion of "operator" as the "person who is in control of the risk connected with the operation of AI and who benefits from its operation" is to be welcomed in this regard, with a distinction between frontend and backend operator. Such operators, as well as producers, would have to comply with specific duties of care, giving rise to liability in the event they failed to comply with such duties.

The defences which currently exist in strict liability systems, such as product liability, should then be reconsidered, particularly having regard to a defence relating to development risks.

Issues regarding the burden of proof also need to be reconsidered in the context of AI systems. Victims should be entitled to facilitation of proof in situations where the difficulties of proving the existence of an element of liability are disproportionate, going beyond what should reasonably be expected. In some cases, the reversal of the burden of proof may be appropriate, such as in the absence of logged information about the operation technology (logging by design) or failure to give the victim reasonable access to this information.[31]

Where several persons have cooperated in order to create an AI unit and the victim cannot prove which one of those persons has created the element leading to the damage, such facilitation rules should also be able to lead to a joint responsibility of these persons towards the victim. Redress claims between the tortfeasors should be possible.

Regarding damages, it seems to be necessary to regard not only physical and material damage but also the destruction of the victim's data as damage, compensable under specific conditions.[32] Those having a claim for damages may include consumers as well as professionals.

Finally, according to the Expert Group's report, compulsory liability insurance could be seen as a solution to give

27 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

28 European Commission: Report from the Expert Group on Liability and New Technologies – New Technologies Formation: Liability for Artificial Intelligence and other emerging digital technologies, December 2019, pp.36–37.

29 On this issue, see, for example: Jean-Sébastien Borghetti: How can artificial intelligence be defective? in Sebastian Lohsse/Reiner Schulze/Dirk Staudenmayer (eds.): Liability for Artificial Intelligence and the Internet of Things, Nomos/Hart (2019).

30 European Commission: Report from the Expert Group on Liability and New Technologies – New Technologies Formation: Liability for Artificial Intelligence and other emerging digital technologies, pp. 39-46.

31 Ibid, pp. 47-55.

32 Ibid, pp. 59-60.

victims better access to compensation in situations exposing third parties to an increased risk of harm and could also protect potential tortfeasors against the risk of liability.[33] When considering this possibility, there may also be broader issues of socio-economic policy to be taken into account. For instance, the perceived desirability of ensuring on the one hand that no-one who suffers loss through the operation of an AI system should go without compensation, set against concerns that there could be a chilling effect on innovation or unwanted interference in business to business relationships.

5.3. CRIMINAL RESPONSIBILITY

Although it is likely that most issues which will arise will be ones of civil liability, questions of criminal responsibility may not be altogether absent.

For example, the Law Commissions for England & Wales and for Scotland recently issued a Joint Consultation Paper on Self-Driving vehicles which, amongst other topics, discussed criminal responsibility in connection with the use of self-driving vehicles. In UK Road Traffic law, certain statutory obligations rest upon the owner or driver of a vehicle to ensure that the vehicle conforms to the relevant vehicle Construction and Use Regulations (such as ensuring that the tyres have sufficient tread depth and are properly inflated, that the brakes function properly etc.). This is done to make sure that the vehicles are not driven dangerously or without due care and attention, and that the driver does not have more than the maximum permitted limit of alcohol in his bloodstream.

AI systems in vehicles presently are merely driver aids, but what is the responsibility of the occupant of the vehicle sitting in the front seat when a vehicle comes to be on a public road, driving itself? In that situation, the occupant would not be regarded as a driver; but what would be the situation where, as is likely, the occupant may be called upon to take over control of the vehicle either in an emergency or if the vehicle ceases to be in its operating domain (such as a motorway)? In order to accommodate this, the Law Commissions suggested the creation of a new class of "user in charge" upon whom various duties would be imposed. However, what if the software is not kept updated, or the vehicle is under the emergency control of an operator situated in a control centre in India and who is drunk? Where does criminal responsibility lie?

This example of self-driving vehicles and the UK Law Commissions' suggested approach is given not to provide answers so much as to serve as an alert regarding the sort of issues which may arise in criminal law in relation AI systems and their operation.

5.4. CONCLUSION

There is no simple one size fits all solution to liability issues which might arise in relation to AI systems, not least because of the complexity of such systems and the diversity of contexts in which such issues might arise, as well also as decisions which may be come to be made as to the policy which the law should adopt. Rather, a balanced and nuanced approach tailored to the particular issue is likely to be called for.

33 Ibid, pp. 61-62.

6. The impact of AI on legal practice

6.1. INTRODUCTION

This part provides a general overview of how European lawyers may utilise tools that utilise some forms of AI. Only those tools will be discussed which are used by lawyers acting in their professional capacity.

The focus is mostly on tools that are or, in the near future, could be of practical interest to sole practitioners as well as smaller law firms.. However, it is not the intention to provide a practical list of accessible tools. First, the omission of any commercial products or brand names is intentional. Second, the objective is to give European lawyers some idea of what the future may look like with regard to AI tools and what areas can be expected to be changed by these tools. The intention is to give a wider overview of AI tools that could be of interest, even if those tools do not yet exist or are not yet practical, especially for lawyers working in markets of limited size.

This chapter starts with emphasising the importance for lawyers of one of the subfields within the typical research areas related to AI – natural language processing. Next, a generic, but important problem area is discussed in the field of AI: what makes it difficult for lawyers to apply AI in their practice? The next part seeks to cover the delivery of legal services and related practical fields of the use of AI in two slightly different, overlapping aspects – from the viewpoint of lawyers and from that of AI applications. The last two parts both address core aspects of the legal profession, namely the effect of the use of AI in legal practice on the ethics of the profession and the training of lawyers.

6.2. THE IMPORTANCE OF NATURAL LANGUAGE PROCESSING FOR LEGAL PRACTICES

A popular and well-known approach to the discussion of AI is to build on four possible characteristics along two dimensions: an Artificial Intelligence could be defined as a machine (a) thinking humanly, (b) thinking rationally, (c) acting humanly, or (d) acting rationally[34]. Based on the "acting humanly" definition, one of the key capabilities for the creation of a working AI tool is the ability of a computer to communicate with humans in the language of humans. That is why computer related work in the field of natural language processing has become one of the key subfields of AI related research. Nevertheless, natural language processing, or NLP for short, is an interdisciplinary field focusing on the objective of getting computers to perform useful tasks involving human language, and not necessarily by way of using machine learning algorithms. The most promising research and recent breakthroughs in natural language processing are all related to advances in the field of AI. Very important parts of the computer tools and models used in NLP are built on machine learning algorithms, and deep learning is one major driving force behind the current new wave of interest and new applications in NLP tools.[35]

For lawyers, natural language processing is important because all our work is related to human language, whether written or spoken. Therefore, for us, most of the advances in AI that may affect our work are likely to be related to NLP tools and new capabilities in the field of NLP.

6.3. GENERAL DIFFICULTIES IN THE USE OF AI IN LEGAL PRACTICES

The central problem for the use of machine learning in general for legal practices is the lack of analysable data in the possession of a law practice. Even if lawyers work with an ever-increasing amount of textual information, this information is mostly unstructured, sensitive and decentralised. Lawyers also have to be mindful that a considerable part of the information which they have to work with will probably never get into a structured,

34 Russel, Stuart and Norvig, Peter, *Artificial Intelligence: A Modern Approach.* Upper Saddle River, New Jersey: Prentice Hall, 2010, p. 2.
35 Deng, Li and Liu, Yang, [ed.]. 2018. *Deep Learning in Natural Language Processing.* Singapore: Springer, 2018. p. 7.

analysable form, whether that be for tactical reasons or otherwise.[36] As a result, **lots of effort is needed to turn this mass of data into features that machine learning can analyse and can gain experience from**.

At the same time, most of the law practices in Europe are sole practitioners and small firms, with either no infrastructure or, at any rate, **an infrastructure which is too small (i) to generate meaningful data about how the lawyer works or (ii) to capture important metadata about documents created by the lawyer**. Timesheets and data recorded for compliance with regulatory requirements (on case and file management) are the exception rather than the rule in the normal operations of a law practice.

Most small practices do not have the necessary resources to record data, and there are no universally accessible tools to do this. There is no European-wide or world-wide market for tools assisting lawyers. Rather, the relevant markets are specific to each of the 27 EU jurisdictions. Even lawyers speaking the same language have to use different tools if they come from different countries because the context of these legal tools differs vastly (for example. a lawyer from Germany may not use the case management software used in Austria, because the regulations applicable to the lawyer and the e-government solutions with which the lawyer interfaces are very different).

Another aspect of this problem is the l**ack of sufficient training data and models in natural language processing domains in general**. Even if researchers are able to achieve stunning advances in English and Chinese (so-called "rich") languages in NLP, this doesn't mean that any developer is able or willing to take the risk of marketing such advances in professional applications in the legal field. In the largest legal markets, the invisible hand of the market may steer developers toward this route, but in the very fragmented smaller legal markets, this is uncertain. Advances in NLP in rich languages may save a lot of time and effort for researchers in other (so-called "rare") languages, but that doesn't directly translate into advances in legal tools in such markets. As mentioned earlier, for legal use, separate models may have to be trained for different jurisdictions using the same languages as well.

Already, many law firms at the leading edge of the use of AI tools have learned through experience that some of the "innovative legal tech tools" heavily marketed in Europe as language-independent, turn out in practice to be unfit for commercial use in languages other than English. A number of contract analysis, due diligence tools and document assembly tools are sold as possessing "multilanguage" capabilities or being language agnostic. However, when the average sized European law firm actually tries to use these tools, this promise turns out to be only a reference to very generic functions accessible in the tools, which turn out to require disproportionate investment on behalf of the user. Such investment could consist of manual training by the user on a large dataset (that has to be gathered, prepared and cleaned by the user) for machine learning purposes. Or it could mean that a scripting type of programming language is accessible in the software based on which user would become responsible for developing (and maintaining) a language specific layer for its own specific "rare language." Scripting language is not necessarily easy to integrate with the tools already available in the given language. In both cases, so much individual investment is required by the user that law firms are better off not using the tool at all.

In many areas of application, **legal uses require so-called strong-sense interpretability[37] of the results a model provides**. That is because coming to conclusions based on machine learning algorithms is often useless in the legal domain unless humans can also explain the results, even if that might mean only explaining it to nationally available experts who may or may not be appointed by the court. This, as explained in previous chapters, is an essential requirement of the rule of law. Furthermore, most of the legal texts lawyers create and use professionally not only have to be convincing for other human actors (such as judges, experts or clients), but also have to rely on a specific set of arguments, including the citation of legislation or past cases.

Naturally, there are uses of AI in the legal sector where strongly interpretable results are not required, such as in retrieval of information from a large body of texts, or summarising texts or statistics on past decisions. However, the much-cited case of the COMPAS tool (used for analysing chances of recidivism) shows that even if the risk scores awarded were based on statistical evidence, many people consider the question of fairness or trust in such results from different perspectives.[38]

We also have to keep in mind that NLP tools trained in one domain tend to have a much worse accuracy when used in a different domain, which is exacerbated by the specific problems of legal specific language. This includes legal concepts using the same words as an ordinary language term, but having one or more very different meanings within different subfields of the same jurisdiction.

Last, one should not forget the joke "**ask 10 lawyers the same question, and you get 20 different answers**". If we suppose that this phenomenon is not the fault of the specific lawyers asked, but a natural product of the nature

36 Simshaw, Drew, Ethical Issues in Robo-Lawyering: The Need for Guidance on Developing and Using AI in the Practice of Law, 1, 2018, Vol. 70, p 187.

37 (Deng, et al., 2018 pp. 320-321). Weak-sense interpretability merely means the ability to draw insights from the already trained neural models that can provide indirect explanation of how the models perform the desired NLP tasks.

38 See also Chapter 4.2 and 4.6 above.

of legal problems and language of law in general, this characteristic of legal problems and legal texts also has a considerable effect on what we can expect from machine learning, how well can we train these tools, and in turn, limiting the areas where AI may be of use to lawyers.

6.4. MAIN CATEGORIES OF TOOLS

6.4.1. AI tools for legal use as seen by lawyers

Just as in many other aspects of our society, lawyers are also affected by the increase in the amount of data which is being generated. Court submissions become longer, case files contain a lot more information than 10 years ago, and even the amount and diversity of evidence available is increasing noticeably. Of all the new tools relying on AI and NLP, lawyers are mostly likely to gain from those tools that help them process a larger volume of data. This not only includes the ability to retrieve meaningful information from new files as fast as possible, but also the requirement by clients that a lawyer should take into account historical information, such as the content of an e-mail sent to the lawyer ten years ago. Even small law practices have to be organised and operated in a way that makes such retrieval possible and this has its own, considerable administrative costs.

One branch of information search used by lawyers to support their research is **analysis of legislation and of case-law and literature**. Analytical tools are often used for confirming or refuting arguments, but even for negotiations with other parties, for example, on what the "usual amount awarded" in similar cases may be.

Another very promising area is what is usually described as **e-discovery solutions, i.e. automated identification of relevant documents, and technology assisted review** (as also discussed in section 4.4). The term "e-discovery" is often used even in European countries, although there is no discovery procedure in place similar to that in civil procedure in England and Wales and certain other common law jurisdictions. Due to liability rules and obligations on the custodian side, considerable investment has already been made in automated identification of relevant documents and, more importantly for lawyers, in technology assisted review. For defence counsel, the availability of such technology assisted review tools at the courts is becoming critically important, even in smaller countries. Without such tools, defence counsel are unable effectively to carry out their work in face of the ever-increasing volumes of evidence that are generally collected in the investigation phase of a criminal case (such as electronic evidence from computer systems etc.). Additionally, the short timeframe available to defence counsel for preparing their case also hinders their ability to effectively carry out their work without these tools. Such review tools are useful in non-criminal cases as well, including in pre-trial research on the documents and evidence available from the client.

The process of carrying out **due diligence of contracts and documents, and compliance reviews** is another major area where the increased ability to find information is, even now, causing great changes. Considering that most of the due diligence work by external parties is currently carried out in virtual data rooms, for such parties it is also important to be able to use these document analysis tools in the virtual data rooms provided.

Besides information retrieval tools, there are also AI applications facilitating the creation by lawyers of more consistent legal documents in a shorter timeframe by means of **document automation**. Even if some lawyers have been using document automation for almost 30 years now, the natural language generation capabilities of AI tools may take the possibilities of document automation to a new level. Currently, document automation tools require the tedious manual work of annotating precedents to create a model for automation. Considerable automation specific expertise is needed for such authoring, including knowledge of a special scripting language, or the involvement of developers in solving integration issues in relation to other tools used in the legal practice. However, authoring in document automation should rather be an exercise for the legal domain experts. Also, these tools should make it possible for lawyers to express legal requirements at a more abstract level than the level of a document (or a specific template of a contract) because that is the only way to ensure consistency of clauses across different templates and many areas of law where a firm provides advice.

The conflicting requirement of a greater abstraction and easier authoring can be resolved only by the reliable use of natural language processing tools for language understanding and generation.

Besides having more consistent documents available faster, document automation also confers other strategic advantages on law practices. Previously unstructured data may be enriched with structured data, making it a lot easier and more reliable for computers to work with (see the problem of having no structured data in the previous section), and such tools also help law firms to capture the knowledge of individual lawyers. Such knowledge is mainly captured when lawyers create or update templates and when a lawyer answers a questionnaire or interview for a specific case. This is because the answer is also recorded alongside the document which is created. It is also more natural for lawyers to record knowledge (explanations or reasons) during the authoring process, then separately creating notes for later use.

AI based tools can change many facets of how a legal practice works and all aspects of the delivery of legal advice. This includes from the way that clients find and connect with lawyers, through the way legal research and internal preparations are carried out, up to how a lawyer delivers advice and provides the service to the client. Even what is seen in some jurisdictions as a possibly grey border between what constitutes legal advice and what does not, could be challenged by the use of AI applications.

6.4.2. AI tools for legal use as seen from the aspect of AI applications

Computer and data scientists have their own literature on AI tools with their own categories. It is worth mentioning those categories of the "AI literature" that will most probably provide useful help for lawyers in the future. Some categories do not need any explanation, but for reasons of correct terminology, it is still useful to mention them.[39]

A trivial category is **speech recognition**. This is already a much-used substitute for elderly lawyers who are used to rely on dictation and not on typing their own text on keyboards, or for lawyers who are on the move and are unable to use keyboards for some reason (making use of time between court hearings, during driving etc.) This is one of the areas where tools using deep learning models have already made a difference in rare languages as well.

Another area where deep learning has made wondrous advances **is machine translation**. Even if translation is not a legal type of work per se, lawyers may spend many hours of lawyers on such tasks, and many hours of less experienced translators can be saved for first drafts, even in less common languages.

In other areas of NLP processing of texts, **deep learning** has so far not made spectacular advances. Nevertheless, lawyers could still make good use of different information retrieval and extraction solutions from the field of NLP, provided that lawyers have access to professional grade tools, and not only research level tools. Currently, even the most mundane word processors that lawyers use have built-in "regular expression" search capabilities,[40] but, because these capabilities are difficult to use, most lawyers do not even know about this possibility.

Similarly, **part-of-speech (POS)** tagging can also be helpful to lawyers in providing an over-view of documents at a different level of search: for example, by highlighting all the references to "lease" used as a noun, but not as a verb. If, in a large set of forty documents, the lawyer wants to get a good overview of the obligations of a "supplier", the lawyer could use "dependency parsing" tools and retrieve only those sentences or paragraphs where the subject of the sentence is the supplier. Similarly, the techniques for **Named Entity Recognition** can be useful for such searches, where software can review and tag all the sentences of a large document set and show an overview to the lawyer of the organisations, persons or locations in the document set, without the lawyer having to read any of it. Similar search capabilities are present for time relations, called "temporal expression recognition" (for example, to search through all contracts and find the payment date or the required period of notice of termination or highlight deadlines for court documents), or for event detection (such as including a calendar entry if the court document mentions a new hearing).

Although mention has been made of language generation as an important subfield of NLP for lawyers in relation to document automation, **automation solutions available for smaller firms currently make use of machine learning tools only in very limited circumstances**. This is done by changing the declination of a noun or a conjugation of a verb of a more abstract clause to fit into a specific document, such as with multiple lessors, lessees or subjects of lease in a document, where the original clause was in the singular, and correctly changing word endings in agglutinating languages. In order to enable higher level abstraction of documents and templates, document automation tools have to rely on a specific language layer of NLP tools.

6.5. ETHICAL ASPECTS CONCERNING THE USE OF AI IN LEGAL PRACTICE

The practice of the profession of lawyer must always be based on respect for ethical principles. This is a precondition for lawyers to maintain their important role in civil society.

The increasing spread of AI systems within law firms requires a discussion on the ethical principles that should govern their use. First of all, it is necessary to verify whether the current ethical rules are sufficient to allow the correct use of AI tools in the legal profession. If this is not the case, there should be an examination of whether the existing rules could be used at least as a basis in light of which new rules might further be elaborated, or whether completely new rules should be established.

39 See Indurkhya, Nitin and Damerau, Fred J., [ed.], Handbook of Natural Language Processing' 2nd Boca Raton, CRC Press, 2010, pp. 168, 169..

40 Regular expression is a 50 year-old search technique (that is not relying on AI) based on search patterns. E.g. retrieve all the references in the document in the format of one to four numbers ending with ". §" or ".§" (a typical Hungarian reference to a provision in a piece of law) would look like "[0-9]{1,4}.\s?§". You can use similar lookups in Microsoft Word "search with wildcards", but lawyers very rarely use it.

The emergence of technology in law firms has already led to discussions on the need to adapt ethical rules to the new tools available to lawyers: on this subject, the CCBE has prepared a number of documents in order to make lawyers who are using electronic tools aware of the risks associated with them. In particular, reference is made to the guidelines on the use of electronic communications (CCBE Guidelines on electronic communication and the internet), on the use of the cloud (CCBE Guidelines on the use of cloud computing services by lawyers) and on the use of online legal platforms (CCBE Guide on lawyers' use of online legal platforms). All of these guidelines emphasise the need for lawyers to make conscious and responsible use of new technologies in order to carry out their activities in the best possible way, protecting the relationship of trust between the lawyer and the client and compliance with applicable regulations. Moreover, a new sentence has recently been added to the commentary on Principle G) of the CCBE Charter of Core Principles of the European Legal Profession, which addresses the lawyer's professional competence.

From these points of view, the most obvious principles in the use of AI tools concern: the duty of competence, the duty to inform the client while maintaining lawyers' independence in terms of defence and advice, and the duty to preserve professional secrecy/legal professional privilege as well as the obligation to protect the confidentiality of clients' data.

6.5.1. The duty of competence

The duty of competence refers to the lawyer's obligation always to be up to date with the rules in force and the relevant case law. In addition, lawyers should be aware of and adopt, to a reasonable extent, different tools that allow them better to meet their clients' needs. This may include, for example, better organisation of the law firm or the adoption of AI tools.

When adopting different AI tools, this duty of competence does not mean that lawyers should become computer engineers, nor it is required that they should understand how a tool works at an algorithmic level. However, if they intend to employ tools that use AI (such as those that suggest answers to legal questions), it will be necessary to understand broadly how these tools work and what their limitations are, while considering the risks and benefits that they can bring to the specific case on which the lawyer is working. This necessity is also highlighted in the recently amended commentary on Principle G of the CCBE Charter, as mentioned above, stating that a lawyer should be aware of the benefits and risks of using relevant technologies in his or her practice.

The duty of competence should therefore entail not only the need to use reliable providers, but also the ability to request and understand the information on the basic characteristics of the program. Perhaps the information to be requested could include ways to verify its compliance with the five principles of the European Ethical Charter on the Use of AI in Judicial Systems developed by the CEPEJ[41]. Moreover, it is important for lawyers to be aware of the limitations of the program in question. For instance, it may be impossible to include in the program certain data that could be relevant in resolving of the case

Competence also means not simply accepting the results produced by the software, or rather by machine learning, but verifying those results using one's own knowledge. Lawyers are required to verify and check and take responsibility for the results of research which may have been carried out for them by others such as trainees or other lawyers who are involved in the examination of the case, and will also have to take responsibility for any advice which he or she may give on the basis of that research. Likewise, where the advice given to the client depends on research carried out by an AI tool, the lawyer will require to verify the results achieved by the AI tool. The results produced by AI systems, although useful, are not infallible and often also depend on the quality of the information which they process and on any bias which may be reflected in the algorithms used. For this reason, it is necessary to verify the results carefully, bearing in mind that not everything can or should be done by AI.

Finally, for the proper development of AI tools in the legal field, it is important that lawyers are also involved in the design process. Their contribution is certainly necessary for the proper development of programs designed to solve legal problems, which cannot be exclusively entrusted to technicians who know how the algorithms work but do not have the necessary legal knowledge. It will therefore be important for lawyers to acquire specific skills in this field.

41 See the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment as adopted by the CEPEJ during its plenary assembly on 3 - 4 December 2018, pp. 7-12.

6.5.2. The duty to preserve professional secrecy/ legal professional privilege and the obligation to protect the confidentiality of clients' data

The overriding obligation of professional secrecy/legal professional privilege must be ensured when using AI tools. This means that communications between lawyers and their clients are kept confidential: there can be no trust without the certainty of confidentiality. As stressed in the CCBE Charter, this principle can be seen as having a dual nature - observing confidentiality is not only the lawyer's duty, it is a fundamental human right of the client.

Confidentiality, in particular when it comes to new technologies, is at the heart of the ethical obligations of lawyers, who are not allowed to disclose information about the representation of their client unless expressly authorised by the client on the basis of informed consent. It may also be that, in certain cases, the need to respect professional secrecy/legal professional privilege might be a reason why an AI tool cannot be used.

The obligation to protect the confidentiality of the client's data has been supplemented by the GDPR, which includes strong security obligations in the protection and retention of that data. Lawyers are required to take the utmost care to observe these obligations in order to avoid the loss or unauthorised disclosure of data (even where this might be unintentional).

In this respect, the use of AI systems within law firms entails even more stringent obligations regarding the new ways in which data is collected, used, linked to the data of others and stored.

When a lawyer chooses to store data in the cloud with third parties, there is still the ability for lawyers to store clients' information that they consider particularly sensitive only at the office and in paper form. On the other hand, AI tools must be able to be implemented with all the data available to the lawyer in order to work properly and meet the needs of increasing accuracy.

Lawyers may need to obtain the clients' informed and explicit consent to the processing and use of their data, in particular sensitive data, in order to implement AI tools; lawyers may be required to prove that they have chosen programs that satisfy the principles of the protection of personal data (privacy by design). They have to be able to inform the client of any and all relevant aspects, including, for example, the possibility of not deleting the data once put into the system.

The client should be free to decide whether or not to allow the lawyer to rely on certain AI systems in dealing with his or her case.

6.6. TRAINING OF LAWYERS AND AI

The new landscape which we are facing and the consequent need to acquire specific skills related to AI is the next great challenge. This constant evolution and the fact that there are many (internal and external) fields involved lead to a situation where lawyers should urgently embrace a life-long training mindset while acknowledging the related investments and resources needed (financial, human resources, time etc.).

With the rise of AI and the arrival of legal tech, legal practice has become increasingly complex due to novel legal issues being raised by AI and the development of highly sophisticated digital tools which lawyers need to master and understand. The impact of AI on the training of lawyers is not limited to the technological skills needed. It is very important also to develop the relevant soft skills and tactical performance, as well as the advanced capacity better to understand the needs of clients. Therefore, training should be used to extend lawyers' general competence in understanding the technological environment that they are likely to be working in, while keeping focus on the principles related to lawyers' ethics and human rights.

Law firms and lawyers are under increasing pressure from growing demands from clients for faster, cheaper and more targeted legal services. In order to remain competitive, the potential and obvious advantages as well as the opportunities of AI must be understood. A professional culture should include a high-level cognitive understanding of AI which would enhance lawyers' critical thinking and creativity, as well as their ability to focus on important and complex matters.

It would be desirable to adopt training programmes and offer training courses which could provide both practical and theoretical knowledge and skills. This would allow lawyers to understand and be able to use the legal technology, including AI, blockchain, smart contracts, big data, online dispute resolution (ODR) tools, automation etc. Such training will enable lawyers to provide legal assistance to a new type of client who might become involved in legal issues (such as liability) in relation to creating, selling or using technological tools.

AI tools should be used to create new ways of delivering training and developing training methodology, significantly improving the learning experience and accelerating the learning process by removing various minor obstacles. This could also improve the quality of the learning experience by using specific algorithms based on a combination of machine learning, deep learning (in due course) and natural language processing. Such teaching

tools could include those that can process users' questions and answers in real time, offering reasoning, advice and clarification. It might encourage the creation of new teaching materials and methods such as integrating AI in adapted and individualised learning needs. Exchange of experience and information on the best relevant training methods for lawyers should accordingly be promoted between the Bars and Law Societies.

Lawyers could also participate in the creation and implementation of AI tools for the profession. Their involvement could improve the design of machine learning tools through working with other professions and stakeholders in the sector. This could lead to new training needs and new opportunities for lawyers.

Such ideas could be assisted by the setting up of IT/AI law laboratories or workshops in law schools. Such laboratories/workshops could also acquire a European dimension by attracting collaborative researchers and innovation professionals, and ensuring cross-border sharing of experience. These laboratories/ workshops might also be eligible for EU funding. Developments in AI could possibly lead to the creation of new specialisations for lawyers, or even the emergence of new professions.

6.7. CONCLUSION

AI tools can thoroughly change many aspects of how legal services are offered and delivered to clients, as well as changing the inner workings of law practices. Even the question of what constitutes legal advice is changed by some AI applications. Although AI does not change the core values of the legal profession, such as the importance of confidentiality, it does make important changes necessary in the way in which legal practices operate. To stay competent and to be able to uphold the rule of law in the interests of their clients, lawyers have to be competent enough to ask meaningful questions about the decisions made by AI systems – and lawyers have to be taught how to do this. Lawyers will always have a very different skill set and approach from data scientists. Nevertheless, understanding and pointing out the limits of applicability and utility of AI systems cannot remain in a purely technical domain. Just as the rule of law requires that judges understand the most important aspects of these decision-making systems, so, too, do lawyers have to support their clients in explaining these workings to the courts.

Overall conclusion

With the great opportunities and benefits offered by AI also comes a great responsibility to ensure that AI remains ethical and respects human rights.

The use of AI does, in certain aspects, pose significant threats to the quality of our justice systems, the protection of fundamental rights and the rule of law. These threats are especially acute when we consider the possible future role of AI based decision making tools in the field of justice and law enforcement. Fundamental rights that underpin the rule of law cannot be subordinated to mere efficiency gains or cost saving benefits, whether for court users or judicial authorities. In order to manage this change effectively, concrete principles and rules must be established, and at the same time, a proper place and role for AI systems has to be identified in such judicial fields.

Transparency, fairness, accountability and ethical rules should be areas of distinct focus. For AI systems to be used as an integral element in a democratic society, it is not sufficient merely to rely on trust in the expertise of technical specialists operating in the field of computer systems. New bridges of trust have to be built amongst the domain specialists, those working in our democratic institutions, and those who are engaged in all areas where the rule of law is engaged. Such integration has to take into account the specific expertise and roles of actors and specialists across different sectors and professions. Transparency and applicability will not be achieved by merely obliging providers of AI services to acquire new certificates, approvals and trust marks supporting compliance with a list of ethical principles.

In line with these requirements, the use of AI in criminal proceedings transforms what is expected from defence counsel, including the expectation that counsel will be able to analyse and interpret data relevant to the trial. Also, clients who are the subject of criminal proceedings should expect that their defence counsel will be able to identify major recurring sources of bias in AI based analyses, and be able to explain this to the judges involved.

Another complex issue is the issue of civil law liability in relation to AI systems. This is not something that can be answered by simply choosing between a fault-based and a strict liability system or by applying a product liability system linked to indemnity insurance. Rather, a balanced and nuanced approach tailored to the particular issue is likely to be called for.

A society has to be confident that AI tools function correctly. The aim here should be to harness the benefits of AI in order to deliver greater access to justice in our systems, while simultaneously mitigating and reducing the dangers and risks associated with this change.

As for lawyers, if they intend to employ tools that use AI when providing legal services, it will be necessary to understand how these tools work and what their limitations are, while considering the risks and benefits that they can bring to the specific case. Training should therefore be used to extend lawyers' general competence to understand the technological environment in which they are likely to be working, while keeping focus on the principles of lawyers' ethics and human rights.

The message which may be taken from this paper is that there is a clear need for the CCBE and its membership to continue monitoring the impact of the use of AI in the legal and justice area. Given lawyers' dual role, on the one hand with their active role in the judicial system and, on the other, as legal service providers, they have a unique role to play when it comes to the further development and deployment of AI tools, especially in those areas where access to justice and due process are at stake.

Therefore, and also taking into account the upcoming policy developments on AI at the EU and Council of Europe level, the CCBE may wish further to articulate its views on aspects of the use of AI on the basis of further studies and reflections by its respective committees and working groups.

Bibliography

- Bertolini Andrea: Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules, (Law Innovation and Technology, 5(2), 2013, 214-247), 19 Mar 2014.
- Borghetti Jean-Sébastien: How can artificial intelligence be defective? in Sebastian Lohsse/Reiner Schulze/Dirk Staudenmayer (eds.): Liability for Artificial Intelligence and the Internet of Things, Nomos/Hart (2019).
- Commission Communication - Investing in a smart, innovative and sustainable Industry – A renewed EU Industrial Policy Strategy, 13 September 2018.
- Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, 25 April 2018.
- Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Coordinated Plan on Artificial Intelligence, 7 December 2018.
- Conclusions adopted by the European Council at its meeting on 19 October 2017, 19 October 2017.
- Conclusions adopted by the European Council inviting the Commission to work with Member States on a coordinated plan on Artificial Intelligence, building on its recent communication, 28 June 2018.
- Conclusions adopted by the European Council underlining the need for the Single Market to evolve so that it fully embraces the digital transformation, including Artificial, 13-14 December 2018.
- Council conclusions on an EU industrial policy strategy for competitiveness, growth and innovation, 12 March 2018.
- Council conclusions on the coordinated plan on the development and use of artificial intelligence made in Europe, 11 February 2019.
- Council of Europe, Commissioner for Human Rights: Unboxing Artificial Intelligence: 10 steps to protect Human Rights
- Council of Europe European Commission for the Efficiency of Justice, European ethical Charter on the use of AI in judicial systems and their environment, December 2018.
- Coulon Cédric: Du robot en droit de la responsabilité civile : à propos des dommages causés par les choses intelligentes, Responsabilité civile et assurances, étude 6, 2016.
- Deng, Li and Yang Liu, Deep Learning in Natural Language Processing, Springer, 2018.
- EPRS Study on Understanding algorithmic decision-making: Opportunities and challenges, March 2019.
- European Commission (EC), Commission Staff Working Document Evaluation of Directive 96/9/EC on the legal protection of databases, 2018.
- European Commission (EC), Commission Staff Working Document Guidance on sharing private sector data in the European data economy Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions “Towards a common European data space”, 2018.
- European Commission (EC), Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (recast), 2018.

- European Commission, Report from the Expert Group on Liability and New Technologies – New Technologies Formation: Liability for Artificial Intelligence and other emerging digital technologies, December 2019.
- European Commission Rolling Plan for ICT Standardisation, which identifies ICT standardisation activities in support of EU policies, 20 March 2019.
- European Data Protection Supervisor (EDPS), Towards a Digital Ethics, Report from EDPS Ethics Advisory Group, 2018
- European Group on Ethics (EGE), "Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems. European Group on Ethics in Science and New Technologies", March 2018.
- European Parliamentary Research Service, Scientific Foresight Unit, A governance framework for algorithmic accountability and transparency, April 2019
- European Parliamentary Research Service, A common EU approach to liability rules and insurance for connected and autonomous vehicles, February 2018
- European Parliamentary Research Service, Cost of non-Europe in robotics and artificial intelligence, June 2019.
- European Parliamentary Research Service, Artificial Intelligence ante portas: Legal & Ethical Reflections, March 2019.
- European Parliamentary Research Service, How Artificial intelligence works, March 2019.
- European Parliamentary Research Service, EU guidelines on ethics in artificial intelligence: Context and implementation, 19 September 2019.
- European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 16 February 2017.
- FRA Focus: Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights, June 2019.
- FRA Focus: Facial recognition technology: fundamental rights considerations in the context of law enforcement, November 2019.
- High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for trustworthy AI, 8 April 2019.
- Indurkhya, Nitin and Fred J. Damerau, Handbook of Natural Language Processing, CRC Press, 2010.
- Jurafsky, Daniel and James H. Martin, Speech and Language Processing, 23 September 2018.
- Lohsse Sebastian, Schulze Reiner, Staudenmayer Dirk (eds.): Liability for Artificial Intelligence and the Internet of Things, Nomos/Hart (2019).
- O'Neil, Cathy, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, 2016.
- Russel, Stuart and Peter Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall, 2010.
- Simshaw, Drew, Ethical Issues in Robo-Lawyering: The Need for Guidance on Developing and Using AI in the Practice of Law. 1, Vol. 70., 2018.
- Zech Herbert: Liability for Autonomous Systems: Tackling Specific Risks of Modern IT (May 1, 2018).