

## Regulating (Artificial) Intelligence in Justice: How Normative Frameworks Protect Citizens from the Risks Related to AI Use in the Judiciary

Lupo, Giampiero

Veröffentlichungsversion / Published Version

Zeitschriftenartikel / journal article

### Empfohlene Zitierung / Suggested Citation:

Lupo, G. (2019). Regulating (Artificial) Intelligence in Justice: How Normative Frameworks Protect Citizens from the Risks Related to AI Use in the Judiciary. *European Quarterly of Political Attitudes and Mentalities*, 8(2), 75-96. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-62463-8>

### Nutzungsbedingungen:

Dieser Text wird unter einer CC BY-NC-ND Lizenz (Namensnennung-Nicht-kommerziell-Keine Bearbeitung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:

<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>

### Terms of use:

This document is made available under a CC BY-NC-ND Licence (Attribution-Non Commercial-NoDerivatives). For more information see:

<https://creativecommons.org/licenses/by-nc-nd/4.0>

## Regulating (Artificial) Intelligence in Justice: How Normative Frameworks Protect Citizens from the Risks Related to AI Use in the Judiciary

**Giampiero Lupo**

Research Institute for Justice Studies  
National Research Council  
Italy

*Date of submission: April 11<sup>th</sup>, 2019*

*Date of acceptance: April 23<sup>rd</sup>, 2019*

### Abstract

Recently there has been a growing diffusion of tools based on AI technology supporting justice professionals. Artificial Intelligence algorithms are starting to support lawyers for instance through artificial intelligence search tools, or to support justice administrations with predictive technologies and business analytics based on the computation of Big Data. The introduction of AI tools in the justice sector poses several implications as for instance (1) the availability of data coming from courts and proceedings and issues in terms of protection of privacy or (2) the use of predictive technologies and issues regarding data protection, discrimination biases and transparency. Private and public actors are growingly dealing with the risks related to the use of AI by developing normative frameworks that discipline AI application in several contexts. However, most of the normative frameworks are not binding and only deal with some of the many concerns related to the impact of AI in justice. The paper has two objectives: first to analyse the main challenges related to the use of AI both by lawyers and by the justice administrations through some examples of AI tools recently developed; second, to assess a selection of the most important frameworks disciplining the application of AI in several contexts developed by different types of actors from international forum to private companies or national and EU parliaments. The analysis acknowledges the several risks related to the use of AI in justice; moreover, it draws the attention to the lack of comprehensive and binding normative frameworks regulating AI.

**Keywords:** AI and justice; justice values; ICT development; normative frameworks.



This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Corresponding Author: Giampiero Lupo, Ph.D., Researcher  
Affiliation: Research Institute on Judicial Systems, National Research Council, Italy  
Address: Via Zamboni 26, Bologna – 40126, Italy  
e-mail: [giampiero.lupo@irsig.cnr.it](mailto:giampiero.lupo@irsig.cnr.it)

Copyright © 2019, Giampiero Lupo  
European Quarterly of Political Attitudes and Mentalities - EQPAM, Volume 8, No.2, April 2019, pp.75-96.

ISSN 2285 – 4916  
ISSN-L 2285 – 4916

## 1. Introduction

In the last years, there has been a growing interest in the technological development of Artificial Intelligence (AI) and on its potential and effective application for the development of tools supporting justice professionals' work. Artificial intelligence involves all types of technologies characterized by a machine mimicking "cognitive" functions associated with human mind, such as "learning", "problem solving", "natural language processing", etc. (Russell and Norvig, 2016).

Artificial intelligence is applied in several fields, such as autonomous vehicles (drones, self-driving cars, etc.) or medical diagnosis. In the justice sector, there is a growing utilization of Artificial Intelligence (AI) algorithms for applications supporting justice professionals' work. The application of AI for supporting justice professionals is not a true innovation given that the first experiments with AI and law date back to 80s (Rissland et al., 2005). As of today however, AI tools are more and more diffusing both in the free market of ICT for lawyers and in some justice systems and are beginning to have a more relevant role in professionals everyday activities. Most of these applications are developed for lawyers (Lupo, 2018). As an example, "Ross", an artificial intelligence search tool, is utilized in law firms for supporting online legal search (of sentences and laws) through keywords. Despite most of the existing applications based on AI are utilized by lawyers, some applications are beginning to be introduced (or at least explored) by the justice administrations. I refer in particular to predictive technologies and business analytics based on the computation of large amount of data (Big Data). For example, "COMPAS", a risk assessment tool, is used in the U.S. by the Wisconsin Department of Corrections to determine if an offender has a high or low risk of recidivism (Skeem and Loudon, 2007).

The introduction of AI technologies into the justice systems may entail several implications both for justice professionals and for the citizens affected by the procedure. These implications regard for instance the use of data, the protection of privacy, the responsibility and accountability of systems and their reliability. On the one hand, these may be just practical implications as the reliability of systems and the responsibility of designers; on the other hand, the introduction of AI may also affect fundamental human rights principles and rule of law. While concerns are apparently similar to the ones posed by previews e-Justice experiences (Contini and Fabri, 2003; Velicogna, 2007; Reiling 2009; Contini and Lanzara, 2009; Velicogna, 2018), the effects of the changes introduced by AI have the potential of being much deeper and less controllable.

The potential consequences of the use of AI represent a considerable concern, and a number of different actors are attempting to develop normative frameworks in order to discipline its use. These frameworks try to set principles or guidelines with the aim of protecting fundamental rights and values from harms that AI technology may cause. Given the profound entanglements between technology in justice and normative regimes (Contini and Mohr, 2008), this paper analyses how normative frameworks can discipline the application of AI in several contexts and in particular in the judicial context. The aim is on the one hand, to understand which are the main risks related to the use of AI in the justice systems, on the other hand, to assess if frameworks are adequately safeguarding citizens, users and professionals from these risks.

In order to pursue these objectives, the paper first focuses on the analysis of a representative selection of e-justice services based on Artificial Intelligence technology (*Section 2*). The analysis takes into account both AI tools utilized by lawyers and AI applications developed for or used by the justice administrations.<sup>1</sup> The investigation of AI tools for justice is only descriptive and for reasons of opportunity

---

<sup>1</sup> Some AI systems have been developed in order to provide self-help tools to self-represented litigants (Simshaw, 2018). For reasons of space, the analysis of these tools is out of the scope of this paper.

and space, does not take into account systems' development and functioning. Successively, the paper focuses on the main ethical and practical implications of the use of AI by justice professionals basing the discussion on the existing literature (section 3). Section 4 analyses a selection of the most important frameworks disciplining the application of AI in several contexts developed by different types of actors, from international forum to private companies or national and EU parliaments. The analysis pursues two objectives: first, to acknowledge if the frameworks analysed "cover" the implications regarding the use of AI in the judiciary discussed in section 3; second, if frameworks "suggest" other potential risks related to AI applied in justice, previously ignored by the literature. A "concluding remarks" section discusses the results of the analysis.

Before introducing the analysis of the AI systems for justice in the next section, it is opportune to describe the method of analysis. With reference to the analysis of AI systems for justice (section 2), I utilized a case study method of analysis. This investigation approach is effective for the study of large scale ICT phenomena in the area of justice (Rosa, Teixeira and Pinto, 2013; Velicogna, 2007a). Moreover, the use of case study approach is useful when researcher has little control over events, and when the focus is on a contemporary phenomenon within some real-life contexts (Yin, 2003). Due to the entanglements between, law, justice systems' organization and technology (Contini and Mohr, 2008) that characterize e-justice systems (also based on AI), the case study approach here applied is interdisciplinary. This allows looking at systems not only from a technological perspective, but also with the eyes of organizational and law studies. As far as the description of the main implications of the use of AI in justice is concerned, this has been pursued by inventorying the main literature on the topic and by focusing on the main official documentation as the ENCJ Judicial Ethics Report (ENCJ, 2013). Finally, the method of analysis of the framework documents disciplining the use of AI, is the qualitative content analysis. For reasons of opportunity and space, the qualitative content analysis applied here does not bring to a quantitative analysis of documents' content, as it is typical of content analysis (Riff et al., 2006; Rourke and Anderson, 2004). The quantitative analysis of documents' content is out of the scope of this paper given that the main aim of the investigation activity is evidencing the main principles and risks deriving from the application of AI in justice described in the framework documents selected.

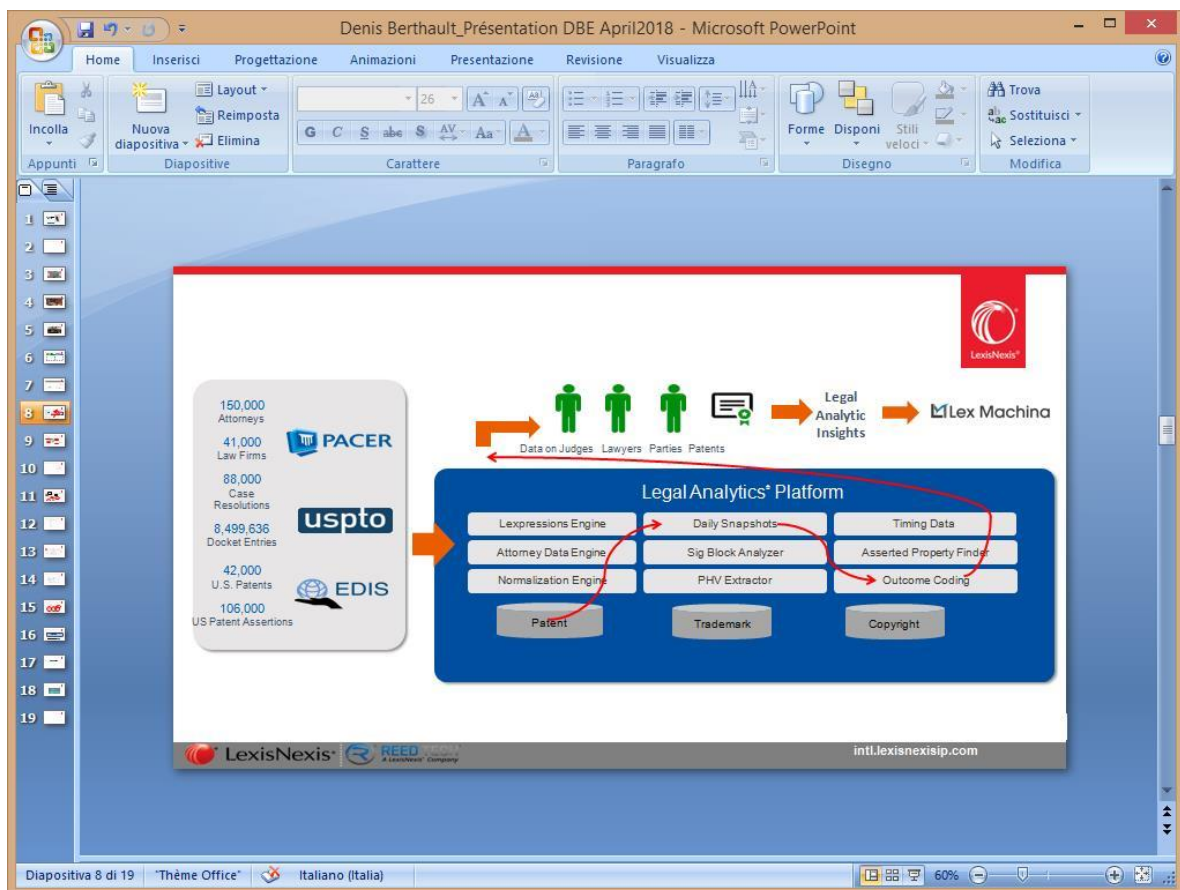
## 2. Artificial Intelligence for JUSTICE

The first experiments of the use of Artificial Intelligence in justice systems date back to the '80s. Most of the tools developed were dedicated to lawyers. For instance, one of the first systems developed, HYPO, was a tool for modelling cases' argumentation in the field of US Trade Secrets Law (Simshaw, 2018; Skeem and Loudon, 2007). The project was developed by Rissland and Ashley with the objective of creating a tool for adversarial argument as a three ply structure and for executing the key tasks performed by lawyers when analysing case law for precedence.

After eighties, the first pilot projects as HYPO or CABARET (Rissland et al. 2003) started to develop real AI tools that could be sold in the free market and effectively utilized by lawyers (Simshaw, 2018). Moreover, AI technologies started to cover different types of requirements and functionalities: not only expert systems as the ones developed in the early experiments with AI and justice, but also document review and outcome prediction systems (Bench-Capon, 1997).

Expert systems are indeed the first typologies of systems developed since the 80s as pilot projects for testing the introduction of AI for legal professionals (Rissland et al. 2003). Called also Case-Based Reasoning (CBR), they are designed to function as assistants in the process of legal problem solving by providing intelligent research tools for case-law and norms related to the case at hands (Suskind, 1987).

CBR can put in evidence which past cases can be helpful to a lawyer's case. One of the best examples of recently developed expert systems is **ROSS**. Ross Intelligence (<https://rossintelligence.com/>) is a legal research engine that utilizes artificial intelligence to automate activities, as legal search that usually involves lawyers and law firms. The system incorporates the IBM's Watson technology and allows users to ask natural language questions, and to search and provide legal information ranging from specific citations to full legal briefs. ROSS semantics allows users to search not only through keywords, but also through similar concepts. Moreover, the system tracks the evolution of case-law and in case of relevant legal updates, ROSS automatically sends notifications. Ross technology focuses on the following matters: 1. Consumer Protection; 2. Personal Bankruptcy; 3 Debts restructuring; 4 Insolvency; 5 Litigation, including defending against lender liability actions, fraudulent conveyance claims and challenges to acquisitions.

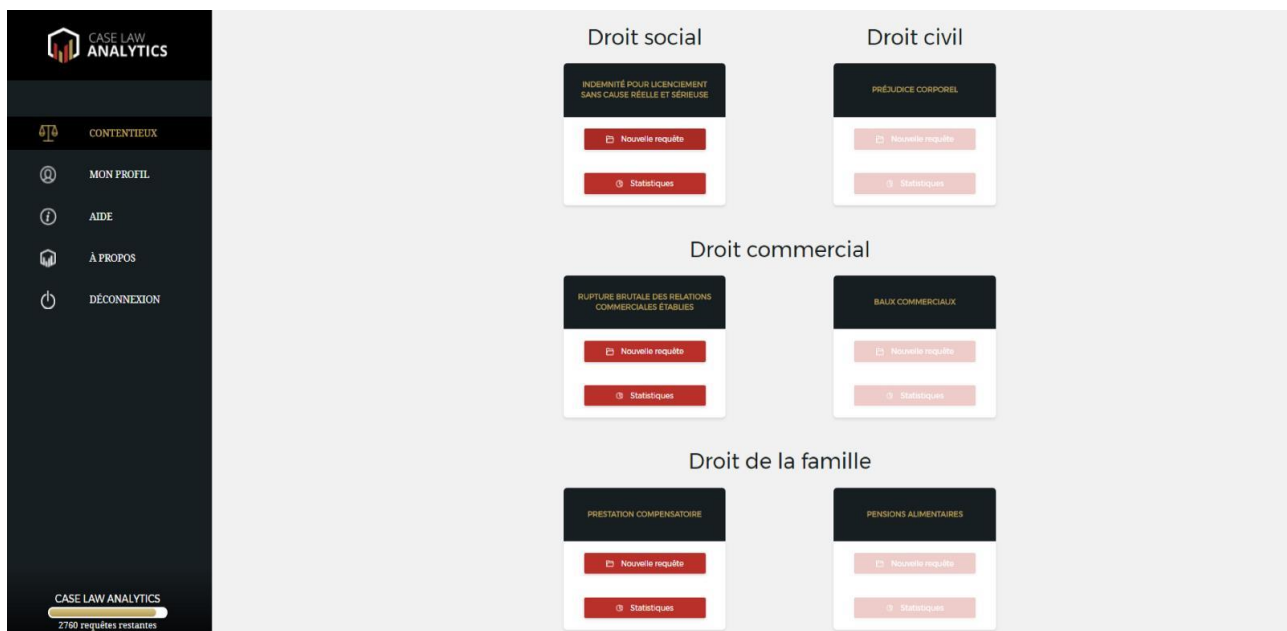


**Figure 1**  
AI for Lawyers: Lex Machina. Source: lexmachina.com

The use of AI allows also to enlarge systems' functionalities up until outcome prediction. A further typology of AI technology for lawyers derived directly from expert systems, but evolved in a different path, utilizes large-datasets for outcome prediction. This typology of software, called predictive analytics, utilizes data mining to provide to users predictions of possible outcomes of a given procedure, in terms of results, costs or ruling of a sentence. An interesting example of predictive analytics technology is the one developed by Lexis Nexis, called Lex Machina. Lex Machina (see **Figure 1**; <https://lexmachina.com>) has

been developed with the objective of predicting court's decisions on US Patent law. The software gathers and combines data on attorneys, judges and parties' behavior in previous proceedings. In order to make predictions, the software analyses data on Judges' decisional trends and approaches, attorney performances, party litigation profiles, patent litigation history, time to termination/trial, successful motion strategy, case outcomes and amount of compensations for damages (Campbell, 2012). The principal operations that can be pursued by the software are the following: a. State the probability of outcomes of a court proceedings for different legal strategies; b. Predict the behavior of judges (decisions), lawyers/parties' strategies; c. Access information related to probability assessments in clear graphs/charts; d. Access to case resolutions data (Campbell, 2012).

**Case Law Analytics** (see **Figure 2**; <https://www.caselawanalytics.com/>) is a further example of predictive analytics technology. The tool has been developed in France in collaboration with the INRIA (Institute of Research of Informatics and Automatization) and with the involvement of both lawyers and mathematicians. The tool analyses the judicial decision processes to forecast decisions on a given file and to offer to legal professionals an estimate of the risk to be faced. Case Law technology is applicable in most areas of law, provided that there is a minimum of case law or transactional history (Lévy Véhel, 2018). The software allows to quantify the legal risk for clients, to obtain case-law information for each jurisdiction and to justify lawyer's remuneration on the basis of the probability of success. Moreover, the system permits to develop a reliable and dedicated team of "virtual lawyers" capable of providing legal risk for current and future cases and valuing the entire legal history of the parts, both for litigation and for alternative dispute resolution.



**Figure 2**

AI for Lawyers: Case Law Analytics. Source: [www.caselawanalytics.com](http://www.caselawanalytics.com)

Another important functionality that AI technology can automatize, substituting the efforts of a real lawyer, is the "document review". An interesting example of document review AI technology is the one developed by the Cambridge University called **Luminance**. Luminance (see **Figure 3**;



<https://www.luminance.com/>) is an artificial intelligence platform for the legal profession. By utilizing pattern recognition and machine learning intelligence, Luminance reads and understands contracts and other legal documents, finding significant information and anomalies (differences in structure and content that Luminance has identified between similar contracts) without any instruction. The software is principally utilized for due diligence, compliance, insurance and contract management (Gandhi, 2017). Luminance uses a combination of supervised and unsupervised machine learning to find key information within thousands of contracts. Clauses, documents, currencies, locations, governing laws and more are automatically tagged for faster navigation, while anomaly detection highlights areas of potential risk. The software has been developed by the Cambridge University for the United Kingdom legal context and is now being adapted to other legal systems. In Italy, for example, a law firm (<http://www.portolano.it/>) is working on the application of the software to the Italian legal context (Lupo, 2018).

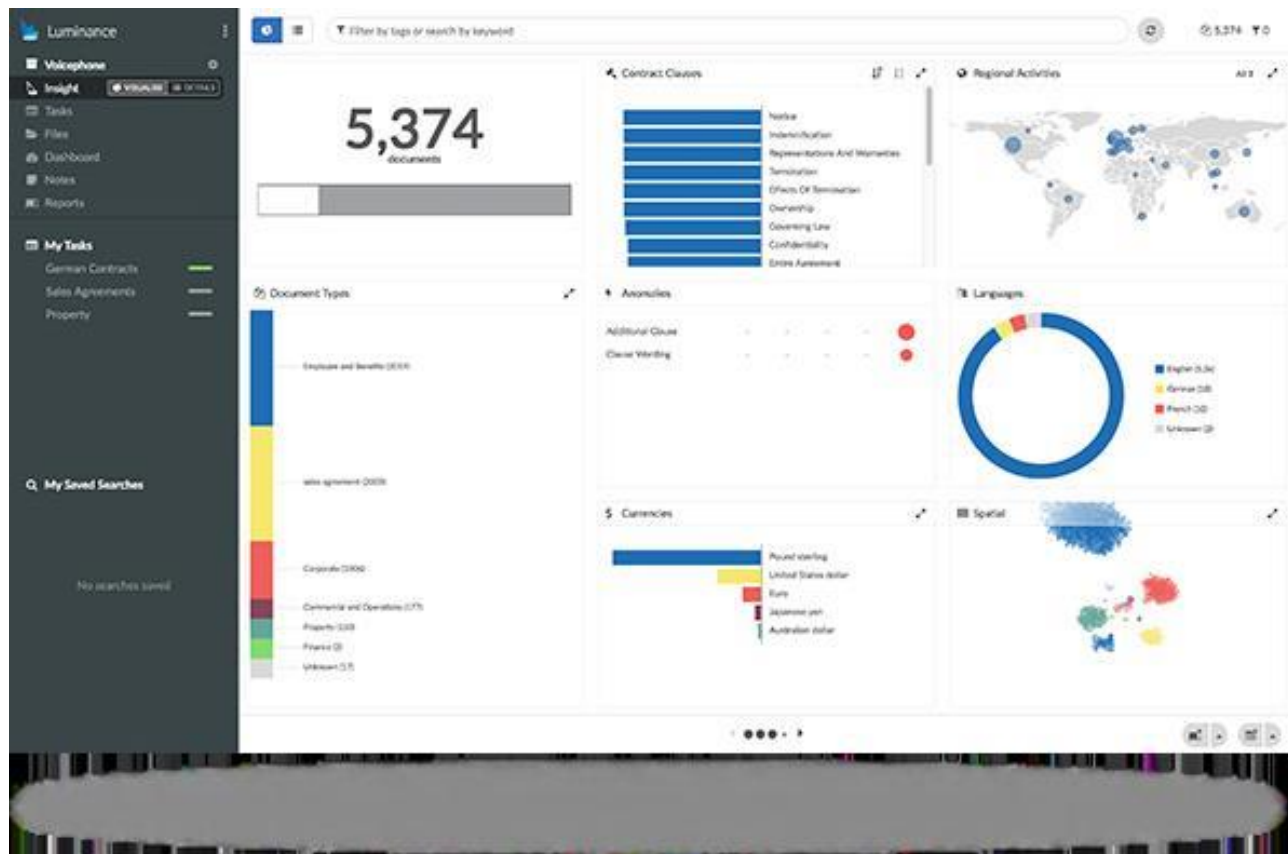


Figure 3

AI for Lawyers: Luminance. Source: [www.luminance.com](http://www.luminance.com)

Aside AI for lawyers, some attempts to apply this technology for supporting justice institutions such as courts, public prosecution offices and police forces have been made.<sup>2</sup> However, the use of AI tools in

<sup>2</sup> Due to the scarce diffusion of AI between judges and court staff, the systems here described also include those tools utilized by other actors of the judiciary as police forces.

the judiciary is not diffused in comparison to AI technologies for lawyers. Particularly interesting examples of AI for the judiciary are the criminal risk assessment tools (Quinsey, 2005). These are technologies that process large amount of data in order to assess the risk that an offender will reiterate the criminal behavior (recidivism). AI criminal risk assessment tools can support judges' decisions regarding different types of precautionary injunctions, from rehabilitative programs to detention (Skeem and Monahan, 2011).

**COMPAS** is a good example of criminal risk assessment tool. The tool has been developed by a privately held company and is used by the Wisconsin and California Department of Corrections. The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is a research-based, risk and needs assessment tool for criminal justice practitioners. The system assists practitioners in the placement, supervision, and case management of offenders in community and secure settings. COMPAS elaborates data gathered through a questionnaire - used to determine overall risk potential and criminogenic needs profile - administered to the arrested and it processes data on the inmate's history regarding substance abuse, education, family background, criminal activity, and social functioning (Brennan and Ehret, 2009). This tool allows the California and Wisconsin Department of Corrections and Rehabilitation (CDCR) to use evidence-based principles in order to provide rehabilitative programming to the higher risk-to-reoffend prisoners and parolees, and to provide other types of programs to low-risk-to-reoffend prisoners and parolees (Skeem and Loudon, 2007). COMPAS also helps correctional staff to assign the inmates to the right programs at the right time based on individual risk and needs assessments.

A further example of criminal risk assessment tool utilized in the judiciary is **HART**. The Harm Assessment Risk Tool (HART) has been developed by the Durham Constabulary. This artificial intelligence system is designed to predict whether suspects are at a low, moderate, or high risk of committing further crimes in a two year period (Ariza et al., 2016). The algorithm is used by police forces in the UK. It does not decide whether a suspect should be kept in custody, but it is intended to help police officers to pick if a person should be referred to a rehabilitation program (called "Checkpoint") or not. HART uses data from 34 different categories – covering a person's age, gender, domicile, civil status, offending history (Oswald et al., 2018). Data for the Harm Assessment Risk Tool (HART) were taken from Durham police records between 2008 and 2012. The system was then tested in 2013, and the results - showing whether suspects did in fact offend or not - were monitored over the following two years. Forecasts that a suspect was low risk turned out to be accurate 98% of the time, while forecasts that they were high risk were accurate 88% of the time (Ariza et al., 2016; Oswald et al., 2018).

Very few are the examples of expert systems based on AI utilized by judges or court staff. One of such examples is the Italian **TOGA**. TOGA (see **Figure 4**; <https://toga.cloud/>) is an artificial intelligence tool that provides different types of information related to criminal procedures. The system has been developed to support prosecutors, however it can be utilized also by lawyers specialized in criminal matters.<sup>3</sup> The tool has been developed by a team composed of ICT experts, lawyers and judges. In order to provide a database for the tool, TOGA team gathered data on all the typologies of crimes defined by the Italian criminal law (4000 typologies). TOGA users can have access to several information by utilizing the research functions of the tool. The research can be activated by filing a norm, a special law or through a keyword research. After activating the research function, the tool can provide information as: penalty, juridical competence, precautionary and interdictory measures, arrest, detention, plea bargain etc. Moreover, TOGA associates one or more crimes to a specific case and get the calculations of deadlines (procedural terms and the prescription).

---

<sup>3</sup> <https://toga.cloud/>



As this short presentation shows, AI technologies are being developed and starting to be utilized not only by lawyers but also by the different institutions of the judiciary. It is plausible that in the near future more and more AI technologies for the judiciary will be developed and will be utilized. This phenomenon implies several challenges both at the practical and ethical level. These implications and the risks related to the use of AI in the judiciary will be discussed in the next section.

| REATO        | PROCESSO               | TIPO                | PENA                        |
|--------------|------------------------|---------------------|-----------------------------|
| Sanzione     | delitto                | Fermo               | no                          |
| Tipo         | reato autonomo         | Arresto             | obbligatorio                |
| Tipo pena    | reclusione             | Misure cautelari    | custodiali e non custodiali |
| Pena         | mesi 6 - anni 5        | Misure interdittive | si                          |
| Prescrizione | anni 6 / anni 7 mesi 6 | Messa alla prova    | no                          |
| Fatto tenue  | si                     | Oblazione           | no                          |

**Figure 4**

AI for the Judiciary: TOGA. Source: <https://toga.cloud/>

### 3. AI in Justice, Why Should Be Regulated

The previous section acknowledged the increasing diffusion of Artificial Intelligence in the justice domain. The almost uncontrolled diffusion of this type of technology in support of justice professionals that have to comply to rigid sets of deontological rules needs a consideration related to the main implications related to the use of AI in justice. The practical and ethical implications discussed here refer to the following main topics:

1. The use of data;
2. Confidentiality;
3. Liability and responsibility of systems;
4. Transparency;
5. The competence of lawyers;
6. Equal access to justice;
7. Clients' confidentiality;
8. Accountability;
9. Protection against discrimination.

As we have seen in the previous section, AI technologies for justice rely on the availability of large amount of data as the main “fuel” for their functioning (Lupo, 2018). Expert systems as Ross and Doctrine (see *Section 2*), utilize data on case-law and norms in order to provide updated information to lawyers on the basis of keywords searches. Moreover, predictive analytics tools as COMPAS obtain and utilize sensible data on arrested in order to assess the probability of recidivism. Therefore, key elements of the AI for justice “fuel” are open and big data.<sup>4</sup> Open data refers to data organized in a database, that are freely downloadable and re-employable without having to pay an operating license (Huijboom and Van den Broek, 2011). Open Data are composed by raw data that are generally not readable as such by all the citizens, but they must be processed to be presented and understandable. On the other hands, big data refers to big set of data, which can be subject to a computer process (open data or data employable with a not-for-free operating license, electronic messages, connection traces, GPS signals etc). The definition of Big Data resembles the definition of a considerably big dataset. However, what distinguishes big data from datasets are three elements (three V rule): a. large “volume” of data; b. large “variety”; c. high “velocity” (Hoffman and Podgurski, 2013). The main issue with the use of Open data by privately developed AI technologies regards the compatibility of algorithms with data protection principles. On the one hand, in order to improve transparency and accountability of public bodies, there is a growing tendency to make available data coming from public institutions (including courts’ decisions) in the form of freely downloadable databases. In particular, justice systems may provide access to two types of case law data: a. public case law data; b. private structured data coming from courts’ Case Management Systems (CMS). The open access to case-law data raises concerns in terms of privacy, data protection of sensitive data (name, addresses, etc.), use and abuse of data by third parties (Lupo, 2018; Huijboom and Van den Broek, 2011). The protection of citizens’ data is also connected to the question of confidentiality, a deontological rule to which lawyers should comply. Systems as Ross or Case Law Analytics need to gather, datafy, format, and use clients information in order to function. Therefore, the lawyer that utilizes the system needs to know how to protect his or her client’s confidentiality when utilizing AI systems (Lupo, 2018; Martyn, 2002). In order to protect confidentiality when utilizing systems lawyers must (1) competently understand how AI systems work; (2) communicate with clients and former clients to understand expectations and preferences; and (3) ensure that the system utilized is able to protect clients’ confidentiality by denying unwanted access to the data utilized (Martyn, 2002).

A second challenge related to Artificial Intelligence and justice regards the liability of systems and issues of responsibility in case of failure. AI systems utilized by judges, public prosecutors, police and lawyers pursue very sensitive tasks that may have important consequences on the future outcome of a procedure. The lawyer may trust in the effective capacity of an AI as Ross to find the right case-law needed to sketch out a lawsuit; moreover, a system contributing to or influencing a judge’s decision regarding a citizen may have serious consequences for him/her. Therefore, the issue of systems’ liability and safety is fundamental. AI technologies are developed by computer scientists that, as fallible human beings, may not avoid errors and vulnerabilities (Abney and Bekey, 2011). While this usually does not result in significant harm with, say, office applications, a flaw in machinery such as a car or a robot based on AI could lead to fatal results.<sup>5</sup> As put in evidence, this is the case also for AI technologies utilized by lawyers and judges

---

<sup>4</sup> Here, the introduction of big data and their use by AI is only descriptive and does not go into deep investigating the different forms of data available as statistical data, structural data or meta data.

<sup>5</sup> For instance, in August 2010, the US military lost control of a helicopter drone during a test flight for more than 30 minutes and 23 miles. The drone veered towards Washington DC, violating airspace restrictions meant to protect the White House and other governmental assets (Bumiller, 2010; Lin et al., 2011).

and this issue is directly related to the question of security and hacking of systems. AI systems store great amount of sensitive data, therefore, the issue of their safety from abuse by criminals or simply mischievous persons is also fundamental.

Related to liability and security is the question of responsibility for failing AI systems. As previously mentioned, AI systems, when failing, may cause dangerous consequences to users or clients (in the case of technologies for lawyers). At the same time, the complexity of such systems may not make clear who is responsible in case of bias and mistakes of systems, if the lawyer or judge that decided to utilize it or the third party that developed the system (Lupo, 2018). This issue may regard the relationship between lawyers and third parties providing a service to lawyers. All lawyers (in any justice system) must comply to rules of professional conduct (deontology). Therefore, by developing AI for lawyers, third parties may run the risk of affecting lawyers' compliance to deontology (for instance divulging sensitive personal data). It is consequential that on the one hand, third parties should take into account the possibility that the systems developed do not comply with lawyers' rules of conduct. On the other hand, lawyers before buying or utilizing systems, should check if they affect their compliance to deontology.

The aspect of responsibility regards also citizens that are affected by a judicial decision based on a failed, flawed or biased system. In this case, citizens should have the right for an "effective remedy".<sup>6</sup> However, this is particularly challenging for individuals affected by a decision supported by AI technologies, due to the opaqueness of the decision and of the uncertainties related to responsibility for failures (Contini, 2019; Abney and Bekey, 2011).

These aspects acknowledge that justice professionals that utilize AI systems should be able to verify their functioning and compliance with procedural rules. In order to pursue these checks however, justice professionals have to understand how the system works and consequentially, must have a level of technological knowledge that it is not diffused between lawyers and judges. This introduces a further implication of the use of AI in justice: "competence".

A fundamental principle of lawyers' rule of conduct is the "competent representation": this requires that lawyers have the legal knowledge, skill, and preparation reasonably necessary for the representation (Davis, 2009). Moreover, lawyers should keep up with changes in the law. It is therefore plausible that the principle of competence may extend to the use of Artificial Intelligence, so that lawyers should understand not only the technical aspects of the technology they adopt, but also the related ethical implications (including eventual AI's bias and limits and confidentiality concerns). Given that there is not a diffused knowledge between lawyers relative to AI, scholars as Simon (2018) suggest that lawyers must be supported by experts that check the system and also double check the outputs of AI technology in comparison to outputs of procedures pursued without the help of the system. The aspect of due competence is also related to the principle of candid advice that lawyers must provide to clients (Lupo, 2018; Simon, 2018). The lawyer's deontology foresees that a lawyer communicates clearly and understandably to a client all the aspect of a case or procedure, including risks, potential outcomes and billing. This may regard also the repercussion for a client of the use of AI technologies. It is consequential that a lawyer supported by AI technologies has to have the capability of providing a candid advice to a client in terms of advantages, disadvantages and risks related to the use of AI.

---

<sup>6</sup> The article 47 of the European Charter of Human Rights establishes the right to an effective remedy and to a fair trial: "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented" (European Union Charter of Fundamental Rights).

Another implication of the use of AI technologies regards the “equal access to justice” of citizens. Equal access is a fundamental justice value (Cappelletti, 1978; Sandefur, 2011; Sherman, 2013; ENCJ, 2013). According to the European Network of Councils for the Judiciary, judges and courts should carry on their activities guaranteeing the equal access of all citizens (ENCJ, 2013). Consequentially, justice systems should not prevent access to the justice system, on the basis of, for example, gender, sexual orientation, geographic location, religion, right of representation, disabilities etc. (Staats et al., 2005). Some scholars put the emphasis on the fact that Artificial Intelligence supporting self-help legal services as DoNotPay<sup>7</sup> may reduce the barriers of access to legal representation (Prillaman, 2000). AI technologies for self-represented litigants may be less costly in comparison to a “human” lawyer. However, an incomplete diffusion of technological literacy may hinder the advantages related to the development of these types of technologies. On the other hand, AI technologies for self-represented litigants only cover a restricted share of procedures (given that they mainly focus on simple procedures that do not need the support of a lawyer as administrative fines).

On a different level, for some scholars, also AI technologies supporting lawyers, here discussed, may affect positively access to justice by reducing the costs of representation (Morgan et al., 2018). AI, by speeding up the work of a lawyer and carrying out time consuming activities that “human” lawyers usually do, should contribute to reduce the costs for clients. However, AI technologies are not easily accessible for lawyers due to the types and amounts of competences needed to utilize these systems. The acquisition of these competences by lawyers is costly and this may favour large law firms more than single lawyers (Lupo, 2018; Moss, 2016). As a consequence, instead of having a positive impact to access to justice, the development of “costly” AI systems for lawyers may hinder accessibility (Brescia et al., 2014).

Some implications related to the application of AI systems in justice regard only systems utilized by judges or other justice institutions, as police forces, and refer to the generic value of rule of law.

One implication regards the fundamental rule of law value of accountability. Accountability is the mechanism by which courts and judicial activities are checked in terms of respecting rule of law values and efficiency (Waterman and Henshon, 2008). Accountability means that judges should be responsible for their actions before legal and political institutions that counter balance judicial power (Contini and Mohr, 2008; Latour, 2002; Simon et al., 1961). Given the main issues that may affect AI systems utilized in the judiciary, it is plausible that also AI should be kept accountable. This may entail for instance the involvement of an independent third party that operates different typologies of control and monitoring in order to safeguard the judiciary and affected citizens, from failure, biases and security break of the systems.

Furthermore, AI utilized by justice institutions may also affect transparency. Transparency is considered a rule of law fundamental value (Lupo, 2019). Transparency concerns disseminating information to the parties and public on judicial procedures, rights, and norms (Lupo, 2019; Wallace, 2003). Information can be disseminated through several channels such as public hearings, the media, reports, use of information, and communication technologies. Transparency also encompasses whether information on norms and procedure is accessible, which is not always the case due to complex legal jargon (Sherman, 2013). On the basis of this, judicial decision-making based on AI tools should provide to affected citizens an

---

<sup>7</sup> DoNotPay is a free chatbot that offers AI-powered legal counsel and services. The chatbot works by asking a series of basic questions (as the description of the claim). The service draws up the documents needed and sends them to the courthouse. Initially created to dispute parking tickets in some USA states, over time increased in complexity in order to offer legal advice in more states (all 50 states across the US are supported) and for a greater variety of issues including volatile airline prices, data breaches, late package deliveries, and unfair bank fees (Morgan et al., 2018).

adequate amount of information regarding the procedure and how the decision has been reached. It is however questionable the accessibility of these types of information, given that they might entail technological specifications that are not easily understandable.

A further implication of the use of AI in the judiciary regards in particular predictive analytics tools as COMPAS utilized for risk assessment and supporting decisions affecting a defendant. The literature suggests that AI risk assessment tools may improve the impartiality of decisions because the usual bias affecting human decision-making (psychological or environmental biases) are absent (Simshaw, 2018). Differently, AI predictive analytics for risk assessment may be highly prejudicial in terms of ethnic and racial backgrounds (Chouldechova, 2017). These systems are “trained” by filing past decisions and existing police and judicial databases. As a consequence, systems may incorporate intentional or unintentional systemic human biases. Moreover, predictive analytics may be affected by the factors influencing their outcomes. Some predictive technologies correlate criminal risk to factors related to address, age, family provenance, belonging to a minority group; therefore, it is plausible that it may associate high criminal risks to minorities’ affiliation (Hall and Gill, 2017). A study by Pro-publica evaluated the capacity of the mentioned tools to forecast future crimes and to assess criminal risks: for the study, the tools are highly unreliable and they are biased towards minority groups (Chouldechova, 2017).

This section acknowledges the many ethical and rule of law implications related to the use of AI in justice. The potential effects of AI on values such as accountability and transparency or on lawyers’ deontological rules as “due competence”, suggests the need for normative frameworks that supports the respect of judicial values disciplining the application of AI in justice.

The next section discusses the several attempts by private and public institutions to discipline the application of AI in general and in the specific of justice systems. The section acknowledges the necessity of a more intense effort by States and international institutions on disciplining on a compulsory fashion the application of AI in justice, thus limiting potential consequences on fundamental justice values.

#### 4. Disciplining Ai in Justice

As we have seen, the introduction of Artificial Intelligence in the justice systems and their use by justice professionals cannot be analysed without taking into account their impact on the complex infrastructure of norms and values on which rule of law is based. Also the introduction of “simple” ICT tools for digitalizing justice procedures or in support of lawyers’ routines, is entangled with the complex sociotechnical context, composed of norms, procedures, routines, actors, skills (Velicogna, 2007; Contini and Mohr, 2008). Due to their impact on normative frameworks, sociotechnical infrastructure, and potentially on rule of law values, ICT introduction in to the judiciary is usually combined with the introduction of norms or the modification of existing norms (Contini and Mohr, 2008). In the case of Artificial Intelligence, due to the only recent and scarce diffusion, there are not so many normative frameworks disciplining the application of these technologies in several contexts and in the specific of justice systems. Nonetheless, the potential negative consequences of AI diffusion ensures that different actors, as international organizations, research centres or even private companies, try to overcome the normative void by drafting normative frameworks regarding AI use.

In order to investigate how the use of Artificial Intelligence in the justice systems is been disciplined, this section focuses on a vast array of normative frameworks with a special focus on which values and principles, between the one listed and discussed in the previous section, are protected against the potential biases of AI. The frameworks analysed include frameworks drafted by private companies, frameworks drafted by international organization, scientific forum, commission and conferences, EU and national



parliaments (for a list of frameworks investigated, see **Table 1**). The analysis is not specifically restricted to frameworks disciplining AI use in justice. This in order to provide a broader spectrum on the topic of Artificial Intelligence regulation, since only few frameworks are specifically drafted for disciplining AI applied in the judiciary.

Three frameworks analysed have been drafted as a result of a discussion in the ambit of an international forum or association:

1. The 40<sup>th</sup> declaration on ethics and data protection in AI;<sup>8</sup>
2. The ACM Code of Ethics and Professional Conduct;<sup>9</sup>
3. The Barcelona Declaration.<sup>10</sup>

The first framework mentioned is the product of the 40th International Conference of Data Protection and Privacy Commissioners that saw the cooperation of three main bodies: Commission Nationale de l'Informatique et des Libertés (CNIL), France; European Data Protection Supervisor (EDPS), European Union; Garante per la protezione dei dati personali, Italy. The second framework mentioned has been drafted by the Association for Computing Machinery (ACM), an educational and scientific computing society that delivers resources that advance computing as a science and a profession. Finally, the Barcelona declaration has been drafted as a result of an international scientific debate organized by “B-Debate”, an international centre for scientific debate (Cataluña, Spain).

With regards to the potential impacts of AI on the values introduced in section 3, with the exception of the Barcelona Declaration, the frameworks quoted recommend the protection of data and privacy. In particular, the declaration on ethics and data protection assesses that when implementing AI, “*technical and organizational measures and procedures – proportional to the type of system that is developed – have to ensure that data subjects’ privacy and personal data are respected, both when determining the means of the processing and at the moment of data processing*”. Both the declaration on ethics and data protection and the ACM declaration, foresees the protection of principles as transparency and accountability; moreover, they take also into account aspects as the necessity of remedies against biases affecting users and citizens in general and the aspect of confidentiality (see *Section 3*). Differently, the Barcelona declaration takes into account the importance of accountability measures and the aspects of reliability of systems, and the responsibility of designers and producers in cases of biases or failures. Interestingly also for the justice context, the Barcelona declaration emphasizes the potential risks of the automation of work and the consequential potential loss of jobs in different sectors. This aspect may also regard justice systems and in particular, lawyers. Indeed, most AI systems for lawyers are applied for routine tasks that regard the processing of large amount of data and documents. For instance, Luminance AI technology is mainly utilized for due diligence, that is the investigation that a business usually takes before entering into an agreement or contract (Roodman, 2012). This task foresees the analysis of documentation usually performed by trainee in law firms. By pursuing this assignment, trainees used to acquire the necessary skills to perform the profession (above all in the field of due diligence). Therefore, the diffusion of AI technologies as Luminance that substitutes trainees’ work may reduce these important occasions for training in the law field.

Between the frameworks investigated, three have been drafted by academic associations or research centres:

1. Asilomar AI principles;<sup>11</sup>

<sup>8</sup> [https://icdppc.org/wp-content/uploads/2018/10/20180922\\_ICDPPC-40th\\_AI-Declaration\\_ADOPTED.pdf](https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf)

<sup>9</sup> <https://www.acm.org/code-of-ethics>

<sup>10</sup> [https://www.bdebate.org/sites/default/files/barcelona-declaration\\_v7-1-eng.pdf](https://www.bdebate.org/sites/default/files/barcelona-declaration_v7-1-eng.pdf)

2. The Japanese Society for Artificial Intelligence Ethical Guidelines;<sup>12</sup>
3. The EPSRC principles of robotics.<sup>13</sup>

The Asilomar AI principles have been developed within the 2017 Asilomar conference, that has been organized by the Future of Life Institute and that brought together a group of AI researchers from academia and industry, and thought leaders in economics, law, ethics, and philosophy. The Ethical guidelines of the Japanese Society for Artificial Intelligence have been drafted by its Ethics Committee, composed by a group of experts with the goal of exploring the relationship between artificial intelligence research/technology and society and its potential consequences. The EPSRC principles of robotics have been developed by EPSRC (the Engineering and Physical Science Research Council) by involving experts from the worlds of technology, industry, the arts, law and social sciences. All the three frameworks emphasize the importance of accountability, foreseeing forms of control over the functioning of systems. The Asilomar principles and the JSAI ethical guidelines, assess also the importance of foreseeing remedies against biases of the AI. Moreover, both frameworks focus on transparency: the Asilomar charter in particular assess two principles: 1. Failure Transparency: If an AI system causes harm, it should be possible to ascertain why; 2. Judicial Transparency: Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.

Interestingly, the Asilomar principles and the EPSRC principles also express concerns regarding the automation of work and the necessity of protecting workers against possible loss of jobs. Of the three frameworks, only the JSAI guidelines focus on aspects related to the protection of data and privacy. The JSAI introduces another aspect that have not been taken into account in our previous analysis (*Section 3*), and regards the protection of intellectual property: “*the development of AI should not bring harm to others through violation of information or properties belonging to others.*” The aspect of intellectual property violation obviously applies also to the development of AI systems to be utilized by justice professionals.

Normative frameworks disciplining development and use of AI have been drafted also by human rights international non-governmental organization as the Human Rights Watch. This organization headquartered in New York City, conducts research and advocacy on human rights by involving country experts, lawyers, journalists. The organization drafted The Toronto Declaration<sup>14</sup> (“*Protecting the right to equality and non-discrimination in machine learning systems*”), a set of guidelines that draw attention to the relevant and well-established framework of international human rights law and standards and aims at exploring the harms arising from AI and machine learning technology for protecting individuals from discrimination, for promoting inclusion, diversity and equity, and safeguarding equality. Of the potential harms on values discussed in the previous section, this framework mainly focuses on protection of data and privacy and on the remedies against biases of the systems. Moreover, the framework introduces also the principle of equal access and non-discrimination, values that as we have seen may be affected by the introduction of AI in the judiciary (see the COMPAS case in *Section 3*). The framework states that “*in employing new technologies, both state and private sector actors will likely need to find new ways to protect human rights, as new challenges to equality and representation groups arise. Moreover, existing patterns of structural discrimination may be reproduced and aggravated in situations that are particular to these technologies – for example, machine learning.*”

---

<sup>11</sup> <https://futureoflife.org/ai-principles/>

<sup>12</sup> <http://ai-elsi.org/wp-content/uploads/2017/05/JSAI-Ethical-Guidelines-1.pdf>

<sup>13</sup> <https://epsrc.ukri.org/research/ourportfolio/themes/engineering/activities/principlesofrobotics/>

<sup>14</sup> [https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration\\_ENG\\_08-2018.pdf](https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf)

Also private companies involved in design and development of Artificial Intelligence work on disciplining the use of these systems by developing guidelines and policies. A framework here analysed is the Phrased's AI Ethics Policy<sup>15</sup> a list of “*practical, specific and explicit*” ethics principles that address potential issues related to the use of AI. Of the values that in our analysis can be affected by the application of AI in the judiciary, the mentioned framework only addresses the potential discriminations derived from the use of these systems: the company commits itself to “*remove prejudice from their data sets and ensure a generalised model.*” The framework, and this introduces an important concept also for the judicial context, focuses also on the importance of developing mechanisms of monitoring of the application of the principles stated in the document.

Even though there is not a compulsory regulation specifically regarding the design and development of Artificial Intelligence in the EU, several EU institutions are working on disciplining this issue with different results and forms.

The EU parliament and in particular the Committee on Legal Affairs drafted in 2016 the European Civil Law Rules in Robotics<sup>16</sup>, a study that evaluates and analyses, from a legal and ethical perspective, a number of future European civil law rules in robotics and proposes a set of principles and recommendations regarding the application of these systems. The document has been drafted as a result of the activities of a working group within the Committee on Legal Affairs constituted in 2015 with the primary aim of drawing up “European” civil law rules in this area (*lege ferenda*). The framework takes into account three aspects that may be fundamental for the application of AI in justice (see section 3) that is the protection of data and privacy, the reliability of systems and the equal access of users. As far as the last recommendation is concerned, the document states that “*technological benefits should be open to all, since European legislation anchors it in the principles of solidarity, equality and fairness*”. It is interesting that the framework sheds light on the risks related to liberty caused by the application of AI systems. For the authors, any risk on liberty coming from these systems should be prevented in respect of the Article 6 of the Charter of Fundamental Rights of the European Union of 7 December 2000 that states that “*everyone has the right to liberty and security of person*”. Another recommendation regards the “*refusal of care*”. The framework, in most of its sections, focuses on AI and robots applied in health care and therefore put an emphasis on the importance of assuring the right for a patient to refuse care if they are pursued by an AI system or robot, respecting the liberty and dignity rights. This principle can be transferred to justice, assessing that a citizen or a defendant should have the right to refuse that an automatized decision pursued by an AI system, affects the procedure.

Between the frameworks focusing on AI, only few regards specifically artificial intelligence applied in justice. A worth mentioning framework is the one drafted by the CEPEJ (Council of Europe European Commission for the efficiency of justice) in 2019: the “*European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*”<sup>17</sup>. The charter has been drafted by involving international experts in different fields from law to technology and philosophy and has the scope of proposing a set of principles that should be supported when applying AI to justice in compliance with the European Convention on Human Rights and the Convention on the Protection of Personal Data. The document sets five basic principles:

1. Respect for fundamental rights;

<sup>15</sup> <https://phrasee.co/support/ai-ethics/>

<sup>16</sup> [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL\\_STU\(2016\)571379\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf)

<sup>17</sup> <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>

2. Principle of non-discrimination;
3. Principle of quality and security;
4. Principle of transparency;
5. Principle “under user control”.

It is evident that the charter takes into account almost all the aspects related to the risks of using AI in the judiciary discussed in *Section 3* (see **Table 1**). However, it omits the importance of mechanisms of accountability, the necessity of remedies against systems' failure, the respect of confidentiality (related to AI systems employed by lawyers), the importance of adequate competence in using the systems, and the value of equal access.

| <b>Tab.1.a Framework Documents and Principles</b>                                     |  |  |                                |                            |   |
|---|--|--|--------------------------------|----------------------------|---|
|   | <i>Declaration on ethics and Data Protection in AI</i> | <i>ACM Code of Ethics and Professional Conduct</i> | <i>Barcelona Declaration</i>   | <i>Asilomar principles</i> | <i>CEPEJ CHARTER</i>  |
| <b><i>Institution that drafted the document</i></b>                                   | 40th International Conference of Data Protection       | Association for Computing Machinery (ACM)          | B-Debate                       | Asilomar conference        | Council of Europe European Commission for the efficiency of justice |
| <b><i>Type of document</i></b>  | Declaration  | Code of Ethics                                     | Declaration of principles      | List of principles         | Charter and study on AI in justice                                  |
| Privacy and Protection of data  | X  | X  |                                |                            | X   |
| Remedies against biases   | X  | X  |                                |                            |   |
| Transparency  | X  | X  |                                | X                          | X   |
| Confidentiality   |  | X  |                                |                            |   |
| Accountability  | X  | X  | X                              | X                          | X   |
| Competence  | X  | X  |                                |                            |   |
| Reliability   |  |  | X                              |                            |   |
| Responsability  |  |  | X                              | X                          |   |
| Safety  |  |  |                                | X                          | X   |
| Discrimination  |  |  |                                |                            | X   |
| Equal Access  |  |  |                                |                            |   |
| Other   | Human rights   |  | Protect against automatization | Human rights               | Human rights  |
| <b>Note:</b> Framework documents, institutions that drafted the document, principles. |  |  |                                |                            |   |



| <b>Tab.1.b Framework Documents and Principles</b>                                     |   |  |   |   |                            |
|---|---|--|---|---|----------------------------|
|   | <i>European Civil Law Rules in Robotics</i> | <i>The Japanese Society for Artificial Intelligence Ethical Guidelines</i> | <i>Phrasee Ethical Guidelines</i>           | <i>EPSRC Ethical Guidelines</i>                   | <i>Toronto Declaration</i> |
| <b>Institution that drafted the document</b>  | EU parliament (Committee on Legal Affairs ) | Japanese Society for Artificial Intelligence (Ethics Committee)            | Phrasee AI company                          | Engineering and Physical Science Research Council | Human Rights Watch         |
| <b>Type of document</b>   | Study and set of rules                      | Ethical Guidelines   | Ethical Guidelines                          | Ethical Guidelines                                | Declaration                |
| Privacy and Protection of data  | X   | X  |   |   | X                          |
| Remedies against biases   |   |  |   |   | X                          |
| Transparency  |   | X  |   |   |                            |
| Confidentiality   |   |  |   |   |                            |
| Accountability  |   | X  |   |   |                            |
| Competence  |   |  |   |   |                            |
| Reliability   |   |  |   |   |                            |
| Responsability  | X   | X  |   | X   |                            |
| Safety  |   |  |   | X   |                            |
| Discrimination  |   | X  | X   |   | X                          |
| Equal Access  | X   | X  |   |   | X                          |
| Other   | Refusal of care                             | Intellectual property  | Monitoring application, respect vulnerables | Human rights, protecting from harm                | Human rights               |
| <b>Note:</b> Framework documents, institutions that drafted the document, principles. |   |  |   |   |                            |

The previous discussion acknowledges that several institutions are dealing with disciplining the growing application of Artificial Intelligence in several fields with non-binding framework documents, covering the lack of norms at the EU and international level. However, it is worth saying that national governments and parliaments are progressively taking into account potential risks related to the development and use of AI, by drafting and approving laws disciplining these issues. As an example, in France a 2016 law focuses on a fundamental aspect related to the use of AI, that is the protection of data. The 2016 law on the digital republic foresees that all court decisions at all instances have to be disseminated in the form of open data, for free and with respect for the privacy of the persons concerned. The law foresees also that public availability of data on a given person should be preceded by an analysis



of the risk of re-identification of the person concerned. Additionally, in Italy, a legislative decree<sup>18</sup> disciplines the use of AI tools for judicial decision making and it states the following norms:

1. Decisions based solely on automated processing, including profiling are prohibited, unless authorized by European Union law or specific legal provisions;
2. The provisions of law must provide adequate guarantees for the rights and freedoms of the interested party. In any case, the right to obtain human intervention by the data manager is guaranteed;
3. Without prejudice to the prohibition laid down in Article 21 of the Charter of Fundamental Rights of the European Union, profiling for the purpose of discrimination against natural persons on the basis of particular categories of personal data referred to in Article 9 of the EU Regulation is prohibited.

### 5. Concluding Remarks on the Results of the Analysis

The analysis provided in this paper allowed to explore the main implications of the use of Artificial Intelligence for supporting justice practitioners, showing that they are intrinsically ethical and affect citizens' fundamental rights and fundamental justice values related to the rule of law. This aspect implies on the one hand, for what regards AI for lawyers, that it is not desirable to leave the regulation of the development and use of AI systems to the free market; on the other hand, for what regards AI for the judiciary, that it is necessary to safeguard citizens that have to deal with justice as claimants or defendants and that may be affected by decisions that are influenced on a various degree by AI systems. As we have seen, these issues represent a considerable concern for several types of actors, from private companies to international forums, from research centres to no-profit international organizations, that tried to regulate AI and prevent risks related to its use in several contexts by drafting non-binding norms included in charter, set of principles or guidelines. The obvious fallacy of these attempts of regulation is that frameworks are not binding and represent only recommendations that actors are free to follow or not. Moreover, the analysis of the normative frameworks described in section 4 allows to state that each single framework takes into account only a set of aspects related to the risks of AI utilize, while leaving aside other aspects which, on the other side, other frameworks focus on. That is to say that it is missing a comprehensive normative framework that takes into account all the potential consequences of the use of AI. Additionally, the analysis shows a shortage of binding normative frameworks specifically designed for the application of Artificial Intelligence in the justice systems. Nonetheless at least at the national level, some countries are more and more dealing with the issue of AI for justice regulation: see for instance the French 2016 law on the digital republic that regulates the dissemination of citizens' open data or the Italian legislative decree<sup>19</sup> that disciplines the use of AI tools for judicial decision making. Despite the national efforts to discipline AI can be considered a fundamental step forward towards the regulation of AI tools for justice professionals, it is worth considering two issues. First, the companies developing systems as ROSS have a globalized perspective and do not focus only on a single national market. Second, due to more and more intense commercial transactions and due also to the existence of economic and political unions as the European Union, there is a considerable diffusion of cross-border procedures interesting citizens at the international level. As a consequence, it is desirable that international institutions as the EU focus on the regulation of the use of AI in the justice sector with binding normative frameworks. It is true that some existing normative

<sup>18</sup> Legislative decree of 18 May 2018, n. 51, in application of the EU directive (UE) 2016/680.

<sup>19</sup> Legislative decree of 18 May 2018, n. 51, in application of the EU directive (UE) 2016/680.

frameworks as the EU GDPR regulation<sup>20</sup> deals with some of the aspects that are closely related to the use of AI in the justice systems as the protection of privacy and personal data; however, several risks related to AI use are still unregulated. Indeed, this study demonstrates that it is necessary a comprehensive and internationally shared legal framework that preserves human rights and fundamental justice values from an undisciplined use of Artificial Intelligence affecting justice professionals' decisions.

## References

- Bench-Capon, T. (1997). Argument in artificial intelligence and law. *Artificial Intelligence and Law*, 5(4), 249-261.
- Brennan, T., Dieterich, W., & Ehret, B. (2009). Evaluating the predictive validity of the COMPAS risk and needs assessment system. *Criminal Justice and Behavior*, 36(1), 21-40.
- Brescia, R. H., McCarthy, W., McDonald, A., Potts, K., & Rivals, C. (2014). Embracing disruption: how technological change in the delivery of legal services can improve access to justice. *Alb. L. Rev.*, 78, 553.
- Cappelletti, M. (1978) Access to Justice. Giuffrè: Milan.
- Chouldechova, A. (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. *Big data*, 5(2), 153-163.
- Contini, F., & Fabri, M. (Eds.). (2003). *Judicial Electronic Data Interchange in Europe: Applications, Policies and Trends: Research Project with Financial Support from the Grotius Civil Programme and Grotius 2. (Criminal)*, European Commission, and from the Italian Ministry of Education, University and Research (FIRB Programme). Lo scarabeo.
- Contini, F., & Lanzara, G. (Eds.) (2009). *ICT and innovation in the public sector: European studies in the making of e-government*. Palgrave Macmillan
- Contini, F. and Mohr, R. (2008) *Judicial Evaluation: Traditions, Innovations and Proposals for Measuring the Quality of Court Performance*, VDM Verlag Dr. Muller, Saarbrücken.
- Davis, L. (2009). Reconsidering Remedies for Ensuring Competent Representation in Removal Proceedings. *Drake L. Rev.*, 58, 123.
- Elisabeth Bumiller, The New York Times: Navy Drone Violated Washington Airspace (Aug. 25, 2010).
- ENCJ (2013) "ENCJ Working Group: Judicial Ethics Report 2009-2010", Report of the Euro-pean Network of Councils for the Judiciary, www.encj.eu.
- Fina, S., & Ng, I. (2017). Big Data & Litigation: Analyzing the Expectation of Lawyers to Provide Big Data Predictions when Advising Clients. *Indian JL & Tech.*, 13, 1.
- Gandhi, M. (2017). Legal technology: Hype, heuristics and humanity. *Proctor, The*, 37(11), 32.
- Hall, P., & Gill, N. (2017). Debugging the Black-Box COMPAS Risk Assessment Instrument to Diagnose and Remediate Bias.
- Hardyns, W., & Rummens, A. (2018). Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. *European Journal on Criminal Policy and Research*, 24(3), 201-218.
- Hoffman, S., & Podgurski, A. (2013). Big bad data: law, public health, and biomedical databases. *The Journal of Law, Medicine & Ethics*, 41(1\_suppl), 56-60.
- <https://toga.cloud/>
- Huijboom, N., & Van den Broek, T. (2011). Open data: an international comparison of strategies. *European journal of ePractice*, 12(1), 4-16.
- Jose Medina Ariza, J., Robinson, A., & Myhill, A. (2016). Cheaper, faster, better: Expectations and achievements in police risk assessment of domestic abuse. *Policing: A Journal of Policy and Practice*, 10(4), 341-350.
- Latour, B. (2002) *La fabrique du droit. Une ethnographie du conseil d'Etat*. Paris: La Decou-verte.
- Lévy dit Véhel, P. E., & Lévy Véhel, J. (2018). Stochastic jump intensity models. *Risk and Decision Analysis*, 7(1-2), 63-75.
- Lin, P., Abney, K., & Bekey, G. (2011). Robot ethics: Mapping the issues for a mechanized world. *Artificial Intelligence*, 175(5-6), 942-949.
- Lupo, G. (2018) "Artificial Intelligence in the Judiciary: some examples and implications", IRSIG-CNR (Istituto di Ricerca sui Sistemi Giudiziari – Consiglio Nazionale delle Ricerche), *report prepared for the Italian Ministry of Justice*.

<sup>20</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

- Lupo, G. (2019) "Assessing e-Justice Smartness: a new Framework for e-Justice Evaluation through Public Values", in Bolivar M. (eds.), *Setting Foundations for the Creation of Public Value in Smart Cities*, Springer.
- Lupo, G., & Bailey, J. (2014). Designing and implementing e-Justice Systems: Some lessons learned from EU and Canadian Examples. *Laws*, 3(2), 353-387.
- Lupo, G., & Velicogna, M. (2018). Making EU justice smart? Looking into the implementation of new technologies to improve the efficiency of cross border justice services delivery. In *Smart Technologies for Smart Governments* (pp. 95-121). Springer, Cham.
- Martyn, S. R. (2002). In Defense of Client-Lawyer Confidentiality... and Its Exceptions... *Neb. L. Rev.*, 81, 1320.
- McGinnis, J. O., & Pearce, R. G. (2013). The great disruption: How machine intelligence will transform the role of lawyers in the delivery of legal services. *Fordham L. Rev.*, 82, 3041.
- McLaughlin, E., Muncie, J., & Hughes, G. (2001). The permanent revolution: New Labour, new public management and the modernization of criminal justice. *Criminal Justice*, 1(3), 301-318.
- McLaughlin, K., Osborne, S. P., & Ferlie, E. (Eds.). (2002). *New public management: Current trends and future prospects*. Psychology Press.
- Morgan, J., Paiement, A., Seisenberger, M., Williams, J., & Wyner, A. (2018). A Chatbot Framework for the Children's Legal Centre.
- Moss, M. A. (2016). Can Technology Bridge the Justice Gap. *Fla. BJ*, 90, 83.
- Oswald, M., Grace, J., Urwin, S., & Barnes, G. C. (2018). Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality. *Information & Communications Technology Law*, 27(2), 223-250.
- Prillaman, W.C. (2000) *The Judiciary and Democratic Decay in Latin America: Declining Confidence in the Rule of Law*, Westport: Praeger.
- Quinsey, V. L., Harris, G. T., Rice, M. E., & Cormier, C. A. (2005). *Violent Offenders: Appraising and Managing Risk (Law and Public Policy)*. American Psychological Association, Washington, DC.
- Reiling, A. D. (2009). Technology for justice: How information technology can support judicial reform.
- Riff, D., Lacy, S., Fico, F., Riffe, D., & Fico, F. G. (2006). *Analyzing media messages: Using quantitative content analysis in research*. Routledge.
- Rissland, E. L., & Ashley, K. D. (1987, December). A case-based system for trade secrets law. In *Proceedings of the 1st international conference on Artificial intelligence and law* (pp. 60-66). ACM.
- Rissland, E. L., Ashley, K. D., & Branting, L. K. (2005). Case-based reasoning and law. *The Knowledge Engineering Review*, 20(3), 293-298.
- Rissland, E. L., Ashley, K. D., & Loui, R. P. (2003). AI and law: a fruitful synergy. *Artificial Intelligence*, 150(1-2), 1-15.
- Roodman, D. M. (2012). *Due diligence: An impertinent inquiry into microfinance*. CGD Books.
- Roy D. Simon, *Artificial Intelligence, Real Ethics*, N.Y. ST. B. ASS'N J., [http://www.nysba.org/Journal/2018/Apr/Artificial\\_Intelligence\\_Real\\_Ethics/](http://www.nysba.org/Journal/2018/Apr/Artificial_Intelligence_Real_Ethics/) (last visited Nov. 21, 2018).
- Rourke, L., & Anderson, T. (2004). Validity in quantitative content analysis. *Educational technology research and development*, 52(1), 5.
- Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited.
- Sandefur, R. "Access to Justice: Classical Approaches and New Directions." In *Access to Justice*, edited by Rebecca L. Sandefur. *Sociology of Crime, Law, and Deviance*, Volume 12. Bingley, UK: Emerald/JAI Press.
- Sherman J. (2013) "Court Information Management Policy Framework to Accommodate the Digital Environment", Discussion Paper for the Canadian Judicial Council.
- Sherman J. (2013) "Court Information Management Policy Framework to Accommodate the Digital Environment", Discussion Paper for the Canadian Judicial Council.
- Simon, H.A., Smithburg, D.W. and Thomson, V.A. (1961) *Public Administration*, NY: Alfred A. Knopf.
- Simshaw, D. (2018). Ethical Issues in Robo-Lawyering: The Need for Guidance on Developing and Using Artificial Intelligence in the Practice of Law. *Hastings Law Journal*.
- Skeem, J. L., & Monahan, J. (2011). Current directions in violence risk assessment. *Current Directions in Psychological Science*, 20(1), 38-42.
- Skeem, J., & Eno Loudon, J. (2007). Assessment of evidence on the quality of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS). *Unpublished report prepared for the California Department of Corrections and Rehabilitation*. Available at: <https://webfiles.uci.edu/skeem/Downloads.html>.

- Staats, J.L., Bowler, S. and Hiskey J.T. (2005) "Measuring Judicial Performance in Latin America", *Latin American Politics & Society*, Volume 47, Number 4.
- Sussan, F., Autio, E., & Kosturik, J. (2016). *Leveraging ICTs for Better Lives: The Introduction of an Index on Digital Life*.
- Susskind, R. E. (2017). *Tomorrow's lawyers: An introduction to your future*. Oxford University Press.
- Velicogna, M. (2007). Justice systems and ICT-What can be learned from Europe. *Utrecht L. Rev.*, 3, 129.
- Velicogna, M. (2018). e-Justice in Europe: From national experiences to EU cross-border service provision. In *International E-Government Development* (pp. 39-72). Palgrave Macmillan, Cham.
- Velicogna, M., & Lupo, G. (2017, December). From drafting common rules to implementing electronic European civil procedures: The rise of e-CODEX. In *From common rules to best practices in European Civil Procedure* (pp. 181-212). Nomos Verlagsgesellschaft mbH & Co. KG.
- Wallace, A. (2003) "Overview of Public Access and Privacy Issues", paper delivered at Queensland University of Technology conference, 6 November 2003.
- Waterman, K. K., & Henshon, M. T. (2008). What's Next for Artificial Intelligence and Robotics? *Scitech Lawyer*, 5(1), 20.

Open Access

This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.