Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Avenida Universidad, 8 – Apdo. 28
20560 Oñati – Gipuzkoa – Spain
Tel. (+34) 943 783064 / opo@iisj.net / https://opo.iisj.net

Risk and danger in the introduction of algorithms to courts: A comparative framework between EU and Brazil

OÑATI SOCIO-LEGAL SERIES FORTHCOMING: NIKLAS LUHMANN'S SYSTEMS THEORY AND SOCIOLOGY OF LAW
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL.1859
RECEIVED 27 SEPTEMBER 2023, ACCEPTED 22 DECEMBER 2023, FIRST-ONLINE PUBLISHED 18 JANUARY 2024

LUISA HEDLER*

Abstract

In a context where public debate regarding technological advances has the potential to deeply impact the functioning of courts of law, both academics and practitioners regularly employ the concept of risk, which has a prominent role in both academic discourse and regulation attempts regarding this matter. Through a qualitative content analysis of the European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environments, as well as the Brazilian Resolution n. 223/2020 of the National Council of Justice, which address the same issue, I compare the EU normative responses to the possibility of introducing algorithms to Courts to their heavily inspired Brazilian counterparts, especially highlighting the commonalities on how risk is communicated about through the documents.

Key words

Risk; algorithms; court management; systems theory

Resumen

En un contexto en el que el debate público sobre los avances tecnológicos tiene un profundo potencial de impacto en el funcionamiento de los tribunales de justicia, tanto académicos como profesionales emplean habitualmente el concepto de riesgo, que tiene un papel destacado tanto en el discurso académico como en los intentos de regulación en esta materia. A través de un análisis de contenido cualitativo de la Carta Ética Europea sobre el uso de la inteligencia artificial en los sistemas judiciales y sus

* Luisa Hedler holds a PhD from the Department of Business, Humanities and Law at Copenhagen Business School. She holds a LLM in International Human Rights Law from Lund University, and a Bachelor of Laws from the University of Brasília. Her current project utilises a systems theoretical approach to analyse the introduction of algorithms in courts of law. Her current research interests include sociology of law, sociology of childhood, Science and Technology Studies (STS), international human rights law. Email: luisa.hedler@gmail.com

entornos, así como de la Resolución brasileña n. 223/2020 del Consejo Nacional de Justicia, que abordan la misma cuestión, comparo las respuestas normativas de la UE a la posibilidad de introducir algoritmos en los tribunales con sus homólogas brasileñas, fuertemente inspiradas, destacando especialmente los puntos en común sobre cómo se comunica el riesgo a través de los documentos.

Palabras clave

Riesgo; algoritmos; gestión de tribunales; teoría de sistemas

Table of contents

1. Introduction

Technology is developing at a fast pace, with the speed of changes outpacing society's capacity to anticipate and react to them. The legal system – already described as following a slower rhythm than general society (Ost 2005) – is also affected by these technological changes. From the discussion about the legality of lawyers using stable-diffusion AI software to write their petitions, to online automated dispute resolution, to debates on bias and discrimination in automated risk-assessment in the criminal system, much has been said, written and tentatively regulated about this issue.

In this scenario, it is not surprising that a considerable amount of public discussion around algorithms and AI revolves around the issue of risk. Whether it is by industry executives and billionaires urge for a halt to the development of AI generative models because of "potential risks to society" (Hart 2023), or discussions in the European Parliament about how to define "high risk AI" (European Parliament 2023), the potential of future harm in different sectors of society is at the centre of considerations in decision-making regarding how these new technologies should regulated (Veale *et al.* 2023). When it comes to courts of law, this discussion concerns the extent to which tasks can be delegated to algorithms. Between automatic sorting of incoming court cases, relevant jurisprudence retrieval, detection of procedural admissibility, risk-assessment of criminal offenders and even automated decision-making, what are the limits to what and how courts are allowed to incorporate algorithms into their functioning?

Considering the centrality of risk in current legal debates, in this paper I will make use of Niklas Luhmann's conceptualization of risk to analyse the current normative frameworks around the implementation of algorithms in courts of law, especially comparing the European Union and the Brazilian regulatory frameworks. In this sense, I ask: *how do European and Brazilian regulation attempts of AI in the Judiciary deal with the concept of risk?* I find that the regulatory responses to the incorporation of algorithms into the legal system are attempts at reducing complexity that transform the unknown danger of algorithms into manageable risk. Luhmann's distinction between risk and danger is a useful prism through which to understand these attempts, providing further insights on the pitfalls of algorithmic regulation, where algorithmic opacity and the harm of discriminatory outcomes can potentially re-introduce dangers into the legal system.

In order to concretely illustrate the contributions of the systems theory concept of risk to the debate on the impact of technological developments in the legal system, I will analyse and compare two different documents that address the issue of the use of Artificial Intelligence withing the Judiciary. The first one, pertaining the EU sphere, is the European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (henceforth the Charter) (CEPEJ 2018). While the Charter is not immediately enforceable or directly translatable into European national legislation, it engages with European legal principles in order to grapple with how judiciaries can incorporate algorithms, and has served as an ample source of inspiration for the second document which will be analysed. The Brazilian National Council of Justice's resolution n. 332/2020, which regulates the use of Artificial Intelligence in the Brazilian Judiciary, was, as said, directly inspired by the Charter, but is able to be more direct and specific, as it internally regulates the development and use of AI in the Brazilian judiciary.

While the main focus of this paper is on the use of the distinction between risk and danger in both normative texts, it takes heed of the context-sensitivity of legal comparative analysis (Adams 2011) in order to draw out the distinctiveness of each document, as well as address differences in language. Both texts were submitted to qualitative content analysis, that is, by reducing the totality of the data in order to identify themes and extract meaningful interpretations (Roller 2019). In this sense, I have submitted both documents to thematic, theory-oriented coding, and extracted every passage that either contained the word "risk" or associated terms, as well as passages in which the communication fit the general pattern of engaging with the possibility of future harm.

The comparison between the European and Brazilian normative frameworks is made possible through their similarity in content, and interesting through their differences in focus and enforcement possibilities, where the latter can be specific while the language of the former has do adopt a more restrained posture. The combination between the strong inspiration and similarities with the added concrete dimensions provided by the Brazilian examples provides additional dimensions in exploring how risk can be communicated about, reinforcing and illustrating the potential of systems theory in capturing complex phenomena across geographical borders.

This paper will begin, in section 2, by contextualising the introduction of algorithms to Courts, followed by a more detailed description of the documents that will be analysed. The theoretical framework of the distinction between risk and danger will be introduced in section 3, placing the discussions surrounding the concept of risk into context. After a brief review of different approaches to risk in the literature of law and technology in section 4, I will proceed to the analysis of the aforementioned documents in section 5, before the conclusion.

2. Regulation of the introduction of algorithms to courts

Considering the introduction of new technologies is a process deeply rooted in the specific contexts in which they operate, this section starts by describing and exploring the different approaches, in Europe and Brazil, to situate the documents that will be the object of analysis.

While the expansion of digitalization and the use Information Technology to measure, quantify and predict different aspects of society has not left Courts and the legal world untouched (Reiling 2020), there is currently no unified approach, especially at an international level, with how algorithms are introduced within a legal system, and how far the automation of tasks or introduction of algorithms is allowed to proceed. There is a big variety across the globe regarding which institution(s) initiates the process, how centralized or fragmented the process is, as well as which types of entities – public service, universities, private initiative- are most involved in the process (Hedler 2023). Aside from these differences, which can be the object of intense political and legal debates, there are a few material considerations that affect the technical feasibility of utilizing natural language processing to make legal data readable, and subsequently train algorithms. The size of a given legal system – in terms of how many cases can be used to train algorithms – is, for example, a relevant factor (Kokol *et al.* 2022), which

consequently makes larger jurisdictions more likely to successfully develop such models.

With these considerations in mind, the diversity of approaches that can be found in the European Union is not surprising when it comes to digitalization and implementation of algorithms in different parts of their legal systems. According to the latest report of the European Commission for Efficiency of Justice (henceforth CEPEJ)[1] in 2022, there is ample variance between member-States when it comes to the digitalization of the judiciary and the spread of the use of Information and Communication Technology (ICT), which are the building blocks upon which algorithms can be developed. There were different levels of investment and amount of budget reserved for the development and maintenance of technologies, for example. While the ICT development of most states was centralized, 63% of them still outsourced at least part of their initiatives to the private sector. When it comes to regulating the matter, two main approaches were identified: while countries like Latvia and Finland chose an experimental approach, introducing new technologies in a smaller scale and "testing it out" before starting to issue legislation on the matter, countries such as Italy and France required the pre-existence of regulation before any new technology could be used within the scope of the judiciary (Council of Europe – CEPEJ – 2022, p. 115).

On the other side of the Atlantic, Brazil, despite being only one state, had a de-centralized and diverse start in the technological development in their Courts of Law. Within a context of accelerated extension of internet services and digitalization of government, the Brazilian Judiciary has developed their digitalization and automation at their own pace and as independent, internal initiatives. Whereas there are possibilities of collaboration and institutional learning,[2] the budgetary and administrative independence afforded to the Brazilian Judiciary[3] creates an environment in which not only the Judiciary, but each Federal or State administrative unit has an independent budget and administrative competence to promote initiatives that are geared towards the improvement of activities related to their finality (Conti 2019, pp. 169–171).

In this sense, when initiatives of the digitalization of the Judiciary began, in the early 2000s, they were developed by internal initiatives of the Courts, deploying their own IT resources in a de-centralized way, and further initiatives of automation or employment of algorithms began much in the same way. This scenario only changed in 2020, when a technical cooperation between the National Council of Justice (CNJ), The Federal Council of Justice (CFJ) and the UN Development Fund (UNDP) launched a centralizing program to increase the interoperability between courts. In this sense, the case of Brazil is not an isolated oddity in terms of digitalizing and implementing algorithms in public service, but rather part of a global trend. While there are some peculiarities about the Brazilian Judiciary that might make its members especially keen on implementing

[1] The CEPEJ was created by the Council of Europe in 2002. It is the international commission that measures, reports and provides guidelines for the use of technology in the Judiciary for its members, among other things.

[2] The extensive institutional history documents highlight a technical visit between the Planning Ministry staff and the developers of the caseload management project in the Judiciary of the State of Sergipe, for example.(Governo Digital 2019).

[3] As guaranteed by art. 99 of the Brazilian Constitution.

algorithms[4], the main possibility of comparison of the European and Brazilian legal frameworks of on the introduction of algorithms to Courts is especially relevant when it comes to the nascent and developing normative frameworks.

In Europe, the CEPEJ, aside from measuring and reporting on technology in the Judiciary, has also adopted the first international legal document on the subject, when the Council of Europe adopted the "Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" in December 2018. This document, which is structured around European legal principles, attempts the balance between the promises of efficiency and quality improvements with the guarantee of fundamental rights (CEPEJ 2018). The Charter does not provide any sanctions or list any prohibitions, but rather communicates in terms of ethical principles that should guide the use of AI in judicial systems, derived from the legal basis in the European Convention on Human Rights and the Council of Europe Convention on the Protection of Data.

A few years later, in Brazil, this document was one of the main inspirations for the development of the CNJ's Resolution no. 332/2020, entitled "on ethics, transparency and governance in the production and use of Artificial Intelligence in the Judiciary" (Resolução n. 332/2020). While the CNJ is a supervisory organ of the Judiciary, it has based the competence to issue regulations in this matter as it pertains to fulfilling the principles of public administration, as present in art. 103-B, § 4º, II, of the Brazilian constitution (1988). In this sense, the CNJ is constitutionally authorized to regulate the Brazilian Judiciary's use of AI, especially considering that there was no general law on the matter at that time. As a piece of domestic regulation, resolution no. 332/2020 is afforded a level of specificity and enforceability that the Charter does not have, such as the possibility of prohibiting certain practices or enforcing consequences and direct rules for the Brazilian judiciary.

While these two documents will be the main objects of analysis, they are not the end-step in terms of regulating the use of AI in the Judiciary, neither in Europe nor in Brazil: A more binding attempt to regulate AI in Europe – including, then, its usage in Courts – is still under discussion in the European Parliament. The proposal of the AI Act was presented by the European Commission in April of 2021. This particular bill sets the issue of risk at the centre of AI regulation, dividing AI-related risks into the four categories of minimal risk, limited risk, high risk and unacceptable risk, the latter of which would be entirely prohibited (Chamberlain 2022, p. 1).

As for general AI legal developments in Brazil, there have been bills attempting to tackle the matter going as far back as 2019, but the most current effort is the PL 2.338/2023. It is the based on the report made by a working group of jurists who worked throughout 2022, and explicitly aligned with EU principles, as well as being attentive to OCDE and UNESCO[5] guidelines in the matter (Possa 2023). It repeats the risk pyramid presented by the EU, with almost identical classifiers of the "unacceptable risk" category, for example. In regards to the Judiciary, art. 17 VII of the bill classifies AI applications that

[4] As I have explored more detail in previous work (Hedler 2022), an enormous, stagnated caseload and the insufficiency of previous legal reforms were perceived, by the Brazilian Judiciary, as a main driver for supporting technological developments as the main strategy to address what they called the "numerical crisis of the Judiciary".

[5] For more information on these particular guidelines, see Veale *et al.* (2023).

are applied to "administration of justice, including systems that assist judiciary authorities in the investigation of facts and application of the law" as high risk (Projeto de Lei 2338).

3. Risk and danger

Whether in parts of a general AI legislation, or in detailed principles of implementation of algorithms in the judiciary, analysing the ways risk is communicated about demands a better conceptual understanding on the system theoretical approach on risk. In this section, I will introduce the concept of risk, situating its central character in contemporary social debate, and give special attention to Niklas Luhmann's definitions, which will be used as the theoretical framework for the analysis. After explaining the relevance of applying the distinction between risk and danger to the introduction of algorithms to courts, I finish the conceptual chapter with a brief note on the language differences in the data, and their impact in dealing with the concept of risk.

Defining risk can be a complicated endeavour, considering that it is a common word which is used in a multiplicity of contexts (Battistelli and Galantino 2019). In general terms, risk is used to conceptualize the possibility of a negative outcome in the future, which is associated with the possibility of acting against or towards it (Renn 2008, p. 50). In this general approach, Ortwin Renn isolates three main elements: the likelihood of the negative outcome; the impact of said outcome in relation to the values in society; and the specific context in which this outcome may happen (Renn 2008, pp. 50–51).

In the context of introducing algorithms to courts, then, there are many different ways to mobilise the concept of risk. As Battistelli and Galantino assert, natural and technical sciences focus more on the first element, which includes the probabilistic, numerical calculation of how likely something is to happen. This type of operation is known as "risk analysis" (Battistelli and Galantino 2019, p. 66), which is precisely the task that risk-assessment algorithms perform, for example, which use enormous amounts of data to calculate the probability of a certain outcome – for example, algorithms that calculate the likelihood of a criminal reoffending as a tool to assist judges in making decisions about arrest or parole.

A more sociology-focused viewpoint, however, can focus more on the context in which risk appears (Battistelli and Galantino 2019, pp. 66–67). In the current context, analysing the context under which "risk-assessment" algorithms are used in Courts, and whether their use produce negative outcomes, such as racial discrimination (see, for example, Ugwudike 2020), or whether it represents a "solutionist"[6] approach to the issues of risk-assessment in Courts (see, for example, Mölders 2021).

This notion of risk, according to Niklas Luhmann, started becoming relevant in the historical moment where society started considering that some advantages could only be achieved if something was at stake – namely, in the transition between Middle Ages and Modernity, with the enormous risks associated to inter-continental maritime commerce (Luhmann 1991). Ulrich Beck, in his seminal work entitled "the risk society", posits that, despite the concept being present in society for many centuries, the growing

[6] Solutionism, in a few words, is an over-reliance on technology in order to solve problems that have complex social dimensions (Mölders 2021).

uncertainties that characterized the Zeitgeist of the post-Second World war has pushed the world into a new phase of modernity that is entirely centred around risk and risk-management (Beck 1986). His work has been quite influential both in sociological academic circles (Rasborg 2021) and public debate (Martins 2015). This is evidenced by the prevalence of the concept of risk in many different areas, varying between management of natural hazards, working conditions and worker's protection, crime prevention and punishment, leisure, terrorism and, of course, the implementation of new technologies (Renn 2008). The main theoretical pillar of this paper, however, will be Niklas Luhmann's concept of risk from his book "sociology of risk" (Luhmann 1991), written as a response to Beck's book (King and Thornhill 2003, p. 184).

While Beck (as well as the most common interpretations of risk) considers that there is a dual distinction between "risk" and "safety", or "risk" and "certainty", he argues that post-war society is characterised by the predominance of uncertainty, which makes the concept of risk more socially relevant (Rasborg 2021). Luhmann disagrees, asserting that uncertainty has always been present in human history, and attributes the changes to how society internalizes and deals with those uncertainties, communicating about it differently (Luhmann 1991). After all, even when there is a decision between a "risky" and "safe" option, he argues, there is still a dimension of risk in choosing more certainty, when there is a perception that the rewards of the less safe options will be lost (Luhmann 1991). Instead of opposing risk and certainty, then, Luhmann argues for a differentiation between risk and danger to characterize the differences in how people communicate about a constantly uncertain world.

In this sense, both risk and danger are ways of communicating about future negative outcomes, and what differentiates them is how much they are affected by human decision-making. Dangers occur when an external force is observed to cause the negative outcome, where the system has no control, while risk presupposes some form of decision-making that contributes to the future harm (Luhmann 1991). For example, the possibility of total annihilation of humanity caused by some astronomical object colliding with Earth (which can be arguably said to be a negative outcome) has been communicated about as a danger for most of human history, where there is no possibility of influencing the movements of astronomical objects. However, with the advent of space exploration and the development of rockets and powerful weapons, not to mention the growing capacity to observe, measure and even predict the movement of astronomical objects, the reaction to the possibility of an extinction event can be communicated about as risk, where there are relevant decisions that can be made. In summary, the expansion of communication in terms of risk is related to the increasing knowledge and complexity within a society, so more and more aspects of life (and death) can be attributed to decision-making, and therefore seen as risks. This does not increase or decrease the amount of uncertainty present - the extinction of humanity can happen both as a risk or a danger – but the way that uncertainty is communicated about is different. It can be, in the case of danger, uncontrollable and external, or, as in the case of risk, as a result of decisions.

As the example illustrates, the difference between risk and danger is positional and subject to change, as what is perceived as external danger from one point of observation, can be observed as the result of decision-making from another perspective. Going back

to the extinction event, certain governments and their space agencies could be able to communicate about approaching meteors as a risk, while apple farmers still regard large objects falling from the sky as a danger. Or, in more relevant terms, when a certain court of law starts using an algorithm to group cases for mass litigation – as it already happens in Brazil – and a case gets misclassified, the IT workers of the Court can observe this occurrence as a risk, as they influence the choice of algorithm and testing thereof. From the perspective of the lawyer in this case, however, the misclassification of the case can still be understood as a danger, as there might not be sufficient knowledge about said algorithm in order for the lawyer to make relevant decisions that could affect whether the case gets misclassified or not. However, if a new petition-writing technique is invented which shows to have a smaller rate of misclassification by the court's algorithm, the decision to use this technique (and therefore mitigate the likelihood of the negative outcome) would place this misclassification as a risk from the perspective of the lawyer.

In summary, risk is a particular way of observing decisions (Luhmann 2018, p. 134), with the temporal dimension of bringing the indeterminate future to the present by binding it with a choice, with the potential of causing – or not – the projected harm. In this sense, the legal documents which are the object of analysis contain many instances of "risk communication" (for a more detailed explanation of risk as communication, see King and Thornhill 2003, pp. 184–185), that is, where the CEPEJ and the CNJ (Brazilian National Council of Justice) communicate about something being seen as a potential source of negative outcomes that can be attributed to decision-making, especially from the judiciary. The difference between risk and danger, used as a category of analysis, gains further relevance when considering the possibility of new technology bringing multi-referentiality to the legal system, that is, when a system starts internally communicating about issues beyond what is considered typical of the legal system. On risk communication, King and Thornhill explain:

> From within a system risks may be identified and taken into account in system communications. Risks are in effect possibilities of future loss which the system is able to see and 'understand'. Dangers, by contrast, represent the contingency of the system, the unknown, the possibility of future loss occurring not within the system's environment. Events which occur outside that environment are necessarily seen by the system as dangers, that is as occurrences which are beyond the reach of the system's code and programs, and which there is no possibility of the system being able to anticipate. (King and Thornhill 2003, p. 186)

Therefore, identifying which factors are considered risks (and therefore subject to decision-making) is helpful in mapping how attempts at regulating technology describe the employment of new technologies in the judiciary. In this sense, it is important to differentiate when factors are described as dangers, and therefore outside the institutional scope of decision-making of the Judiciary (such as budget limitations imposed by Parliament), or as risks (for example, when the CNJ authorizes the use of a certain machine learning model, thereby placing any harms caused by the model as a result of decision-making).

When it comes to the different languages involved in the analysis and their impact on the use of the risk/danger distinction, the English translation of official documents in the European framework make it easier to avoid misunderstandings, dealing with a Portuguese-speaking jurisdiction invites further clarification regarding translations and

mistranslations. While Luhmann's use of "risk" and "danger" does not deviate significantly to common ways the English language uses them (Boholm 2012), translations of this work by Portuguese (via Spanish) use the words "risco" and "perigo" (David 2011) to translate the system theoretical concepts. While there is some specialized use for "risco" and "perigo" when it comes to specific labour safety technical terms,[7] in general there are no specific translation issues that emerge in a Portuguese-speaking context.

4. Risk and algorithms

After clarifying the concept of risk, and especially the distinction between risk and danger, this section will use these distinctions to make a brief overview of the law and technology literature, and see where risks (and dangers) more often emerge. This brief review serves not only to situate the current debate, but to delineate arguments that the two algorithmic regulation documents engage with. Literature in law and technology, after all, is mainly concerned with projecting the consequences of the use of technology into the future, constantly engaging with the possibility of undesirable outcomes. In this sense, they engage in communicating about risk (or danger) when pointing out how the decision to use certain algorithmic tools could lead to some form of expected harm.

In the context of assessing how "smart technologies" interact with fundamental rights, Mireille Hildebrandt warns against the premature usage of "risk", as there would be too many unknown factors which could be a-critically absorbed through the probabilistic calculations incurred by the framework of "risk". Instead, she prefers to refer to them as "threats" (Hildebrandt 2016, pp. 77–78). The focus on the amount of knowledge about the expectation of future harm, in this paper's theoretical framework, would rather describe this situation as danger, and Hildebrandt's insight points towards one of the effects of shifting between the two concepts: how conceptualizing something as a risk (that can be decided upon, communicated about, and managed through decision) can obscure the extent to which there are still unknown factors that can appear as dangers. Ugwudike's (2020) analysis of risk assessment algorithms is an emblematic example: while many risk-assessment algorithms were specifically designed with "race neutral" parameters in order to avoid racial discrimination (managing it as risks), they continued to produce racially biased outcomes. Her conclusions point towards the lack of scrutiny and regulation in the selection and analysis of the datasets, and the choice of variables that represent the risk predictors – which, from the point of view of a court of law or a regulator, is still a danger.

As for the role of the legal system in society's assessment of new technologies, Lyria Bennett Moses, among others (Maas 2019, Ranchordás and Van't Schip 2020) highlights the role of the legal system in minimizing risk-generating situations in society in general (Bennett Moses 2016), including negative outcomes generated by the use of new technology. In this sense, the timing of regulatory intervention – especially considering the amount of knowledge about the negative effects of technology – follows the pattern

[7] In labour safety terms, the term "danger" is mainly used to denote the natural or social phenomena that, by themselves, have the potential to generate harm, and risk happens when the worker has the potential of encountering that "danger". So in that sense, a poisonous chemical is a danger, but risks happens when a worker has to handle that material.

in the Science and Technology Studies (STS) classic of the Collingridge dilemma (Collingridge 1980). It states that any attempt to regulate technology, if done too early, generates the risk of a mismatch between regulation and the harm it seeks to prevent, due to the insufficient knowledge on the matter. On the other hand, if the timing of regulation is delayed until there is sufficient information (or, as Hildebrandt puts it, when vague "threats" becomes measurable "risks"), it generates the risk that the technology has been entrenched in society in such a way that makes it difficult to successfully mitigate its negative effects through regulation.

Roger Brownsword (2019), in his assessment of the effects of technology on the legal system, observes how technology can appear to the legal system as a disruptive danger, which can go beyond creating new situations to which existing legal responses are ineffective (such as classic contract law in face of mass consumptions and terms of service of tech giants), but can potentially make law, as a normative response, unable to address the harms caused by algorithms in society. Applying a system theoretical outlook on the legal system[8], that would mean that new technologies could go from irritants to the legal system, prompting the changes of legal categories, but could outright impede law's function of stabilizing normative expectations (Luhmann 1989).

Further focusing on the specific use of algorithms within the legal system, the use of risk, coming from different departure points, is abundant in the literature. Firstly, there is the issue of algorithmic risk-assessments, where risk calculation is both at the heart of the automated activity, and at the evaluation of potential negative impacts that their use can generate (Ugwudike 2020, Berk *et al.* 2021, Derave *et al.* 2022). In a more general perspective, there are several appraisals of different types of risks of incorporating new technologies to the legal system. Susser (2019), in a wide argument that could apply to many organisations, highlights the risks associated with technologies becoming "invisible" to users, obfuscating knowledge and generating loss of critical thinking regarding the automated tasks. In this sense, an algorithm that selects relevant jurisprudence for a case could come to be relied upon as the only jurisprudence possible for the case, leading to a loss of creative thinking, and to a path dependency towards the particular selections of that algorithm.

Gowder (2018), after acknowledging the potential of extending legal thought to areas where it was previously inaccessible (thereby implicitly introducing the risk of not choosing to use technology to do so), does pragmatically warn about the possibility of using algorithms to produce cheaper, but lower quality legal services to the population. From the specific point of view of lawyers, he highlights the aspects of the legal profession which are not included in automation, highlighting the risk of epistemic losses. Regarding wider consequences for the rule of law, Pasquale (2018) highlights the risks of undermining with technological advancements, especially in terms of epistemological incompatibilities (Pasquale and Cashwell 2018), even leading to the potential of misuses of the rule of law and due process (Citron and Pasquale 2014). As

[8] In a few words, Luhmann defines law as a social system that has the function of stabilising normative expectations (Luhmann 1989), which maintains itself by resisting disappointments from the environment (for example, that homicides are still illegal despite murders happening in society). For a more detailed explanation, see chapter 1 of this Special Issue.

an actionable response, Hildebrandt (2016) advocates for the incorporation of rule of law precepts into the design of new technologies as a measure of risk-mitigation.

Specifically focusing on epistemological concerns – as well as their political implications when interacting with the legal system – is another relevant area of identifying algorithmic risk. Kitchin (2014) focuses on the implications of relying on technologies that represent the world by the use of "big data", which relies on correlation rather than causation, as it becomes a dominant way of knowing. Esposito (2013) goes further in specifying how the non-causal *modus operandi* of algorithms presents risk, drawing parallels between algorithmic and oracular truth. The specific epistemological risk being addressed by these authors is the abandonment of causality, which is a building block of many parts of the legal system. More concretely, Danaher (2016) conceptualizes the harmful negative outcome as "algocracy", a governance system in which "algorithms structure and constrain the ways in which humans within those systems interact with one another, the relevant data, and the broader community affected by those systems". This could lead to limiting the scope of human freedom, and include risks to the erosion of democracy (Hildebrandt 2017).

A wider epistemic risk is explored by Alain Supiot (2017, p. 169), who focuses specifically on how normative uses of quantification have the effect of disconnecting the world from its material existence, causing an over-reliance on representations – quantitative and numerical – where the biggest risk is of a growing distortion of these representations. In this sense, the institutional incorporation of algorithms that assess the procedural admissibility of incoming cases, for example, could lead to the situation where cases which would be clearly admissible if assessed by a judge could end up being rejected without a chance of re-dress.

Finally, while the ultimate risk (especially from the point of observation of legal professionals), or, for some, ultimate aspiration of law and technology (Goldsworthy 2019) is the possibility of "legal singularity", that is, the possibility that the judiciary would be able to be partially or completely substituted by machines(Cobbe 2020). While this last possibility might seem far-fetched both from technical and political standpoints, the articulation of the singularity argument as a risk might be common enough in public discourse to keep in mind when considering the ways these regulatory attempts, that will be analysed in the next section, incorporate notions of risk in the text.

5. Risks and dangers in the introduction of algorithms to courts of law

With all those different outlooks on how risks emerge when algorithms are incorporated into the functioning of the legal system, it is not surprising that attempts at normative responses would incorporate, in part, at least a few of them. In this section, I will highlight the appearance of risk in the specific legal documents that regulate the incorporation of algorithms in Courts – that is, the European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (CEPEJ 2018), and the Resolution n. 332/2020 of the CNJ, which concerns ethics, transparency and governance in the production and use of Artificial Intelligence in the Judiciary.

The titles of the documents already highlight both the similarities in general intent, and the slightly different focus on addressees and scope: while the CEPEJ addresses member-states in their multiple points of observation – hence the broader object of "judicial

systems and their environment" – the CNJ document is circumscribed to the Judiciary branch of the State, and therefore is able to be more specific, adding the dimensions of transparency and governance. The use of "production and use" specifically reflects the active participation and control that the Brazilian judiciary has of the technologies they create.

The general structure of both documents also differs in structure and language: while the normative part of the CEPEJ charter consists of five principles, there are 4 appendixes that provide the addressees with further information about current (as of 2018) uses of AI in Courts, recommends types of uses that should be encouraged our discouraged, presents a glossary and suggests a checklist for integrating the charter's principles into processing methods when developing algorithms (appendix 3). In contrast, the CNJ resolution is a legal document, which starts with a preamble stating the general context and main goals of the document, followed by 30 articles of text in concise, prescriptive language. Aside from describing general principles (which are explicitly inspired by the CEPEJ Charter), it details how the principles are to be implemented, describes the structures that will control their implementation, and establishes the competency to supervise, correct mistakes and, if necessary, punish those responsible for non-compliance.

The CEPEJ Charter, which is directed towards "public and private stakeholders responsible for the design and deployment of artificial intelligence tools and services that involve the processing of judicial decisions and data" (CEPEJ 2018, p5), is structured around five main principles, that are to be regularly applied, monitored and evaluated by public and private actors (p.6). They are: (1) the principle of respect for fundamental rights; (2) principle of non-discrimination; (3) principle of quality and security; (4) principle of transparency, impartiality and fairness; (5) and the principle "under user control".

Seen through the angle of risk, each of these principles reflect the expectation of future harm that might be caused if actions are not taken (in this case if the principle is not implemented/respected). From the perspective of the CEPEJ, therefore, they structure it around principles that, if followed, would allow the State employing algorithms to avoid the harms caused by the "risk-shadow" of the Charter. The algorithms might, then, (1)be somehow incompatible, or disrespecting to fundamental rights ; (2) develop or intensify already existing discriminations between individuals and groups; (3) be based on data collected in a suboptimal way, with inappropriately conceived models, leading to security breaches; (4) have opaque and unfair data processing methods which benefit a few groups more than others; (5) and that users lose control of their choices, and have incomplete or bad information about how the systems are being used.

This is illustrated in the way the principles are described, on page 7 of the Charter (CEPEJ 2008). Taking the first principle as an example: "Principle of respect for fundamental rights: ensure that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights", pointing towards the possibility of future harm if it is not followed. While further explaining the content of the principle, the forecast of potential negative outcomes becomes even more specific:

> When AI tools are used to resolve a dispute or as a tool to assist in judicial decision-making or to give guidance to the public, it is essential to ensure that *they do not*

> *undermine the guarantees of the right of access to the judge and the right to fair trial (equality of arms and respect for the adversarial process).* (CEPEJ 2018, p. 8, emphasis added)

These descriptions echo the concerns in the literature, as well as the risk-management suggestions pointed out subsequently: "Preference should therefore be given to ethical-by-design or human-rights-by-design approaches…" (CEPEJ 2018, p. 8), which can both be observed as directed to technology developers and regulating authorities that could regulate and mandate the use of such an approach.

Similarly, the Resolution n. 332/2020 of the CNJ, identifies several risks of the utilization of algorithms in the Judiciary, as it enumerates legal principles with the intent of avoiding future harm. The second to seventh chapters of the resolution mirror almost exactly the five principles of the CEPEJ chapter, only with a few minor differences in chapter division. Following on the previous example of the notion of respect to fundamental rights, Article 4 of the Resolution states "In the development, implantation and use of Artificial Intelligence, Courts will observe its compatibility with Fundamental Rights, especially those inscribed in the Constitution or International Treaties to which the Federative Republic of Brazil is part of.[9] It still reflects the same "risk-shadow" of algorithms which are not compatible with fundamental rights, and seeks to minimize this risk by adding the requirement that Courts assure this compatibility in every step of the "life-cycle" of the new technologies.

Aside from the five principles, as previously mentioned, the CEPEJ charter details, in Appendix 2, which uses of AI in European judicial systems should be encouraged, avoided, or only allowed after very careful consideration – organizing them according to the magnitude of risk that they present, and in some level resonating with what would later become the AI Act in separating levels of risk. In this sense, while data-visualization, research "case-law enhancement", and chatbots that facilitate access to law are recommended without many reservations by the CEPEJ, it is possible to derive how deciding to employ certain uses of new technologies could present risks – and how they relate to the risks implied by the five principles. For example, in the matter of offering "predictive justice" tools to support for alternative dispute settlement in civil matters (CEPEJ 2018, p. 65), the CEPEJ identifies risks of lack of transparency and bad quality of data, as well as the notion that quantitative data might be used uncritically without due considerations to the "causative factors" of certain decisions. Moreover, when it comes to using algorithms as risk-assessment tools in criminal matters, the CEPEJ classified it as "uses to be considered with the most extreme reservations" (CEPEJ 2018, p. 66) because of the high risk of racial bias, which would clearly go against the principle of non-discrimination. In this sense, the identification of risks provided in the charter point towards the possibility of being at odds with binding international legislation: that is, the European Convention on Human Rights and its fundamental guarantees.

Another interesting difference in the nuance of conceptualizing algorithmic risk is regarding the principle of non-discrimination. The CNJ goes beyond the possible scope

[9] As it pertains the hierarchic relationship between Brazilian domestic law and international treaties, art. 5, §3 of the Federal Constitution states that international human rights treaties ratified by Brazil have the equivalent legal status of constitutional amendment. As clarified by jurisprudence of the Supreme Federal Court of Brazil, this means that international treaties ratified by Brazil have a supra-legal, infra-constitutional status.

of the CEPEJ to not only affirm the preservation of equality and non-discrimination, it adds the dimensions of solidarity, plurality, and the objectives of creating conditions that minimize oppression, marginalization of human being and judgment errors that arise due to prejudices. In this sense, the CNJ not only refers to the algorithmic risk of producing unequal outcomes but orients the use of algorithms as a tool of managing biases and prejudices in non-algorithmic decision-making. In this sense, algorithms are represented not only as a source of risk, but as a potential irritation to the analogue Justice system, where there is an already identified risk of prejudices and biases. Additionally, the resolution, in art. 7 §3, mandates the discontinuation of use of any AI models where it is impossible to eliminate discriminatory bias. This sensitivity to the risk of bias also extends to measures about the research, development and implantation of new projects. Article 20 dictates that a diverse team, both in terms of gender, race, ability, sexual orientation and generation, among others, should be considered in all steps of the process, from research to implementation. The progressiveness of this measure, however, is promptly undercut by the pragmatic acknowledgment that the pool of candidates available within the personnel of the judiciary might severely limit the diversity of the profiles that get involved in the process.

When it comes to complying with requirements of transparency, the corresponding risk of opacity is fleshed out in every paragraph of article 8, which explains the concept: of a potential irresponsible width of sensitive data being made public (I), of the development of tools without a clear goal or benefit for the public (II), of the lack of documentation (or even existence) of identifying risks with every new application, and lack of preparation in facing potential security breaches (III), the lack of identification of the reason for any potential damage (IV), of the lack of auditing and certification (V), and the lack of possibility of human auditing (VI). In summary, detailing the requisites of transparency means that there is an awareness of decisions, by the part of developers and users of algorithms, that might cause opacity in different ways, and needs to be avoided.

The rest of the principle-related articles follow approximately the same pattern – strengthening and complementing the CEPEJ framework with more detailed instructions about how to develop, implement and use AI tools in the judiciary. They are especially sensitive to avoiding the possibility of epistemic losses or lack of agency as a risk of the use of algorithms, as exemplified by Art. 17:

> The intelligent system must assure the autonomy of internal users, with the use of models which:
>
> - Enable increment, and not restrictions;
> - Makes it possible for the decision proposal and underlying data to be revised, and without any binding effect.

A few specific uses are also singled out as to being discouraged or forbidden, such as facial recognition for the use of facial recognition, which would be only permitted under express authorization of the CNJ (art. 22, §2), or the use of AI in criminal matters, especially when it concerns predictive models (art. 23). The risk of constraining the *in dubio pro reo* fundamental principle of criminal law is especially addressed on article 23 §2, where calculations of risk of recidivism are forbidden of suggesting results that would be more punitive to the defendant than those made by judges. This particular

articulation of the risk is an especially interesting interaction between expectations of algorithmic risk and "human risk" when it comes to bias in criminal adjudication: it simultaneously acknowledge the potential of algorithms of irritating a legal system which is structurally biased (by making it possible for risk-assessment tools to suggest a course of action that is more favourable to the defendant, and potentially identifying biases in a judge), while also acknowledging the risk that the algorithm itself might internalize such biases and incorporate it in the risk-assessment itself.

The current document regulating the presence of AI models in the Brazilian Judiciary, as well as the Ethical Charter, reflect many of the risks raised by the literature, and is visible in their attempts at addressing risks such as opacity, bias, and even some efforts to prevent epistemic losses. The CNJ document, inspired by the European Charter, goes further into detail about the expected risks, as well as instituting more measures to address them. Aside from responding to perceived algorithmic risks, it also acknowledges and works with risks of bias that result from an "analogue", non-AI mediated jurisdictional activity, and envisions the employment of algorithms as one of the tools to address and minimize that risk.

In this sense, another commonality between the two documents is a very clear notion of the opposite risk in terms of missing out on the potential benefits of the use of algorithms, which can also be observed as a risky decision. Considering all the possible advantages that are enumerated at the preamble of both documents, (and with even further emphasis in the articles of the CNJ resolution), it also communicates about the potential future harm that might come with the absence of technologies that could be assisting in fulfilling the role of the Judiciary with efficiency, in both cases, and even with an enhanced sensitivity to discrimination and bias, as is highlighted in the Brazilian documents.

A crucial point of departure between the two documents lies in their positions in terms of liability for problems or mistakes originated from the use of said technologies. The European Charter generally avoids the issue, or, as is the case with the annex I containing the study of the use of AI in judicial systems, presents a multiplicity of possibilities in this regard. The CNJ's response, however, departs from the inspiration by firmly placing the responsibility very clearly in the developers/creators of the algorithms.

On the same note, when it comes to the common economic argument of over-regulation as an economically stifling force, the European Charter is more explicit at addressing this as a potential problem (Council of Europe – CEPEJ – 2019), while the CNJ seems to place much more trust in the regulating body – i.e. themselves – to find the right balance between innovation and regulation. It stands to reason that a commission of the Council of Europe, while observing the activities of many different judiciaries, would describe over-regulating as a risk to a greater degree than the public administration organ who is also charged with centralizing the pulverized technological developments.

In summary, despite their differences and nuances regarding their positioning within their respective legal orders, both documents engage with algorithmic risks through a multiplicity of angles: while the legal principles clearly include the projection of future harm in their descriptions, in a clear attempt at regulation as risk-mitigating measure, other types of risk are also identified in the documents. Firstly, there is the risk associated with *not* pursuing the technology, which is enunciated in preambles describing the

potential advantages to be gained with the use of new technologies, as well as the risks associated with the non-algorithmic mediated society, made explicit when both documents mention the use of algorithms in order to uncover discrimination and bias already existing within the Judiciary.

6. Conclusion

The use of algorithms in the Judiciary, for case management and decision-making assistance is part of a growing trend of using more and more technological "solutions" in public administration. Their use is intended to assist overburdened judiciaries with tasks such as increasing efficiency, promoting access to justice and even serving as a diagnostic tool to improve upon the failing of the system as it is now, reliant on humans. However, the decision to develop and employ these technologies come with many associated risks – if not dangers – that are extensively identified and listed by the literature, including the risk of stagnation and alienation of the legal system, lower quality of decisions, all the way to increased bias and discrimination which, to the people affected, can be perceived as dangers of arbitrariness.

In this scenario, both regulatory documents regarding the subject seem to be quite sensitive and responsive towards a plethora of risks already identified by the literature, while also responding to the unsaid risk of deciding *not* to use algorithms, and the expected future harm of missing out on potential improvements. Through the use of the language of fundamental rights, the potential harms can be classified as acceptable or unacceptable risks. While the CEPEJ document, because of its supra-national, non-binding and wide-scope, presents recommendations of more or less desirable uses, and a "compliance checklist" as a risk-mitigating strategy, in the case of Brazil, centralization and control in the hands of the CNJ is employed as a tool to transform the diffuse danger of change and disruption into a series of calculated steps of risks that are deemed acceptable.

In a framework of public discussion and legal drafts densely populated with concepts of risk, adopting a system theoretical approach allows for a flexible framework where the directionality and positionality of the concept become even more apparent, and can lead to fresh lines of inquiry by the identification of multiple lines of risk that go beyond utilizing regulation as ways of mitigating risk. Comparing the CEPEJ and CNJ documents, with their alignment in terms of principles and purpose, allows the insight into how the more general and non-binding language of international legal documents can be applied and further specified, as the CNJ did. The differing scopes between the documents further highlights the directionality of the concepts of risk and danger, showing how the change of addressee (public and private stakeholders in the former, and the judiciary in the latter), lead to variation in what can be decided upon, and therefore put in the sphere of risk.

Further research could be dedicated to observing how different points of observation (judiciaries, tech developing companies, private and public legal practitioners) would lead to perceiving algorithmic bias as risk, dangers or even threats; on identifying where and how the shift between risk and danger happens along different social systems when it comes to the introduction of new technologies. Considering how technology regulation aspires to mitigate the risks of new technology, it would be also especially

relevant to further study how the perspective of future harms is addressed in these legislative efforts as risk, and which other perspective harms are not captured, with the potential of the re-emergence of these factors as dangers.

References

Adams, M., 2011. Doing What Doesn't Come Naturally. On the Distinctiveness of Comparative Law. *In:* M. Van Hoecke, ed., *Methodologies of Legal Research: What Kind of Method for What Kind of Discipline?* London: Hart, pp. 229–240.

Battistelli, F., and Galantino, M.G., 2019. Dangers, risks and threats: An alternative conceptualization to the catch-all concept of risk. *Current Sociology* [online], 67(1), pp. 64–78. Available at: https://doi.org/10.1177/0011392118793675

Beck, U., 1986. *Risikogesellschaft. Auf dem Weg in eine andere Moderne.* Frankfurt am Mein: Suhrkamp.

Bennett Moses, L., 2016. Regulating in the Face of Sociotechnical Change. *In:* R. Brownsword, E. Scotford and K. Yeung, eds., *The Oxford Handbook of Law, Regulation and Technology.* Oxford University Press, p. 574.

Berk, R., *et al.*, 2021. Fairness in Criminal Justice Risk Assessments: The State of the Art. *Sociological Methods and Research* [online], 50(1), pp. 3–44. Available at: https://doi.org/10.1177/0049124118782533

Boholm, M., 2012. The Semantic Distinction Between "Risk" and "Danger": A Linguistic Analysis. *Risk Analysis* [online], 32(2), pp. 281–293. Available at: https://doi.org/10.1111/j.1539-6924.2011.01668.x

Brownsword, R., 2019. Law Disrupted, Law Re-Imagined, Law Re-Invented. *Technology and Regulation* [online], pp. 10–30. Available at: https://doi.org/10.26116/techreg.2019.002

CEPEJ, 2018. *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment* [online]. Strasbourg: Council of Europe. Available at: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment

Chamberlain, J., 2022. The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective. *European Journal of Risk Regulation* [online], 14(1), pp. 1–13. Available at: https://doi.org/10.1017/err.2022.38

Citron, D.K., and Pasquale, F., 2014. The scored Society: due process for automated predictions. *Washington Law Review* [online], 89(1), pp. 1–33. Available at: https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2/

Cobbe, J., 2020. Legal Singularity and the Reflexivity of Law. *In:* S. Deakin and C. Markou, eds., *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence.* Oxford: Hart, pp. 286–290.

Collingridge, D., 1980. *The social control of technology.* London: Frances Pinter.

Constitution of the Federative Republic of Brazil, 1988. Documentation and Information Center of the Chamber of Deputies.

Conti, J.M., 2019. *A autonomia financiera do poder judiciário* [online]. 2nd ed. São Paulo: Blucher. Available at: https://doi.org/10.5151/9788580394061

Council of Europe (CEPEJ), 2019. *European ethical charter on the use of Artificial Intelligence in judicial systems and their environment* [online]. Adopted at the 31st Plenary Meeting of the CEPEJ, December 2018, pp. 1–77. Available at: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

Council of Europe (CEPEJ), 2022. *European judicial systems CEPEJ Evaluation Report Part 1 - Tables, graphs and analyses, CEPEJ* [online]. Strasbourg: Council of Europe. Available at: https://rm.coe.int/cepej-report-2020-22-e-web/1680a86279

Danaher, J., 2016. The Threat of Algocracy: Reality, Resistance and Accommodation. *Philosophy and Technology* [online], 29(3), pp. 245–268. Available at: https://doi.org/10.1007/s13347-015-0211-1

David, M.L., 2011. Sobre os conceitos de risco em Luhmann e Giddens. *Em Tese* [online], 8(1), pp. 30–45. Available at: https://doi.org/10.5007/1806-5023.2011v8n1p30

Derave, C., Genicot, N., and Hetmanska, N., 2022. The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System. *European Journal of Risk Regulation* [online], 13(3), pp. 389–420. Available at: https://doi.org/10.1017/err.2022.5

Esposito, E., 2013. Digital prophecies and web intelligence. *In:* M. Hildebrandt and K. de Vries, eds., *Privacy, Due Process and the Computational Turn* [online]. London: Routledge, pp. 117–138. Available at: https://doi.org/10.4324/9780203427644

European Commission, 2021. *The EU Artificial Intelligence Act, The EU Artificial Intelligence Act* (COM(2021)206 final) [online]. Available at: https://artificialintelligenceact.eu/the-act/

European Parliament, 2023. *Press release AI Act : a step closer to the first rules on Artificial Intelligence* [online]. European Parliament News. 11 May. Available at: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

Goldsworthy, D., 2019. Dworkin's dream: Towards a singularity of law. *Alternative Law Journal* [online], 44(4), pp. 286–290. Available at: https://doi.org/10.1177/1037969X19875825

Governo Digital, 2019. *Do Eletrônico ao Digital, Estratégia de Governança Digital* [online]. Last updated 6 January 2023. Available at: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital

Gowder, P., 2018. Transformative legal technology and the rule of law. *University of Toronto Law Journal* [online], 68(Cl), pp. 82–105. Available at: https://doi.org/10.3138/utlj.2017-0047

Hart, R., 2023. Elon Musk And Tech Leaders Call for AI "Pause" Over Risks To Humanity. *Forbes* [online], 29 March, pp. 1–5. Available at: https://www.forbes.com/sites/roberthart/2023/03/29/elon-musk-and-tech-leaders-call-for-ai-pause-over-risks-to-humanity/?sh=5f5bbd136dfc

Hedler, L., 2022. Algorithms, Efficiency and the Two Faces of Courts – A Case Study of the Brazilian Superior Court of Justice (STJ). *Soziale Systeme* [online], 26(1–2), pp. 370–395. Available at: https://doi.org/10.1515/sosys-2021-0014

Hedler, L., 2023. *Time, Law, and Tech: The Introduction of Algorithms to Courts of Law* [online]. PhD Thesis. Copenhagen Business School. Available at: https://doi.org/10.22439/phd.17.2023

Hildebrandt, M., 2016. *Smart Technologies and the End(s) of Law* [online]. Cheltenham: Edward Elgar. Available at: https://doi.org/10.4337/9781849808774

Hildebrandt, M., 2017. Law As an Affordance: The Devil Is in the Vanishing Point(s). *Critical Analysis of Law* [online], 4(1), pp. 116–128. Available at: https://doi.org/10.33137/cal.v4i1.28154

King, M., and Thornhill, C., 2003. *Niklas Luhmann's theory of politics and law* [online]. London/Basingstoke: Palgrave Macmillan. Available at: https://doi.org/10.1057/9780230503588

Kitchin, R., 2014. Big Data, new epistemologies and paradigm shifts. *Big Data and Society* [online], 1(1), pp. 1–12. Available at: https://doi.org/10.1177/2053951714528481

Kokol, P., Kokol, M., and Zagoranski, S., 2022. Machine learning on small size samples: A synthetic knowledge synthesis. *Science Progress* [online], 105(1). Available at: https://doi.org/10.1177/00368504211029777

Luhmann, N., 1989. Law as a social system. *Northwestern University Law Review*, 136(1 & 2), pp. 136–150.

Luhmann, N., 1991. *Soziologie des Risikos.* Berlin: Walter de Gruyter.

Luhmann, N., 2018. *Organization and Decision, Organization and Decision* [online]. Cambridge University Press. Available at: https://doi.org/10.1017/9781108560672

Maas, M.M., 2019. Innovation-Proof Global Governance for Military Artificial Intelligence? How I Learned to Stop Worrying, and Love the Bot. *Journal of International Humanitarian Legal Studies* [online], 10(1), pp. 129–157. Available at: https://doi.org/10.1163/18781527-01001006

Martins, R.C., 2015. Beck in Brazil by Rodrigo Constante Martins — in memoriam. *Theory, Culture & Society* [online], 12 March. Available at: https://www.theoryculturesociety.org/blog/beck-in-brazil-by-rodrigo-constante-martins

Mölders, M., 2021. Legal Algorithms and Solutionism: Reflections on Two Recidivism Scores. *SCRIPT-ed* [online], 18(1), pp. 57–82. Available at: https://doi.org/10.2966/scrip.180121.57

Ost, F., 2005. *O Tempo do Direito.* 1st ed. Edusc.

Pasquale, F., 2018. *A Rule of Persons, Not Machines : The Limits of Legal Automation* [online]. University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2018-08. Available at: http://ssrn.com/abstract=3135549

Pasquale, F., and Cashwell, G., 2018. Prediction, persuasion, and the jurisprudence of behaviourism. *University of Toronto Law Journal* [online], 68(Issue supplement 1), pp. 63–81. Available at: https://doi.org/10.3138/utlj.2017-0056

Possa, J., 2023. Entenda o projeto que prevê a regulamentação da IA no Brasil. *UOL Giz* [online], 9 May. Available at: https://gizmodo.uol.com.br/entenda-o-projeto-que-preve-a-regulamentacao-da-ia-no-brasil/

Projeto de Lei n. 2338 de 2023. Brazilian Federal Senate.

Ranchordás, S., and Van't Schip, M., 2020. Future-Proofing Legislation for the Digital Age. *In:* S. Ranchordás and Y. Roznai, eds., *Time, Law and Change: an interdisciplinary study* [online]. Oxford: Hart, pp. 347–365. Available at: https://doi.org/10.5040/9781509930968.ch-016

Rasborg, K., 2021. *Ulrich Beck - Theorising World Risk Society and Cosmopolitanism* [online]. London: Palgrave Macmillan. Available at: https://doi.org/10.1007/978-3-030-89201-2

Reiling, A.D., 2020. Courts and Artificial Intelligence. *International Journal for Court Administration* [online], 11(2), pp. 1–10. Available at: https://doi.org/10.36745/ijca.343

Renn, O., 2008. Concepts of risk: An interdisciplinary review. *GAIA - Ecological Perspectives for Science and Society* [online], 17(2), pp. 196–204. Available at: https://doi.org/10.14512/gaia.17.2.7

Resolução n. 332 from 21/08/2020, DJe/CNJ n.274 [online]. Conselho Nacional de Justiça. Available at: https://atos.cnj.jus.br/atos/detalhar/3429

Roller, M.R., 2019. A quality approach to qualitative content analysis: Similarities and differences compared to other qualitative methods. *Forum Qualitative Sozialforschung* [online], 20(3). Available at: https://doi.org/10.17169/fqs-20.3.3385

Supiot, A., 2017. *Governance by numbers: The making of a legal model of allegiance.* Oxford: Hart.

Susser, D., 2019. Invisible influence: Artificial intelligence and the ethics of adaptive choice architectures. *AIES 2019 - Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* [online], pp. 403–408. Available at: https://doi.org/10.1145/3306618.3314286

Ugwudike, P., 2020, Digital prediction technologies in the justice system: The implications of a "race-neutral" agenda. *Theoretical Criminology* [online], 24(3), pp. 1–20. Available at: https://doi.org/10.1177/1362480619896006

Veale, M., Matus, K., and Gorwa, R., 2023. AI and Global Governance : Modalities , Rationales , Tensions. *Annual Review of Law and Social Science* [online], 19, pp. 1–30. Available at: https://doi.org/10.1146/annurev-lawsocsci-020223-040749