# ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS: HUMAN RIGHTS AT RISK?[1]

◉ Túlio Felippe Xavier Januário*

* PhD Candidate in Law at the University of Coimbra (Portugal), with a fellowship from the Fundação para a Ciência e a Tecnologia–FCT. M.Sc. in Law by the University of Coimbra, with a research internship of the "ERASMUS+" Program at the Georg-August-Universität Göttingen (Germany).
e-mail: tuliofxj@gmail.com

**Abstract:** The aim of the present paper is to analyze some of the possible applications of artificial intelligence in the criminal justice system and how it could affect some human rights of those involved. For that, the first topic presents the concept and functioning of this technology and how it could be used in the most varied stages of criminal procedure. Subsequently, the second topic addresses some limitations and challenges to be overcome in its application in the criminal justice system and, mainly, which human rights may be at stake with that use. The third and final topic presents some possible guidelines aimed at achieving the necessary balance between the efficiency and effectiveness of criminal justice and the protection of human rights of those affected by these technologies.

**Resumen:** El objetivo del presente trabajo es analizar algunas de las posibles aplicaciones de la inteligencia artificial en el sistema de justicia penal y cómo podría afectar derechos humanos de los involucrados. Para ello, el primer capítulo presenta el concepto y funcionamiento de esta tecnología y cómo podría ser utilizada en las más variadas etapas del proceso penal. Posteriormente, el segundo capítulo aborda algunas limitaciones y desafíos a superar en su aplicación en el sistema de justicia penal y, principalmente, qué derechos humanos pueden estar en juego con ese uso. El tercer y último capítulo presenta algunos posibles lineamientos direccionados a lograr el necesario equilibrio entre la eficiencia y eficacia de la justicia penal y la protección de los derechos humanos de los afectados por estas tecnologías.

SUMMARY:

**I. Introduction. II. Artificial Intelligence: concepts and applications in criminal proceedings. III. Challenges and limitations in applying artificial intelligence in criminal justice system. IV. Drawing some guidelines. V. Conclusion. VI. List of references.**

## I. INTRODUCTION

The progressive use of new technologies in the most varied sectors of society is an irrefutable reality in the contemporary world. Great examples of that are the scientific and technological developments in the field of artificial intelligence (A.I.), which has been applied in several activities that demand processing of a large amount of data in reduced time (Januário, 2021c: 128, Steibel, Vicente & Jesus, 2019).

In addition to impacts on sectors such as transports (Januário, 2020b, Estellita & Leite, 2019, Hilgendorf, 2020), medicine (Januário, 2020a, 2022, Pereira, 2021, Machado, 2019) and communications, more and more implications of these technologies are also expected in criminal investigations and proceedings, whether due to the evidentiary interest that the access to the information stored by them can generate, or for their potential to assist in state activities of intelligence, surveillance and even judicial decisions. However, we can immediately observe that their application in criminal investigations and procedures can imply several risks and may even affect internationally recognized human rights.

The objective of this investigation is precisely to analyze how the increasing use of new technologies, especially A.I. in criminal investigations and proceedings can affect human rights and to propose some alternative to mitigate these risks. To this intent, we will initially study what we can understand by new technologies and A.I. and how they are intended to be used in these procedures. Subsequently, in the light of the main international human rights charters, we will seek to understand, from a deductive methodology, which are the main guarantees that may be affected in these contexts. At the end of the paper, we will demonstrate that, although we can neither completely abstract from A.I. and new technologies as a whole nor ignore their potential implications in criminal proceedings, we need to find a point of balance between the interests at stake in order

to avoid that the incessant search of society for security ends up disproportionately affecting human rights, especially those of the people implicated in these procedures.

## II. ARTIFICIAL INTELLIGENCE: CONCEPTS AND APPLICATIONS IN CRIMINAL PROCEEDINGS

It is curious to observe that, although it sounds like a very recent term, the origins of the expression "artificial intelligence" date back for decades, more precisely to the 50. In fact, in Greek mythology, the dream of creating androids capable of performing human activities was already mentioned through "Talos", a robot responsible for the security of the island of Crete (Mayor, 2018: 7, Januário, 2021b).

But, scientifically speaking, the origin of the term artificial intelligence derives from the "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence", when John McCarthy defined it as "the science and engineering of making intelligent machines, especially intelligent computer programs". Moreover, "it is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable" (McCarthy, 2007, McCarthy, Minsky, Rochester & Shannon, 2006: 14).

Well, a lot has evolved in technological terms in this matter since 1955 and currently, the understanding of what A.I. is can involve two perspectives: by I) Artificial Intelligence as "systems", we can understand software or hardware that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected data, reasoning on this data and deciding the best action(s) to take (according to pre-defined parameters). Moreover, they can also be designed to learn to adapt their behaviour by analyzing how the environment is affected by their previous actions. II) As a scientific discipline, A.I. includes several approaches and techniques, such as machine learning, machine reasoning and robotics (The European Commission's High-Level Expert Group on Artificial Intelligence, 2018).

In proportion to scientific and technological advances, we have witnessed the expansion of A.I. to various scopes and activities, such as health, transports, stock market, surveillance and criminal investigations

and proceedings. Regarding this last area, we can divide its applications in four procedural phases.

The first of them, which can be referred to as the "pre-investigative" phase, concerns to when there isn't any suspect or even an illicit to be investigated yet (Canestraro, Kassada & Januário, 2019). It encompasses, therefore, daily supervision activities, public or private, carried out for the most varied purposes. In this context, the first example of A.I. that we can mention is that of predictive police (predPol). It is a police strategy oriented to crime prevention, which makes use of algorithmic models made possible by data and information obtained through several other technological systems —surveillance and body temperature cameras, internet publications and statistical analyses of past events—, integrating them with other information, such as opening hours of trade, people flows, etc., with the objective of determining where the occurrence of crimes (hotspots) is most likely and directing a bigger police enforcement to those areas, creating a kind of map of future crime (Barona Vilar, 2021: 445ff).

It is also worth mentioning the use of autonomous systems and artificial intelligence in the internationally standardized model of money laundering prevention and detection. Briefly, FIUs receive an immense amount of data from obligated entities, which are impossible to be manually checked. Therefore, employing automation in identifying patterns of suspicious activities is crucial (Agapito, Miranda & Januário, 2021: 90).

In the private sphere, the ability to process a large amount of data in a short time has made artificial intelligence a very useful tool in the business environment, especially in conducting internal investigations, due diligence procedures, risk assessment and even in the day-to-day supervision of employees (Januário, 2023, Canestraro & Januário, 2022, Rodrigues, 2021b, Rodrigues & Sousa, 2021). We can say that "digital criminal compliance" is one of the most relevant topics in this area, either because of its potentialities in terms of efficiency or the risks that arise from it (Burchard, 2020: 28).

In the second procedural phase, which can be referred to as the "investigative phase", we can include those activities carried out for the investigation of a determined fact, which has already come to the knowledge of the prosecution entities. In this scope, among the examples of application of A.I., it is worth mentioning the VERIPOL system, from Spain, aimed at identifying possible false reports (Barona Vilar, 2021: 458), as well as some other ones aimed at discovering details of what really happened in a specific case. This occurs, for example, with Interpol's use of the International

Child Sexual Exploitation Image Database (ICSE DB) to fight child sexual abuse, and, also, with the use of chatbots, emulating real people, to identify sexual predators in virtual forums. As Završnik (2020: 570) explains:

> In Europe, Interpol manages the International Child Sexual Exploitation Image Database (ICSE DB) to fight child sexual abuse. The database can facilitate the identification of victims and perpetrators through an analysis of, for instance, furniture and other mundane items in the background of abusive images –e.g., it matches carpets, curtains, furniture, and room accessories– or identifiable background noise in the video. Chatbots acting as real people are another advancement in the fight against grooming and webcam 'sex tourism'. […] The Sweetie avatar [from the NGO 'Terre des Hommes'], posing as a ten-year-old Filipino girl, was used to identify offenders in chatrooms and online forums and operated by an agent of the organisation, whose goal was to gather information on individuals who contacted Sweetie and solicited webcam sex. Moreover, Terre des Hommes started engineering an ai system capable of depicting and acting as Sweetie without human intervention in order to not only identify persistent perpetrators but also to deter first-time offenders.

In the procedural phase itself, artificial intelligence gains relevance not only in terms of becoming a relevant means of obtaining evidence, if we consider its high data storage (Quattrocolo, 2020: 37ff, Gless, 2020: 202ff, Fidalgo, 2020: 129ff), but also of assisting justice itself. This is the case, for example, of tools that assist in the selection of documents according to their relevance to the case, in the evaluation of evidence and even in the decision-making itself (Miró Llinares, 2018: 106, Nieva Fenoll, 2018). These automated risk assessment systems, of which the most paradigmatic examples are COMPAS and HART, end up using personal factors to assess whether there are greater or lesser risk of recidivism and, consequently, to analyze the adequacy of precautionary measures or specific sanctions (Miró Llinares, 2018: 108ff).

Finally, we can also highlight the application of artificial intelligence in the sentence serving phase. In this context, the so-called smart prisons stand out, in which this technology is used in the design, management and daily supervision of prisons. They are equipped with mechanisms that allow, for example, the supervision and tracking of prisoners, the detection of illegal activities and the control of possible violent acts or escapes (Barona Villar, 2021: 683ff).

## III. CHALLENGES AND LIMITATIONS IN APPLYING ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE SYSTEM

Having highlighted the potentialities of artificial intelligence, especially in terms of greater efficiency of activities related to the criminal process and investigation, it is important to address what its limitations are and its possible impacts on human rights.

First of all, it must be pointed out that artificial intelligence is considered "opaque". In other words, it means that its internal procedures, the relationships between a given input and an achieved output, and especially the foundations of a given decision, are difficult (if not impossible) for human understanding. So far, the conditions for fully understanding the "how" and "why" of a given decision made by A.I. are very limited, which is why it is often compared to black boxes (Burrell, 2016: 1, Price II, 2017: 2, Wimmer, 2019, Rodrigues, 2020b: 25).

Furthermore, due to the ability of some more advanced systems to learn from their previous experiences and adapt their algorithms, the output achieved by A.I. it is often unpredictable even for programmers. As explained by Susana Aires de Sousa (2020: 64), the specificity of autonomous systems lies precisely in the ability to obtain answers without the interference of the programmer, but only from the information and experiences acquired by the system, reaching outputs that perhaps were not even imagined by the individual and making decisions from them that can often be against the law.

Due to these facts, some scholars understand the application of artificial intelligence in criminal justice system, depending on its form and intensity, would violate the defendant's rights and guarantees, especially those related to the fair trial, such as his right to defense, to the publicity of the trial, to the presumption of innocence, to be judged by a competent impartial judge and the right to appeal the decision. These rights are widely recognized by human rights charters, such as Article 7th of the African Charter on Human and Peoples' Rights, Article 8th of the American Convention on Human Rights and Article 6th of the European Convention on Human Rights.

Anabela Miranda Rodrigues (2020a: 230ff), for example, highlights the difficulties imposed by the opacity of the algorithms, especially the fact that decisions regarding the Defendants are taken without giving them the opportunity to know the foundations of these decisions. This situation is

aggravated by the fact that the development of these algorithms is under charge of private companies, which have no interest in disclosing the particularities of their operation. This not only imposes difficulties on the public control of judicial decisions, but also entails a certain "unaccountability" on the part of the judges regarding the merits of the decisions, since they no longer see them as their own. Similarly, Luís Greco (2020: 43ff) also refers to the lack of a person accountable for the decisions as the core problem of the so-called "robot judges".

In addition, there is an evident concern with the data used as input by the algorithms. First, for a possible excessive violation of people's privacy (*American Convention on Human Rights,* 1969, Article 11th, *European Convention on Human Rights,* 1950, Article 8th). Unlike in the past, in which data sharing depended on a minimally conscious conduct of data subjects, currently, they are shared in a massive way and often depend on a simple active conduct of the person. Therefore, there is a justified fear that, based on arguments such as greater efficiency in police activities and increased security of people, there will be an ever-increasing intrusion on people's intimacy and privacy (Miró Llinares, 2018: 114ff).

Secondly, it is feared that the use of these algorithms, especially in criminal prosecution, ends up accentuating even further the criminal selectivity to the detriment of certain groups. If we use factors such as ethnicity, race, gender, place of residence, profession, etc., to determine greater or lesser preventive policing or even the risk of recidivism and, consequently, whether a specific citizen is entitled to a certain alternative penalty or precautionary measure, wouldn't we be faced with an "algorithmic discrimination" (Miró Llinares, 2018: 120ff) and consequently a violation of Article 3 of the *African Charter on Human and Peoples' Rights* (1981) and Article 1 of the *Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms* (2000)?. It is interesting to observe, as Anabela Miranda Rodrigues (2020a: 233) points out, that although the variable "race" is generally not expressly used, other elements used end up replacing it and implicitly reflect racial prejudice.

Furthermore, we cannot rule out the possibility of the data quality itself being poor (Mulholland & Frajhof, 2019, Yapo & Weiss, 2018: 5366, Peixoto & Martins, 2019: 34-35, Miranda & Januário, 2021: 286ff). In other words, the data applied for training the algorithm may have been poorly qualified by the programmer; have been collected in a very strict period of time; or else, in general, not being representative. With inaccurate

or invalid data being used as input, the chance of errors is much greater, which can make outputs of poor quality and increase the chances of perpetuating discrimination and prejudice (Miró Llinares, 2018: 122ff).

Finally, an important question to be addressed is the potential "lack of humanity" behind a greater use of artificial intelligence in criminal prosecution. What we mean is that when we use computer systems to make predictions such as the chances of recidivism, or even of committing a crime, which demands greater police contingents in certain areas, we run the risk of not taking into account important variables, only analyzable through human emotions and feelings. Empathy, forgiveness and the very consideration that people are capable of contradicting statistics or acting contrary to their history, are variables that, in our point of view, can only be considered when we do not remove human beings from the equation of justice.

## IV. DRAWING SOME GUIDELINES

Firstly, it is important to point out that eventual legal proposals for the issues under analysis are dependent on the scientific and technological developments in this area. In other words, even if juridical scholars reach a minimum consensus on some guidelines to seek, they may end up being limited by the techniques available to do so.

This is the case, for example, of the need for transparency in artificial intelligence. It is somehow pacific that the application of artificial intelligence in criminal justice system depends on providing the interested parties with knowledge about the foundations of a certain decision-making so that they can challenge it, if necessary.

However, artificial intelligence, by its very structure and functioning, ends up being opaque and unpredictable even for programmers. Therefore, there is some scepticism on the feasibility and even usefulness of full transparency in the sector. Despite some occasional rumors regarding the increasingly transparency of A.I., we are not aware of any concrete progress on this path so far.

In this sense, as Matheus de Alencar and Miranda (2023: 105-111) points out, when we refer to transparency in the scope of artificial intelligence, we may be referring to i) one's knowledge that he/she is facing this technology (provided for, for example, by Article 9th of the Portuguese Law 27/2021, of May, 17th) or ii) his/her understanding of the functioning of

these systems, such as their programming rules, coding methods and source codes. According to the author, if on the one hand the first possibility is a fundamental measure to mitigate the reduction in the autonomy of those involved caused by the use of algorithms of automated decision, on the other hand, the second hypothesis would not contribute much in terms of attributing criminal responsibilities, not only due to the technical difficulties associated with it, but also because of the excessive evidentiary difficulties that it would impose on the Prosecution, in its task of demonstrating the specific error that caused the damage. However, with regard not to the attribution of criminal liability for damages caused by artificial intelligence, but rather to the its use in the most varied phases of an investigation and criminal procedure, we understand that algorithmic transparency is fundamental to ensure the plenitude of the Defendant's defense and, consequently, a fair trial.

Despite all these technical reservations, we agree with the scholars that sustain that, even if developed and maintained by private companies, A.I. should be publicized when applied in the criminal justice system. By that we mean that, contrary to what happened in the well-known case of *Loomis v. Wisconsin* (Caria, 2020), trade secrecy should not be invoked as an obstacle to the disclosure of source codes, data used as input and, as far as possible, the functioning of the technology. This is essential so that, as far as technically possible, data and the technology be audited and the interested parties can have access to and eventually challenge the conclusions reached by it at any stage of criminal prosecution (Miró Llinares, 2018: 122ff).

Furthermore, just as when algorithms are used in the stock market, specifically in the so-called high frequency trading (Rodrigues, 2021a), training in controlled and supervised environments (the so-called sandboxes) must be enforced (Sousa, 2020: 86ff). This is crucial so that programmers can have greater knowledge about the concrete operation of the algorithm in face of certain situations and how its machine-learning will evolve, being possible to make the necessary adjustments (Januário, 2021c: 161).

With regard to the evidentiary potentialities of artificial intelligence and the data that it stores, the discussion related to the chain of custody of digital evidence gains importance. Although it is a well-established institute in some legal systems (such as the North American), in some others it is still disregarded. In our opinion, it is a fundamental institute to ensure the credibility, legality and validity of the evidence that is intended to be used in a

judicial process, also guaranteeing the counterparty means of contesting not only the content of the evidence, but also the scientific method applied in its collection, transport and storage (Januário, 2021a, Prado, 2021).

Finally, it seems that the most important guideline to follow is not to take the human being out of the equation of the criminal justice system. Despite the potential of artificial intelligence and new technologies as a whole, which can, in fact, make justice more efficient and, in some cases, fairer, we cannot forget that this same justice system was created by us, human beings, and for us, human beings, for the protection of those goods that we consider most fundamental. Therefore, it is essential that human empathy and solidarity be always relevant factors in decision-making in the criminal sphere, however simple they may be. Artificial intelligence should, therefore, be a fundamental instrument to assist in the provision of justice, but never the core of this activity.

## V. CONCLUSION

As demonstrated, the expansion of new technologies, including artificial intelligence, is a reality that has been observed in the most varied sectors of our society. It is no different in the criminal justice system, where they have been applied in state activities of supervision, inspection and also in criminal investigations, prosecutions and sanctioning.

However, it was also demonstrated that the use of these technologies does not come unaccompanied by obstacles, either due to their own particularities and limitations —such as the opacity and unpredictability that are inherent to them— or due to their potential risks to people's rights and guarantees —like those related to people's intimacy and privacy, right to non-discrimination and also to a fair trial—.

For this reason, we proposed some standards to be achieved in order to mitigate these difficulties. Enforcing i) the publicity of A.I. and its algorithms when applied to the justice system, ii) the training in simulated and supervised environments and iii) the documentation of the chain of custody of digital evidence under penalty of its inadmissibility in court are some of the measures that, in our point of view, can help ensuring the protection of the rights and guarantees of those affected by these technologies within the scope of criminal justice, which, however, can never leave aside the human element in its procedures.

It is evident that many of the legal proposals in this area are dependent on their technical and scientific feasibility to be achieved. However, the prompt establishment of these guidelines is crucial in order to assure legal provisions in face of the unstoppable proliferation of these technologies and also that they are aligned with human rights.

## VI. LIST OF REFERENCES

*African Charter on Human and Peoples' Rights* (1981). Available on https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf

Agapito, L. S., Miranda, M. A., & Januário, T. F. X. (2021). On the Potentialities and Limitations of Autonomous Systems in Money Laundering Control. *RIDP, 92*(1), 87-105.

*American Convention on Human Rights* (1969). Available on https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm

Barona Vilar, S. (2021). *Algoritmización del derecho y de la justicia: de la inteligencia artificial a la smart justice.* Valencia: Tirant lo Blanch.

Burchard, C. (2020). Das »Strafrecht« der Prädiktionsgesellschaft: …oder wie »smarte« Algorithmen die Strafrechtspflege verändern (könnten). *Forschung Frankfurt: das Wissenschaftsmagazin: Recht und Gesetz,* (1), 27-31. Available on: http://publikationen.ub.uni-frankfurt.de/frontdoor/index/index/year/2020/docId/55171

Burrell, J. (2016). How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms. *Big Data & Society, 3*(1). Available on https://doi.org/10.1177/2053951715622512

Canestraro, A. C., & Januário, T. F. X. (2022). Inteligência Artificial e Programas de Compliance: Uma Análise dos Possíveis Reflexos no Processo Penal. In F. R. D'Ávila, & M. E. A. Amaral (Eds.), *Direito e Tecnologia* (pp. 363-392). Porto Alegre: Citadel.

Canestraro, A. C., Kassada, D. A., & Januário, T. F. X. (2019). Nemo tenetur se detegere e programas de compliance: o direito de não produzir prova contra si próprio em face da Lei n. 13.303/16. In E. Saad-Diniz, L. A. Brodt, H. A. A. Torres, & L. S. Lopes (Eds.), *Direito Penal Econômico nas Ciências Criminais* (pp. 311-342). Belo Horizonte: Vorto.

Caria, R. (2020). O Caso State v. Loomis-A Pessoa e a Máquina na Decisão Judicial. In A. M. Rodrigues (Ed.), *A Inteligência Artificial no Direito Penal* (pp. 245-266). Coimbra: Almedina.

Estellita, H. & Leite, A. (2019). Veículos Autônomos e Direito Penal: uma introdução. In H. Estellita & A. Leite (Orgs.), *Veículos Autônomos e Direito Penal* (pp. 15-36). São Paulo: Marcial Pons.

*European Convention on Human Rights* (1950). Available on https://www.echr.coe.int/documents/d/echr/convention_eng

Fidalgo, S. (2020). A Utilização de Inteligência Artificial no Âmbito da Prova Digital-Direitos Fundamentais (Ainda Mais) Desprotegidos. In A. M. Rodrigues (Ed.), *A Inteligência Artificial no Direito Penal* (pp. 129-162). Coimbra: Almedina.

Gless, S. (2020). AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials. *Georgetown Journal of International Law*, *51*(2), 195-253. Available on https://ssrn.com/abstract=3602038

Greco, L. (2020). *Poder de julgar sem responsabilidade de julgador: a impossibilidade jurídica do juíz-robô.* São Paulo: Marcial Pons.

Hilgendorf, E. (2020). Sistemas Autônomos, Inteligência Artificial e Robótica: uma orientação a partir da perspectiva jurídico-penal. In E. Hilgendorf, & O. Gleizer (Eds.), *Digitalização e Direito* (pp. 43-60). São Paulo: Marcial Pons.

Januário, T. F. X. (2020a). Inteligência Artificial e Responsabilidade Penal no Setor da Medicina. *Lex Medicinae: Revista Portuguesa de Direito da Saúde 17*(34), 37-64. Available on https://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/revistas

Januário, T. F. X. (2020b). Veículos Autônomos e Imputação de Responsabilidades Criminais por Acidentes. In A. M. Rodrigues (Ed) *A Inteligência Artificial no Direito Penal* (pp. 95-128). Coimbra: Almedina.

Januário, T. F. X. (2021a). Cadeia de Custódia da Prova e Investigações Internas Empresariais: Possibilidades, Exigibilidade e Consequências Processuais Penais de sua Violação. *Revista Brasileira de Direito Processual Penal, 7*(2), 1453-1510. Available on https://doi.org/10.22197/rbdpp.v7i2.453

Januário, T. F. X. (2021b). Considerações Preambulares acerca das Reverberações da Inteligência Artificial no Direito Penal. In M. S. Comério, & T. A. Junquilho (Eds.), *Direito e Tecnologia: Um Debate Multidisciplinar* (pp. 295-314). Rio de Janeiro: Lumen Juris.

Januário, T. F. X. (2021c). Inteligência Artificial e Manipulação do Mercado de Capitais: uma análise das negociações algorítmicas de alta frequência (High-Frequency Trading-HFT) à luz do ordenamento jurídico brasileiro. *Revista Brasileira de Ciências Criminais, 186*(29), 127-173.

Januário, T. F. X. (2022). Inteligência artificial e direito penal da medicina. In A. M. Rodrigues (Ed.), *A inteligência artificial no direito penal* (2nd Vol., pp. 125-174). Coimbra: Almedina.

Januário, T. F. X. (2023). Corporate Internal Investigations 4.0: on the criminal procedural aspects of applying artificial intelligence in the reactive corporate compliance. *Revista Brasileira de Direito Processual Penal*, *9*(2), 723-785. Available on https://doi.org/10.22197/rbdpp.v9i2.837

*Lei n.º 27/2021, de 17 de maio: Carta Portuguesa de Direitos Humanos na Era Digital.* Available on https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3446&tabela=leis&so_miolo=

Machado, L. S. (2019). Médico robô: responsabilidade civil por danos praticados por atos autônomos de sistemas informáticos dotados de inteligência artificial. *Lex Medicinae: Revista Portuguesa de Direito da Saúde, 16*(31), 101-114. Available on https://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/revistas/lex-medicinae-revista-portuguesa-de-direito-da-sa%C3%BAde-ano-16-n%C2%BA-31-32

Mayor, A. (2018). *Gods and Robots: myths, machines and ancient dreams of technology.* Princeton: Princeton University Press.

McCarthy, J. (2007). *What is Artificial Intelligence?* Stanford: Stanford University. Available on http://jmc.stanford.edu/artificial-intelligence/index.html

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine, 27*(4), 12-14. Available on https://doi.org/10.1609/aimag.v27i4.1904

Miranda, M. A. (2023). *Técnica, decisões automatizadas e responsabilidade penal* (Doctoral Thesis). Universidade do Estado do Rio de Janeiro, Rio de Janeiro, Brasil.

Miranda, M. A., & Januário, T. F. X. (2021). Novas tecnologias e justiça criminal: a tutela de direitos humanos e fundamentais no âmbito do direito penal e processual penal. In V. Moreira *et al.* (Eds.), *Temas de Direitos Humanos do VI cidh Coimbra 2021* (pp. 284-298). Campinas/Jundiaí: Brasílica/ Edições Brasil.

Miró Llinares, F. (2018). Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología, 3*(20), 87-130.

Mulholland, C., & Frajhof, I. Z. (2019). Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: Breves Anotações Sobre o Direito à Explicação Perante a Tomada de Decisões por Meio de Machine Learning.

In A. Frazão, & C. Mulholland (Eds.), *Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade* (Ebook, N.P.). São Paulo: Thomson Reuters Brasil.

Nieva Fenoll, J. (2018). *Inteligencia Artificial y Proceso Judicial.* Madrid: Marcial Pons.

Peixoto, F. H., & Silva, R. Z. M. (2019). *Inteligência Artificial e Direito.* Curitiba: Alteridade Editora.

Pereira, A. G. D. (2021). Inteligência Artificial, Saúde e Direito: considerações jurídicas em torno da medicina de conforto e da medicina transparente. *Julgar,* (45), 235-262.

Prado, G. (2021). *A cadeia de custódia da prova no processo penal* (2nd edn). São Paulo: Marcial Pons.

Price II, W. N. (2017). Artificial Intelligence in Health Care: Applications and Legal Issues. *U of Michigan Public Law Research Paper*, (599), 1-7. Available on https://ssrn.com/abstract=3078704

*Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms* (2000). Available on https://www.echr.coe.int/documents/d/echr/convention_eng

Quattrocolo, S. (2020). *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a European Legal Discussion.* Cham: Springer.

Rodrigues, A. M. (2020a). A questão da pena e a decisão do juiz-entre a dogmática e o algoritmo. In A. M. Rodrigues (Ed.) *A inteligência artificial no direito penal* (pp. 219-244). Coimbra: Almedina.

Rodrigues, A. M. (2020b). Inteligência Artificial no Direito Penal-A Justiça Preditiva entre a Americanização e a Europeização. In A. M. Rodrigues (Ed.), *A Inteligência Artificial no Direito Penal* (pp. 11-58).

Rodrigues, A. M. (2021a). Os crimes de abuso de mercado e a "escada impossível" de Escher (o caso do spoofing). *Julgar,* (45), 65-86.

Rodrigues, A. M. (2021b). The Last Cocktail-Economic and Financial Crime, Corporate Criminal Responsibility, Compliance and Artificial Intelligence. In M. J. Antunes, & S. A. Sousa (Eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility* (pp. 119-133). Coimbra: Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra. Available on https://doi.org/10.47907/livro2021_4c5

Rodrigues, A. M., & Sousa, S. A. (2021). Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal. *Julgar,* (45), 193-214.

Sousa, S. A. (2020). "Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial. In A. M. Rodrigues (Ed.), *A inteligência artificial no direito penal* (pp. 59-94). Coimbra: Almedina.

Steibel, F., Vicente, V. F., & Jesus, D. S. V. (2019). Possibilidades e Potenciais da Utilização da Inteligência Artificial. In A. Frazão, & C. Mulholland (Eds.), *Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade* (Ebook, N. P.) São Paulo: Thomson Reuters Brasil.

The European Commission's High-Level Expert Group on Artificial Intelligence (2018). *A Definition of AI: Main Capabilities and Scientific Disciplines: Definition Developed for the Purpose of the Deliverables of the High-Level Expert Group.* Brussels: European Commission. Available on https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

Wimmer, M. (2019). Inteligência Artificial, Algoritmos e o Direito: Um Panorama dos Principais Desafios. In A. P. M. C. Lima, C. B. Hissa, & P. M. Saldanha (Eds.), *Direito Digital: Debates Contemporâneos* (Ebook, N. P.). São Paulo: Thomson Reuters Brasil.

Yapo, A., & Weiss, J. (2018). Ethical Implications of Bias in Machine Learning. In *Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 5365-5372). Available on http://hdl.handle.net/10125/50557

Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. *ERA Forum,* (20), 567-583. Available on https://doi.org/10.1007/s12027-020-00602-0