AI AND ADMINISTRATION OF CRIMINAL JUSTICE

PORTUGUESE REPORT[1]

By *Anabela Miranda Rodrigues*[2], *Sónia Fidalgo*[3] and *Ana Pais*[4]

I. PREDICTIVE POLICING[5]

1. National practices

1. In Portugal, the Criminal Policy Law for the biennium 2020-2022 (Law no. 55/2020, August 27) is currently in force. Among other objectives, priorities and orientations of the State´s criminal policy, one of the important axes of that legal act is crime prevention (Article 2, Article 3, paragraph a), and Article 4). This target goes along with the option of the general legal framework on criminal policy (included in Law no. 17/2006, May 23) which defines criminal prevention as a general objective of the criminal policy (Articles 1 and 4). However, none of these legal acts provides a definition of criminal prevention.

2. Neither is there a formal definition of "predictive policing" in Portugal as there isn´t a legislative act or any normative instrument that defines or even refers to this concept. We assume the concept implies foreseeing criminal behaviour by using AI-based systems in order to identify specific potential agents and previse concrete data on the time and place where those behaviours will take place. In other words, it relates to the use of AI-based systems to predict crime in order to prevent it through policing measures.

3. In fact, AI-based systems aren´t yet being used in our country in this specific domain and for the time being no plans to use them in the future have been publicly announced.

---

[1] This report was written and finished in January (Part I) and April (Parts II and III) of 2022.

[2] Full Professor – Faculty of Law – University of Coimbra

[3] Tenured Assistant Professor – Faculty of Law – University of Coimbra

[4] Assistant Professor (Guest) – Faculty of Law – University of Coimbra

[5] This part (I) of the report was put through with the collaboration of the National Director of the Security Intelligence Service Dr. Adélio Neiva da Cruz, the Portuguese Public Prosecutor Dr. Pedro Verdelho (Coordinator of the Cybercrime Council), the Portuguese Criminal Police (Polícia Judiciária – PJ) represented by Dra. Luísa Proença (National Assistant Director) and Dr. Rogério Bravo (Inspector Chief), and also the Public Safety Police (Polícia de Segurança Pública – PSP) represented by Dr. Dário Prates (Superintendent, Head of the PSP Criminal Investigation Department).

However, the police services in general, but specially the Portuguese Criminal Police – Polícia Judiciária (PJ) – are committed to the development of numerous projects concerning the future use of AI systems in the field of criminal prevention, in cooperation with the European institutions. Those "investigation and development projects" mainly integrate the Horizon 2020 EU Program.

The project GRACE (*Global Response Against Child Exploitation*)[6] aims to equip European Law Enforcement Agencies (LEA) with advanced analytical and investigative capabilities to respond to the spread of online child sexual exploitation material, mainly through the implementation of a server network based on high-level AI systems.

The project CREST *(Fighting Crime and TerroRism with an IoT-enabled Autonomous Platform based on an Ecosystem of Advanced IntelligEnce, Operations, and InveStigation Technologies)*[7] aims to leverage the Internet of Things ecosystem, autonomous systems and targeted technologies. This will help the police detect and assess threats, plan surveillance, distribute command and control of law enforcement missions, share information and exchange digital evidence through blockchain technologies. CREST will also provide chain-of-custody and path-to-court for digital evidence. The project will test its methods in three operational use cases, including the protection of public figures in motorcades, counter terrorism security in crowded areas, and cross-border fight against organised crime.

The project AIDA *(Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies)*[8] focuses on cybercrime and terrorism by approaching specific issues related to law enforcement agencies (LEAs) using pioneering machine learning and artificial intelligence methods. The project will deliver a descriptive and predictive data analytics platform and related tools which will prevent, identify, analyse and combat cybercrime and terrorist activities. The platform is based on the fundamental technology applied to Big Data analytics provided with AI and deep learning techniques expanded and tailored with additional crime-specific capabilities and tools. The system will be delivered to LEAs through a safe sandbox environment, improving the technological readiness level in operational conditions with real data.

The project INFINITY *(Revolutionising data-driven investigations)*[9] aims to transform the traditional idea of criminal investigation and analysis using immersive and collaborative environments. The primary goals of INFINITY are to revolutionise data driven investigations through the use of artificial intelligence, machine learning and big data analytics to facilitate

[6] https://cordis.europa.eu/project/id/883341.
[7] https://cordis.europa.eu/project/id/833464.
[8] https://cordis.europa.eu/project/id/883596.
[9] https://cordis.europa.eu/project/id/883293.

effectiveness of an investigation and utilise modern innovations in virtual reality, augmented reality and visual analytics in order to facilitate a better intel cycle. Both of which will be driven by end-users and designed to address law enforcement needs.

The project DARLENE (*Deep AR law enforcement ecosystem)*[10] investigates how cutting-edge augmented reality (AR) technology can be deployed to help law enforcement agencies (LEAs) and first responders make more informed and rapid decisions especially in situations where time is of the essence. The project develops innovative augmented reality (AR) tools that aim to improve situational awareness when responding to criminal and terrorist activities. DARLENE will combine innovative AR smart glass technology and powerful computer vision algorithms with 5G network architectures to allow agile processing of real-time data by LEAs even in high-pressure situations. The project will also carry out an integrated ethical, data protection and social impact assessment of augmented reality tools to ensure compliance with ethics requirements and build public trust for the lawful use of technology.

The project RISEN (*Real-tIme on-site forenSic tracE qualificatioN*)[11] aims to develop a set of real-time contactless sensors for the optimization of the trace, detection, visualisation, identification and interpretation on site, with a consequent reduction of the time and resources in the laboratory, and for a fast exchange of information among LEAs. The recreated 3D model of the scene resorts to augmented reality techniques for sensor data, collected evidence and identified points of interest in order to deliver a realistic and immersive visual environment for investigators, allowing them to conduct highly detailed investigations. The crime scenes, with analytical information from traces, will be digitally frozen to be available at any time for several purposes in the criminal justice system. The identified traces will be digitally marked and inventoried, and a digitalised Chain of Custody will be established in real-time implementing mechanisms that assure data integrity over its lifecycle.

The project GLASS *(SinGLe Sign-on eGovernAnce paradigm based on a distributed file exchange networkfor Security, transparency, cost effectiveness and trust)*[12] aims to place EU citizens in control of their personal information and streamline access to eGovernment services across Member States and beyond. The project introduces a citizen-centric e-governance model that enables beneficiaries to participate in a network for big data exchange and service delivery, which is by design digital, efficient, cost-effective, interoperable, cross-border, secure and promotes the once-only priority.

[10] https://cordis.europa.eu/project/id/883297.
[11] https://cordis.europa.eu/project/id/883116.
[12] https://cordis.europa.eu/project/id/959879.

The project CONNEXIONs (*Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services)*[13] aims to develop and demonstrate next-generation detection, prediction, prevention, and investigation services. These services will be based on multidimensional integration and correlation of heterogeneous multimodal data, and delivery of pertinent information to various stakeholders in an interactive manner tailored to their needs, through augmented and virtual reality environments. The CONNEXIONs solution encompasses the entire lifecycle of law enforcement operations including: pre-occurrence crime prediction and prevention; during-occurrence LEA operations; post-occurrence investigation, and crime-scene simulation and 3D reconstruction.

The project STARLIGHT (*Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats)*[14] aims to increase awareness, ability, adoption, and long-term results of AI applications in European LEAs. By offering opportunities to exploit AI tools and solutions, STARLIGHT will ensure LEAs can protect their own AI systems, and increase LEA expertise and capacity against AI-supported crime and terrorism. The project will raise high-quality datasets, an interoperable and standardised framework, and an AI hub to enhance the EU's strategic autonomy in AI.

The project CounteR (*Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection*)[15] addresses the fight against radicalisation leading to terrorism and aims to develop a frontline community policing tool aimed at countering radicalisation in Europe. It will draw data from disperse sources into an analysis and early alert platform for data mining and prediction of critical areas such as communities. It will make use of the latest natural language processing technologies and will support information sharing between law enforcement agencies and collaboration between agencies by providing an open platform.

The project MArIA (*Detection of illegal MArIjuana plantations using Artificial Intelligence-based technologies*)[16] consists of procurement processes to implement and validate two innovate AI-based systems (AI-based satellite imagery analysis for the detection of outdoor cannabis plantations; AI-based electricity consumption analysis for the detection of indoor cannabis plantations), each of them adapted to the specific type of cannabis plantation. Both systems will

[13] https://cordis.europa.eu/project/id/786731.
[14] https://cordis.europa.eu/project/id/101021797.
[15] https://cordis.europa.eu/project/id/101021607.
[16] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/983734231/project/952812/program/31077817/details.

provide investigators with direct and real-time detection notifications that will be automatically inserted in the LEA's IT corporate investigations systems.

The project NOTIONES (*iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS)*[17] aims to build a network of practitioners from security and intelligence services, by the monitoring of technologies and the definition of requirements and recommendations for their industrialization, through a wide disclosure in seminars and conferences in order to provide a great advantage to practitioners in the fields of intelligence and security.

The participation in this wide range of projects that relate to the use of AI in criminal prediction and prevention through policing methods proves that Portugal is aware of the numerous possibilities that AI-based systems allow. However, future usage of those systems will demand the lawmaker´s intervention so that the country´s legal order admits and regulates those kinds of policing practises.

2. Normative framework

For the time being, there isn´t a legal framework on predictive policing. So far, as it is publicly known, there are no legislative proposals with such scope.

Nevertheless, recently the Portuguese Parliament approved Law no. 95/2021, December 29[18], which regulates the use and access, by the security forces and services and by the Portuguese National Authority for Civil Protection, of video surveillance systems (including body cams) which collect, record and process image and sound data, in public spaces and also in private spaces of public access[19]. Under Article 3, paragraph 1, d) and e), video surveillance systems can be used to *prevent crimes in places where there is considerable risk of its occurrence* or to *prevent terrorist acts*.

These video surveillance systems can´t be considered a form of AI-based system as the processing of information and the forward decision are still human made, but it reveals a new

[17] https://cordis.europa.eu/project/id/101021853.
[18] Published here: https://dre.pt/dre/detalhe/lei/95-2021-176714548.
[19] This legislation refers to the definitions contained in Law no. 59/2019, August 8, which transposes into national law Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

form of using sensors that contribute to a wide collection of data in what could be considered a demonstration of what is called *Augmented Reality*.

3. General principles of law

1. Although legal scholars have already introduced in some academic articles, recent seminars and conferences[20] the topic of protecting fundamental rights with regard to the use of AI-based systems, in fact there has not yet been any structured public discussion about the subject concerning predictive policing.

The only public forum where the issues of principles of constitutional law and fundamental rights regarding the use of AI-based systems have been addressed, although under a general perspective, was the Portuguese Parliament during the discussion and approval of the above referred Law no. 95/2021[21].

2. Nevertheless, it is important to state that the rights to equality and to non-discrimination (Article 13), the right to privacy (Article 26), the rights to liberty and security (Article 27) are enshrined in the *Constitution of the Portuguese Republic* (hereafter identified as CPR), as fundamental rights. This means that they will apply in any case or situation, even if a future legal text or practise does not refer to it. Concerning the principle of procedural legality, it is the same, since it is also a constitutional guarantee of the citizens (Articles 29 and 32). The principle of proportionality is a central principle of constitutional law and also applies mandatorily to any situation related to the restriction of fundamental rights (Article 18).

3. Apart from this general remarks, it is imperative to highlight the forerunner feature of the Portuguese Charter on Human Rights in the Digital Age (Law no. 27/2021, May 17)[22], which entered into force on 18 July 2021. It is a national legal instrument approved as an ordinary legislative act and therefore it only enforces at national level.

The Charter establishes a set of innovative standards regulating the digital environment and the provision of new rights and duties, such as the right to free access to the digital

[20] In November 2020 took place in the Faculty of Law of the University of Coimbra an International Conference on the subject *Artificial Intelligence and Criminal Law* organized by the Portuguese Group of AIDP. The book of abstracts can be accessed here: https://aidp-pt.org/2021/06/14/livro-de-resumos-book-of-abstracts/.

[21] The discussion which took place in the Parliament can be watched in the Parliament channel, available here: https://canal.parlamento.pt/?cid=5705&title=reuniao-plenaria.

[22] Available here: https://dre.pt/dre/legislacao-consolidada/lei/2021-164870244.

environment (Article 3), the right of freedom of expression and creation in a digital environment (Article 4), the right to protection against disinformation (Article 6), the rights to assemble, demonstrate, associate and participate in a digital environment (Article 7), the right to privacy in a digital environment (Article 8), the right to neutrality in the Internet (Article 10), the right to develop digital skills (Article 11), the right to identity and other personal rights (Article 12), the right to oblivion (Article 13), rights in digital platforms (Article 14), the right to cybersecurity (Article 15), the right to freedom of creation and protection of contents (Article 16), the right of protection against abusive geolocation (Article 17), the right to a digital will (Article 18), etc. These days, the discussion that takes place is mainly about the potential interpretative problems that may arise because the majority of the provisions of the Charter foresee redundant norms as they refer to rights that are already present in the system, whether in the Constitution or in ordinary law.

Though, Article 9 specifically addresses the use of AI and foresees that it *should be guided by the respect for fundamental rights, assuring a fair balance between the principles of explainability, security, transparency and responsibility, considering the circumstances of each concrete case and establishing processes that aim to avoid any prejudice or other forms of discrimination* (paragraph 1). Paragraph 2 states that the *decisions made by algorithms with considerable impact on the recipient´s realm should be communicated to the concerned people and are appealable*. Paragraph 3 relates to the creation and use of robots and determines the observation of the *principles of beneficence and non-maleficence, respect for human autonomy and justice, as well as all the principles and values enshrined in article 2.º of the EU Treaty, namely non-discrimination and tolerance*.

4. In conclusion, there is no legislation in Portugal concerning the use of AI-based systems as predictive policing methods. Still there is a wide range of sensors in use which are responsible for gathering and comparing information that is essential to the efficiency of policing but the processing and decision on those data are still human made.

Anyway, the country is aware of the advantages and problems associated to this new reality and is keeping up with the EU projects on the matter so that in a close future it will be possible to draw conclusions on the subject and to – eventually – legislate according to them.

II. PREDICTIVE JUSTICE[23]

1. National practices

1. Portugal has not adopted, to this date, an official definition of "predictive justice", which is, in fact, an underdeveloped topic in our country. It can, however, be mentioned that Portugal was involved in the preparatory work of the *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, adopted by European Commission for the efficiency of justice (CEPEJ) in 2018. This European Ethical Charter provides decisive contributions in understanding the issues associated to the implementation of these technologies in the various Member States of the Council of Europe. In fact, the accompanying study (Appendix I) deals in a quite in-depth manner with the various sides of this topic, among which can be highlighted: its operational features [chapter 3]; potential influence on the behaviour of judges [chapter 4]; and opportunities and limitations [chapter 9]. As regards its definition, it was included in the *Glossary* adopted in the same exercise (Appendix III): *Predictive justice is the analysis of large amounts of judicial decisions by artificial intelligence technologies in order to make predictions for the outcome of certain types of specialised disputes (for example, redundancy payments or alimentary pensions)*[24].

The term also appears – albeit in the guise of 'predictive analytics' – in another essential document to consider when approaching this topic within the European Union: the *Study on the use of innovative technologies in the field of justice*, published by the Commission on 14 September 2020, which collected data on the use of artificial intelligence and blockchain technologies in the administration of justice in the various Member States. In this case, the definition adopted is as follows: *Predictive analytics – A solution to business problems in the categories of LKS [Linking information across different sources], PCD [Processing high volume of data] and PPD [Preparing high volume of data], using AI technology to analyse current and historical facts to make predictions about the future or and/or identify risks and opportunities. In the justice field, such solutions are typically referred to as "predictive justice" and are used to help the judiciary in the decision-making process.*

That said, although a definition of "predictive justice" has not been adopted, the Portuguese lawmakers have at their disposal these references to consider when deemed appropriate.

---

[23] This part (II) of the report was put through with the collaboration of the Director-General for Justice Policy, Dr. Jorge Costa.

[24] See Anabela Miranda RODRIGUES, 'Inteligência artificial no direito penal – a justiça preditiva entre a americanização e a europeização', *in*: A *Inteligência Artificial no Direito Penal* (A. M. Rodrigues ed.), Almedina, 2020, p. 32 f.

2. AI-based systems for predictive justice are not used in Portugal (therefore, no judicial authority is obliged to use systems of this type at any stage of criminal proceedings). And the alternative dispute resolution is also carried out without using these technologies.

However, Portugal has not closed the door to the possibility of studying the use of predictive justice tools, although within a very limited scope. In this regard, it is worth mentioning two projects stated in the *Commission's Study on the use of innovative technologies in the field of justice*, we already referred to, namely:

a) The project "*Modelação, Predição e Decisão em Contexto de Jurisprudência"* (page 132) to be developed by the Portuguese Ministry of Justice, described as follows: *This pilot project will use past court decisions to assist magistrates when receiving inquiries or documents from lawyers. It will enable faster conclusions by magistrates, thus enabling faster justice for citizens*; and

b) The project *AI technology for evidence analysis* (page 131), to be implemented by the General Public Prosecutor's Office, described as follows: *This project uses classification, indexation and advanced search AI technologies for the new case management system (CMS) of the Public Prosecutor's Office. The tool will take into account the specificities of the procedural rules of the Portuguese judiciary. The CMS is expected to bring more comprehensive ways to visualise the concrete documents.*

Furthermore, there is not any indication from the judicial authorities not to use these means or any specific policy decision in this regard. Nevertheless, the (former) Minister of Justice (Francisca Van Dunem) has referred in several occasions to the need for adequate safeguards for the use of artificial intelligence technologies in the judiciary[25].

3. In Portugal there is still very little discussion about AI-based systems for predictive justice. The media usually don't address this topic. A few of the Portuguese legal scholars have paid attention to this problem - referring to what has happened especially in common law systems, namely in the United States of America and the United Kingdom - and to the possibility of applying AI-based systems in certain areas: in business management and in the fight against the practice of certain illicit acts or, in the administration of justice, for example, in the application of the penalty by the judge[26].

[25] For example, at the Conference *Access to Justice in the Digital Era - Prospects and Challenge*, held online on 16 July 2020, and *Conference on the importance of Ethics and Human Rights in the regulation of Artificial Intelligence*, promoted by the Slovenian Presidency of the Council of the European Union in July 2021.

[26] Anabela Miranda RODRIGUES, 'Medida da pena de prisão: desafios na era da inteligência artificial', *Revista de Legislação e de Jurisprudência*, no. 4021 (2020), p. 258 f., the same author 'Inteligência artificial no direito penal – a justiça preditiva…, p. 11 f., and, still the same author, 'A questão da pena e a decisão do juiz – entre a dogmática e o algoritmo?, *in*: A

4. Since AI-based systems for predictive justice are not used in Portugal, we don't have any data concerning the assessment of reliability, impartiality, equality, adaptability of these systems.

2. Normative framework law and soft law

1. So far, Portugal has not adopted any legislation specifically addressing "predictive justice".

There are, however, some legal rules which must be considered in case of using AI by public authorities.

Article 35(2) of the CPR states that *the law shall define the concept of personal data, together with the terms and conditions applicable to its automatised treatment and its linkage, transmission and use, and shall guarantee its protection, particularly by means of an independent administrative entity*.

Article 22 of the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), directly applicable in the Portuguese national legal system, regulates the rights of the data subjects regarding *automated individual decision-making, including profiling*. Solely automated decision making is the ability to make decisions by technological means without human involvement[27]. According to Article 22 (1), *the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*. However, paragraph 2 states that paragraph 1 shall not apply (a) *if the decision is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject´s rights and freedoms and legitimate interests*; or (c) *is based on the data subject's explicit consent*. According to paragraph 3, in the cases referred in point (c) of paragraph 2, *the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the*

Inteligência Artificial no Direito Penal (A. M. Rodrigues ed.), Almedina, 2020, p. 219 f.; Rui CARIA, 'O caso State v. Loomis – a pessoa e a máquina na decisão judicial, *in*: A *Inteligência Artificial no Direito Penal* (A. M. Rodrigues ed.), Almedina, 2020, p. 245 f.; and Paulo Sousa MENDES, 'A representação do conhecimento jurídico, inteligência artificial e os sistemas de apoio à decisão jurídica', *in*: *Inteligência Artificial e Direito* (M. L. Rocha / R. S Pereira eds.), Almedina, 2020, p. 51 f. See *infra* point 3 (*General principles of law*).

[27] See Article 29 *Data Protection Working Party - Guidelines for Automated individual decision-making and profiling for the purpose of the Regulation 2016/679* (as last revised and adopted on the 6th of February 2018), p. 8.

right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. And, according to paragraph 4, *decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point a)* [explicit consent of the data subject] *or (g)* [processing necessary for reasons of substantial public interest] *of Article 9(2) applies and suitable measures to safeguard the data subject´s rights and freedoms legitimate interests are in place.* Recital 71 also refers to this problem of the rights of the data subjects regarding automated individual decision-making[28].

On the other hand, Law no. 59/2019, August 8, lays down the rules on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding and preventing threats to public security, transposing into national legal order the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. This law *applies to the processing of personal data wholly or partly by automates means* (Article 2(2)). This law gives a definition of "profiling": for the purposes of the law, "profiling" *means any form of automated processing of personal data consisting of the use of these data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, reliability, behavior, location or movements* (Article 3(1)f). And, according to Article 11, *a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, is prohibited unless authorized by law, which provides the right of the data subject to obtain human intervention on the part of the controller* (1); and *decisions referred in paragraph 1 of this article shall not be based on special categories of personal data referred to in Article 6* [special categories of personal data] (2). Unlike the provisions of Article 22 of the General Data Protection Regulation, article 11 of the Law no. 59/2019 does not expressly provide for the legitimizing effectiveness of the express consent of the data subject, when it comes to automated individual decision-making for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

As we have already mentioned in Part I of this report (Predictive Policing)[29], the Portuguese Charter on Human Rights in the Digital Age (Law no. 27/2021, May 17) is a very innovative legal instrument which appears to be relevant also in the field of predictive justice. In addition to what was previously pointed out, we must emphasize, among others, the right to

[28] About the automated individual decision-making, see A. Menezes CORDEIRO, *Direito da Proteção de Dados*, Almedina, 2020, p. 148 f., and, Mafalda Miranda BARBOSA, 'Dos *expert systems* aos *data systems* AI: impacto ao nível da proteção de dados', *Julgar*, 45 (2021), p. 21 f.
[29] Part I, 3.

cybersecurity (Article 15), according to which *everyone has the right to security in cyberspace, and the State is responsible for defining public policies that guarantee the protection of citizens and information networks and systems, and that create mechanisms that increase security in the use of the Internet, especially by children and young people*; the right of protection against abusive geolocation (Article 17), according to which *everyone is entitled to protection against the illegal collection and processing of information about their location when they make a call obtained from any device* (1), *and the use of data from the geographical position of a user's equipment can only be done with his consent or legal authorization* (2); and the right to digital popular action (Article 21), according to which *in order to defend the provisions of this law, everyone is entitled to the rights provided for in the legislation regarding popular action, duly adapted to the reality of the digital environment.*

2. We are not aware of any government memos, ministerial recommendations or other normative instruments produced by the Portuguese executive authorities dealing with AI-based systems for predictive justice. On a broader level, however, on the use of artificial intelligence, Portugal already adopted the *AI Portugal 2030 – Portuguese National Initiative on digital skills: An innovation and growth strategy to foster AI in Portugal in the European context*[30]. This strategy is aligned with the Coordinated Action Plan of the EU and its Member States and the Portuguese initiative to foster digital skills is included in INCoDe.2030. It considers and promotes a coordinated approach at a European level encouraging the use of AI to help solve global challenges, from health to climate, from transport to agriculture, and from cybersecurity to industry in general. The current text is the result of a two-year dialogue and should continuously evolve as a result of annual reviews and a systematic process of mobilising citizens and key stakeholders. The objectives include economic growth, scientific excellence, and increasing the qualifications of the labour force, particularly with regard to using new technologies, while promoting inclusion and awareness at all levels of education. The growing use of AI should also strengthen societal robustness by building a clear vision of the impacts of AI in democracy, privacy, security, fairness, the labour market, governmental and commercial transparency, and equity. We all know that AI could be highly disruptive in all these dimensions. We hope that if its usage is made ethical-by-design it could provide a set of tools which improve society and democracy.

3. Portuguese criminal justice system does not refer to international or regional normative instruments concerning AI-based systems for predictive justice. It is worth mentioning, however,

[30] Available here: https://ai-watch.ec.europa.eu/index_en#aistrategy

that, as a member of several regional organizations, Portugal recognizes the importance of several instruments adopted and to the work in progress in their respective contexts. For example, in the Council of Europe, besides the ECHR, which must continue to be regarded as a beacon in any regulatory exercise in this area, a considerable number of instruments that must be considered in any regulatory effort in this area were already adopted[31]. There are also other important instruments at the EU[32] and at the OECD[33] level, and it is worth also mentioning some of the UN work regarding AI[34].

4. As far as we know, neither criminal courts, nor the civil and administrative ones, as well as the Constitutional Court have been confronted with AI-based systems used for predictive justice in Portugal.

5. The use of AI-based systems for predictive justice is still unregulated in the Portuguese legislation for the simple reason that they are still not implemented in the public sector. In any case, at this level, we believe that any such solutions would be tailor-made to fit the specificities

[31] To name just a few, we consider the following as being of particular importance: the Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling; the Recommendation of the Parliamentary Assembly of the Council of Europe about Mass Surveillance; the Recommendation of the Parliamentary Assembly of the Council of Europe about Technological convergence, artificial intelligence and human rights; the Recommendation of the Committee of Ministers to member States on guidelines to respect, protect and fulfil the rights of the child in the digital environment; the European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment; the Guidelines on Artificial Intelligence and Data Protection; the Recommendation of the Commissioner for Human Rights 'Unboxing AI: 10 steps to protect human rights'; the Recommendation on developing and promoting digital citizenship education; the Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems; the Declaration by the Committee of Ministers on the risks of computer-assisted or artificial-intelligence-enabled decision making in the field of the social safety net; the Guidelines of the Committee of Ministers of the Council of Europe on upholding equality and protecting against discrimination and hate during the Covid-19 pandemic and similar crises in the future; and the Guidelines of the Committee of Ministers of the Council of Europe on online dispute resolution mechanisms in civil and administrative court proceedings.

[32] We can point out the following: the Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); the Regulation (EU) N 524/2013 of the European parliament and of the council of 21 May 2013 on online dispute resolution for consumer disputes; the Report from the Commission on the application of Directive 2013/11/EU and of the Regulation No 524/13; the Directive 2011/92/EU of December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and a report focusing on the measures against website containing child pornography [2016]; the Directive 2013/40/EU of August 2013 on attacks against information systems; the Study on digital criminal justice - Cross-border digital criminal justice - Final report (June 2020); the study on the use of innovative technologies – final report (April 2020); the EU pages on digitalisation of justice; the White Paper on Artificial Intelligence: a European approach to excellence and trust (February 2020); the Fact sheet on artificial intelligence for Europe (2018); the Communication: "Building trust in Human-Centric Artificial Intelligence" (2019); the Communication: "A European strategy for data" (2020); the Communication: "Artificial Intelligence for Europe" (2018); the Ethics guidelines for trustworthy AI (2018); the Communication: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" (2017); the Conclusions on improving criminal justice in cyberspace (2016); the Internet Organized Crime Threat Assessment (2019).

[33] For instance, the OECD AI Principles; and the OECD Framework for the Classification of AI Systems: a tool for effective AI policies.

[34] For instance, the Recommendation on Artificial Intelligence and Human Rights – "Unboxing artificial intelligence: 10 steps to protect human rights"; and the Recommendation on the Ethics of Artificial Intelligence.

of the area in which they would be implemented (not destined to be marketed). Regarding private solutions – *e.g.*, used by law firms or insurance companies –, we are unaware of such legislation.

6. It is worth to mention the EU horizontal *proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act)*, submitted by the Commission on 21 April 2021 aiming to protect fundamental rights, ensure safety and improve the functioning of the internal market by laying down a uniform legal framework, in particular for the development, placement on the market and use of AI in conformity with Union values. The proposal supports the Union's objective of being a global leader and standard-setter in the development of secure, trustworthy and lawful AI, and, as regulation, it will be directly applicable in all Member States. On the specific field of Justice, the AI proposal does not explicitly prohibit any uses of AI in the judiciary, such as delegating judicial decision-making to an AI system. However, some AI systems that are directly relevant for judicial processes are classified as high-risk under Annex III to the legislative proposal. This includes:

– In the sector of "administration of justice": "AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts" (Annex III, point 8);

– But also some systems listed under "law enforcement" but which could, depending on the exact scope and possibly the Member State concerned, be considered as part of judicial proceedings in criminal matters (Annex III, point 6): "AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences" (point a); "AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person (point b)"; "AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences" (point d).

The proposal clearly states that AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases do not fall under this category (*e.g.* anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks or allocation of resources). Consequently, all AI systems that are developed and used in the judiciary and fall outside of the scope of "high-risk AI system" as defined in Annex III (points 6 and 8) remain unregulated by the AI Act and are only subject to the existing applicable legislation, and to voluntary codes

of conduct (Article 69). Furthermore, the AI Act does not make any distinctions on the use of AI in different types of judicial proceedings despite the fact that the use of AI in criminal proceedings might be considered more sensitive. For example, the Council of Europe's Ethical Charter suggests that in criminal matters a judicial decision processed by AI must be considered with the greatest reservations in order to prevent discrimination based on sensitive data, in conformity with the guarantees of a fair trial.

Concerning this specific question, the proposal clearly establishes that when developing and deploying high-risk AI systems in judicial proceedings (such as predictive justice systems), the AI proposal sets out some obligations that must be followed. They include respect for mandatory requirements relating to data and data governance, documentation and record keeping, transparency, human oversight, robustness, accuracy and cybersecurity. Title III, Chapter 3 places a set of horizontal obligations on providers and other stakeholders, including a general obligation for providers of AI systems used in the judiciary to ensure that the system undergoes a conformity assessment prior to its placing on the market or putting into service (*e.g.* where a system is developed internally and not placed on the market at all), an obligation for a quality management system and risk management system to be implemented throughout the life cycle of the applications concerned and the need to register high-risk AI systems in Annex III which have undergone such conformity assessment procedures in the EU-wide database managed by the Commission. The requirements attached to high-risk systems will have a profound impact both on fundamental rights and on innovation and modernisation.

This said, even though there is currently no legislation specifically designed for these cases, the fact is that, in accordance to what we have just said, it is possible to predict with some degree of certainty the direction of the regulation that will, in the near future, rule the use of these systems in the context of the Union.

3. General principles of law

1. Bearing in mind that AI-based systems for predictive justice are still to be implemented in Portugal, there is no real debate about protecting the right to equality, the right to a fair trial or the presumption of innocence concerning the use of these new technologies[35]. There isn't either a debate on the need to recognize the right of access to a human judge, nor on replacing legal reasoning with mathematical calculation for criminal justice purposes. However,

[35] See *infra*, Part III of this report.

as we have already said, a few of the Portuguese legal scholars have paid attention to this problem, referring to what has happened especially in common law systems, namely in the United States of America and the United Kingdom[36].

Currently, the use of AI-based systems for predictive justice raises legal, epistemological and ethical questions[37]. The objectivity of the decision process carried out through an algorithm can be an advantage, as it suppresses the *arbitrariness* of human decision. But the risk is that of suppressing the necessary *discretion* in judicial decisions, where intuitive thinking or personal valuations take nowadays part of the process. Discretion is inherent in the exercise of the judge's role in any decision-making process that involves determining guilt and punishing those who committed a criminal act. But a "fully automatic algorithmic operation removes from the judicial decision the human dimension and the *responsibility* that only a human being is capable of feeling"[38]. We can hand over the accomplishment of criminal justice to machine intelligence, but – bearing in mind all the problems inherent in that possibility – what we have to decide is whether we *want* to do it and, ultimately, whether we *should* do it[39].

2. In summary, the discussion in Portugal about the positive and negative outcomes of AI-based systems for predictive justice is underdeveloped and lacks a more profound analysis, although its future usage has already raised an undergoing (but still inchoate) reflexion on the consequences it will imply to the general principles of constitutional and criminal law as well as criminal procedure.

[36] See *supra*, Part II of this report, 1.3 and footnote 26.
[37] Anabela Miranda RODRIGUES, 'Inteligência artificial no direito penal – a justiça preditiva entre a americanização e a europeização'…, p. 20.
[38] *Ibidem*, p. 26 and p. 43.
[39] *Ibidem*, p. 49 f.

III. EVIDENCE LAW[40]

1. Introduction

1. The Portuguese system is a legal system (continental system) and the most important current law source of criminal procedure is the 1987 *Code of Criminal Procedure* (hereafter identified as CCP), which entered into force on January 1st, 1988. Besides the CCP, other legislation exists regulating certain chapters or specific issues of criminal law procedure, namely, the problem of evidence gathering.

Matters of criminal procedure are also regulated in the CPR, which provides some of the most important principles concerning criminal procedure: the principle of presumption of innocence; the principle of the accusatorial structure of criminal procedure; the principle of the prohibition of using evidence obtained by torture, coercion or attacks on physical or moral welfare of persons in general; the principle of the inviolability of one's home; and the principle of the publicity of court hearings[41].

2. Since 1988 the Portuguese criminal procedure system is accusatorial, but it recognizes also as its main feature the principle of instruction[42]. Actually, the administration of criminal justice is fundamentally carried out through the activities of two distinct entities, the public prosecutor and the judge, who share between them the functions of investigating/indicting (public prosecutor) and judging (judge) the infraction.

In this accusatorial system of criminal procedure, it is the responsibility of the public prosecutor to investigate the existence of a crime, to find its perpetrators and to discover and gather the necessary evidence with a view to reaching a decision concerning indictment (Article 262 CCP). The public prosecutor in Portugal is a magistrate who benefits from individual status and autonomy in relation to the government (Article 219 CPR). It is his duty, in criminal procedure, to collaborate with the courts in order to discover the truth and do justice, but always obeying criteria of strict objectivity in all his procedural interventions (Article 53 CCP)[43].

---

[40] This part (III) of the report was put through with the collaboration of the Portuguese Public Prosecutor Dr. Pedro Verdelho (Coordinator of the Cybercrime Council),

[41] See Maria João ANTUNES, *Direito Processual Penal*, Almedina, 2021, p. 21 f.

[42] *Ibidem*, p. 25 f.

[43] *Ibidem*, p. 40 f. and 83 f.

However, the structuring of Portuguese criminal procedure according to an accusatorial model is especially related to the adoption of the principle of instruction (Article 340 CCP). According to this principle, courts have the power and duty to clarify and investigate *ex officio* the facts presented to them for judgment. As such, the court itself creates the necessary basis for its decision, independently of the contributions of the prosecution and the defense. Nevertheless, this principle assumes a markedly subsidiary nature as the court's intervention can only occur when it is necessary for the purpose of the whole truth[44].

3. With regard to gathering evidence, the CPR establishes the nullity of the evidence gathered by torture, coercion, infringement of personal physical or moral integrity, forbidden intromission into personal life, the home, correspondence or telecommunications (Article 32(8)). But there are other relevant provisions in the CPR concerning this topic: the rules that provide for the dignity of the human person (Article 1), the right to moral integrity (Article 25(1)), the right to our likeness, to speak out and to protect the privacy of our personal and family life (Article 26), the inviolability of home and correspondence (Article 34) and the right to informational self-determination (Article 35).

Article 26 states, among other rights, the right to the development of personality and the right to protect the privacy of personal and family life. The Constitution does not provide the content and scope of the right to privacy, nor defines what privacy signifies as a legal interest with constitutional protection. Therefore, it is very difficult to determine what belongs to the field of privacy. However, the right to protect the privacy of personal and family life must be understood in relation to the guarantee of the inviolability of home and correspondence (Article 34). And, on the other hand, there is no doubt that the right to privacy imposes limits on the evidence assessment in criminal proceedings when it represents a forbidden intromission into personal life (Article 38(6)).

Article 34(1) provides for the inviolability of home and correspondence, and expressly establishes that personal home shall be inviolable. The same article states that *entry into a citizen´s home may only be ordered by the competent judicial authority and then only in such cases and in compliance with such forms as may be laid down by law* (2). And *no one shall enter any person's home at night without his consent, except in situations of flagrante delicto, or with judicial authorization in cases of especially violent or highly organized crime, including terrorism and trafficking in persons, arms or narcotics, as laid down by law* (3).

[44] *Ibidem*, p. 185 f.

The CPR states also that personal correspondence secrecy and other means of private communication shall be inviolable (Article 34(1)); and that the public authorities shall be prohibited from interfering in any way with correspondence, telecommunications or other means of communication, save in such cases as the law may provide for in relation with criminal proceedings (Article 34(4)).

Article 35 provides for the right to informational self-determination: *every citizen has the right of access to all computerised data that concern him, which he may require to be corrected and updated, and the right to be informed of the purpose for which they are intended, as laid down by law* (1); *the law shall define the concept of personal data, together with the terms and conditions applicable to its automatised treatment and its linkage, transmission and use, and shall guarantee its protection, particularly by means of an independent administrative entity* (2); and *third-party access to personal data is prohibited, save in exceptional cases provided for by law* (4).

And the legislator has laid down, in the CCP, the rules on seizure of correspondence (Article 179) and the rules on wiretapping (Articles 187 to 190).

4. The Portuguese CCP establishes the principle of legality of evidence, defined as the admission of all forms of evidence not forbidden by law (Article 125). All evidence obtained by torture, coercion or, in general, by infringement of personal physical or moral integrity is null and cannot be assessed (Article 126(1)). Excepting the cases established by law, all evidence obtained by intromission into personal life, the home, correspondence or telecommunications without the consent of the owner is null and cannot be assessed (Article 126(3))[45].

5. Besides the CCP, there are other laws that regulate the gathering and assessment of evidence. It is worth to mention the laws that regulate photographic records (Law no. 5/2002, January 11), video-surveillance (Law no. 95/2021, December 29) and digital evidence (Law no. 109/2009, September 15).

Law no. 5/2002 establishes measures to combat organized and economic-financial crime. This law states that, by order of the judge, when necessary to investigate certain offences (referred to in Article 1 of the law), the record of voice and image is allowed by any means without consent of the person (Article 6).

[45] Concerning forbidden evidence, see Manuel da Costa ANDRADE, *Sobre as proibições de prova em processo penal*, Coimbra Editora, 1992, *passim*. Exceptionally the CPP allows the assessment of prohibited evidence. If the way people obtain prohibited evidence (under Article 126) constitutes a crime, the prohibited evidence can be used to prosecute the agents of the crime (Article 126(4) CPP). In the Portuguese Penal Code we can find the crime of torture and other cruel, inhuman or degrading treatment (Articles 243 and 244).

Law no. 95/2021, regulates the use and access, by the security forces and services and by the Portuguese National Authority for Civil Protection, of video surveillance systems which collect, record and process image and sound data, in public spaces and also in private spaces of public access[46]. When a video camera records the commission of a crime, the security service must report the fact to the public prosecutor (Article 18).

The Law no. 109/2009 (known as *Cybercrime Law*) establishes substantive and procedural criminal provisions, as well as provisions relating to international cooperation in criminal matters, relating to the field of cybercrime and the gathering of evidence in electronic form, transposing Framework Decision 2005/222/JHA, of the Council, of 24 February, concerning attacks against information systems, and adapting domestic law to the Convention on Cybercrime of the Council of Europe (Article 1).

6. Until this Cybercrime Law came into force, there were no special rules in Portugal regarding the gathering of evidence in electronic form. The gathering of evidence in cyberspace was carried out using the general rules of the CPP. The Cybercrime Law sought to condense into a single piece of legislation all the special rules concerning cybercrime: rules of substantive law, rules of procedural law and rules relating to international judicial cooperation[47].

Article 11 of the Cybercrime Law defines the scope of application of procedural provisions. This rule establishes that the procedural rules provided for, with the exception of the provisions of article 18 (interception of communications) and article 19 (covert actions), apply: (a) to proceedings relating to crimes provided for in the law itself (in Articles 3 to 8); (b) proceedings relating to crimes committed through a computer system; and (c) proceedings relating to crimes in which it is necessary to gather evidence in electronic form. The Cybercrime Law thus comprises a general regime on the gathering of evidence in electronic form, applicable to proceedings for any crime (these are not specific procedural rules for the cybercrime sector).

The procedural dimension of the Cybercrime Law is the most innovative and one of the most important of this law. This law provided for new means of gathering evidence: expedited preservation of stored computer data (Article 12); expedited preservation of traffic data (Article 13); and the production order (Article 14). On the other hand, through this law, some 'traditional' criminal procedure institutes were adapted to the gathering of evidence in cyberspace. This is what happened with the search of stored computer data (Article 15); the seizure of stored

[46] See Part I of this report, 2.

[47] See Sónia FIDALGO, 'A apreensão de correio eletrónico e a utilização noutro processo das mensagens apreendidas', *Revista Portuguesa de Ciência Criminal*, 2019, p. 59.

computer data (Article 16); the seizure of electronic mail and records of communications of a similar nature (Article 17); the interception of communications (Article 18); and covert actions in a digital environment (Article 19). The Cybercrime Law does not regulate, however, the use of malware as a means of evidence gathering. The use of malware is a clear violation of the fundamental rights of those affected, therefore, as long as it is not expressly regulated by law, it cannot be used as a means of evidence gathering[48].

Article 15 of the Cybercrime Law regulates the search of stored computer data. As a rule, it is the competent judicial authority – judge or public prosecutor – that authorizes or orders the carrying out of the search, and should, whenever possible, preside over the investigation (Article 15(1)). Article 15(3) provides, however, for cases in which the criminal police may carry out the search, without prior authorization from the judicial authority: *when the search is voluntarily consented by whoever has the availability or control of such data, provided that the consent given is, in any way, documented* (a); *in cases of terrorism, violent or highly organized crime, when there are well-founded indications of the imminent practice of a crime that puts the life or integrity of any person at serious risk* (b). As for the execution of searches (Article 15(6)), the rules provided for in the CCP (Article 174 f.) and in the Journalist Statute[49] are applicable, with the necessary adaptations.

2. Evidence gathering through AI based systems

1. In Portugal, there is not a specific normative framework ruling the use of AI-based systems to gather evidence.

However, we may mention once again the Law 59/2019, of August 8[50], which lays down the rules on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This law *applies to the processing of personal data wholly or partly by automates means* (Article 2(2)). And, according to Article 11, *a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, is prohibited unless authorized by law, which provides the right of the data subject to obtain human intervention on the part of the controller* (1); and

[48] See Sónia FIDALGO, 'A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo', *in*: *A Inteligência Artificial no Direito Penal* (A. M. Rodrigues ed.), Almedina, 2020, p. 153 f.
[49] Law no. 1/99, January 13.
[50] See Part II of this report, 2.1.

decisions referred in paragraph 1 of this article shall not be based on special categories of personal data referred to in Article 6 [special categories of personal data] (2).

And we may also refer to what has already been stated before about the Portuguese Charter on Human Rights in the Digital Age (Law no. 27/2021, May 17)[51] as its regulation is also relevant in the field of evidence gathering and its forward use in criminal proceedings.

2. In Portugal, AI-based systems are not used to process and sort through large quantities of documents and communications to gather evidence of a crime. This kind of systems are also not used to extract data from mobile devices and analyse that data to gather evidence. One of the techniques used in the search of stored computer data involves the use of algorithms, which help to look for similar data based on a sample or a digital signature ("hash signature")[52]. These are semi-intelligent or semi-autonomous systems, but they do not use AI-based techniques in the proper sense. Therefore, the Portuguese courts have never been confronted with the use of AI-based systems to gather evidence.

Although these AI-based systems are not used to gather evidence, the police services in general, but specially the Portuguese Criminal Police – Polícia Judiciária (PJ) – are committed to the development of numerous projects concerning the future use of AI systems in the field of criminal prevention and investigation, in cooperation with the European institutions. Those "investigation and development projects" mainly integrate the Horizon 2020 EU Program. We have already referred to those projects in the Part I of the report (Predictive Policing), but some of them aim not only to prevent crime, but also to change information and to gather / exchange digital evidence (*e. g.*, Project CREST; Project AIDA; Project INFINITY; Project RISEN; and Project CONNEXIONs)[53].

3. In Portugal there is still very little discussion about the use of AI-based systems to gather evidence. Very few of the Portuguese legal scholars have paid attention to this problem, referring to what has happened in other countries[54]. The use of AI-based systems to gather digital evidence raises problems from a double point of view: from the point of view of the right to privacy and from the point of view of the exercise of the defendant's right of defense[55]. From the point of view of the right to privacy, the admissibility of the use of such techniques will always depend on a

[51] See Part I of this report, 3, and Part II, 2.1.
[52] In Portugal, the Criminal Police uses the *ADF Inspector* program.
[53] See Part I of this report, 1.
[54] See Sónia FIDALGO, 'A utilização de inteligência artificial…', p. 129 f.
[55] *Ibidem*, p. 137.

prior intervention by the legislator, which defines the terms in which AI techniques can be used. This is truly 'automated evidence'[56] and, therefore, when the Portuguese legislator regulated the *traditional* computer searches, it did not count on the possibility of using AI techniques, and it did not make the necessary proportionality judgment[57].

On the other hand, for the right of defense to be considered assured, the opportunity which is given to the defendant to counter the evidence must be *effective*. When automatic learning techniques have been used to gather the evidence, the possibility of counteracting this *automated evidence* will clearly be impaired. Therefore, in the field of gathering evidence in a digital environment, only the use of *explainable* and *transparent* AI systems could be admitted[58].

3. Evidence produced by AI-based systems

1. AI-based systems that perform facial recognition and/or voice recognition (or other kinds of evidence) are not used in Portugal to produce evidence for the purpose of criminal justice.

2. In Portugal there isn't a normative framework governing evidence-producing AI-based systems and their use over the course of the criminal process. There isn't yet significant academic debate regarding the use of AI-based systems for producing evidence.

3. As we have already stated, the Portuguese CCP establishes the principle of legality of evidence, defined as the admission of all forms of evidence not forbidden by law (Article 125 CCP). The CPP thus admits all means of evidence that are not prohibited, even if they are *atypical* means of evidence (means of evidence not expressly provided for in the law). Thus, a certain *freedom of the means of evidence* is affirmed, because the legislator is unable to anticipate the technical-scientific developments applicable in gathering evidence. The admissibility of atypical evidence is justified precisely in situations where technological progress is ahead of the legislator's ability to predict. However, when the atypical evidence implies a significant restriction of fundamental rights (for example, a restriction of the right to privacy), its

[56] The expression 'automated evidence' is used by Serena QUATTROCOLO / Cosimo ANGLANO / Massimo CANONICO / Marco GUAZZONE, 'Technical Solutions for Legal Challenges: Equality of Arms in Criminal Proceedings', *Global Jurist*, vol. 20, 1 (2020), p. 7-8.
[57] Sónia FIDALGO, 'A utilização de inteligência artificial…', p. 151.
[58] *Ibidem*, p. 146.

admissibility will always depend on the prior intervention of the legislator (Articles 18(2) and 34(2) (4) CPR)[59]. Therefore, we would say that, for instance, the drowsiness detection and distraction warning system embedded in an automated vehicle could be used as evidence in criminal proceedings, unless we conclude that such evidence implies a sensitive restriction of fundamental rights. In that case, there must be a law that expressly regulates this means of evidence.

However, the use of this information provided by AI-based systems as evidence in criminal proceedings could also be problematic either from the point of view of the right of defence, or from the point of view of the presumption of innocence.

4. In Portugal there no specific exclusionary rules concerning AI-produced evidence. As we have already mentioned, as a general rule all evidence obtained by torture, coercion or, in general, by infringement of personal physical or moral integrity is null and cannot be assessed (Article 126(1) CCP). Excepting the cases established by law, all evidence obtained by intromission into personal life, the home, correspondence or telecommunications without the consent of the owner is null and cannot be assessed (Article 126(3) CCP).

5. The Convention on Cybercrime of the Council of Europe was approved in Portugal in 2009[60] and, as we have already said, the Cybercrime Law (Law no. 109/2009) has adapted the domestic law to this Convention. However, neither the Cybercrime Convention nor the Portuguese Cybercrime Law expressly regulate the admissibility of AI-produced evidence.

4. Evidence assessed through AI-based systems

1. In Portugal, AI-based systems are not used as a tool – at least not yet – to help judges, courts or regulators in order to assess criminal evidence. As far as we know, the Portuguese courts have never been confronted with judicial decisions or criminal judgements for which the evidence was assessed with the help of AI-based systems. We also acknowledge that there is no significant academic debate on this issue.

[59] See Manuel da Costa ANDRADE, 'Proibições da prova em processo penal (conceitos e princípios fundamentais', *Revista Jurídica da Universidade Portucalense*, 13 (2008), p. 147.
[60] Resolution of the Assembly of the Republic no. 88/2009, September 15; ratified by the Decree of the President of the Republic no. 91/2009, September 15.

2. In conclusion, the Portuguese legal system doesn´t include a specific normative framework ruling the use of AI-based systems to gather criminal evidence, to produce evidence or to assess evidence. In our country there is still very little discussion about the use of AI-based systems for these purposes. However, as we have already mentioned, some Portuguese legal scholars have reflected about some of these topics and are aware of the problems they rise, essentially by referring to what has happened in other countries.