GREEK REPORT ON AI AND ADMINISTRATION OF JUSTICE

By Maria Kaiafa Gbandi[*]*, Athina Sachoulidou*[*] *and Dafni Lima*[*]

Abstract

While the EU is close to achieving the ambitious goal of being the first regional actor to regulate the design and use of AI systems and the implications thereof for fundamental rights by means of a dedicated legal instrument, 'AI and criminal law' continues to present national legislators with significant challenges. In numerous legal orders, predictive policing, predictive justice, AI-generated evidence or AI-supported crime analytics may have already attracted scholarly attention, but their regulation is still pending or limited to soft-law interventions. This is also the case with the Greek legal order which has recently started navigating the AI realities in law enforcement and criminal justice settings. This report embarks to provide an overview of the national practices in the areas of automated policing and criminal justice, the normative frameworks that govern them and the applicable general principles of law. In doing so, it underlines the specificities of employing AI in a sensitive area of public governance, namely the administration of criminal justice, and showcases the need for dedicated procedural safeguards.

1 Introduction

While artificial intelligence (AI) has captivated our collective imagination for decades, recent technological developments have rendered possible an unprecedented growth in the deployment of AI systems. From automated vehicles and AI-powered image recognition to virtual assistants and sophisticated chatbots, AI is gaining ground across different industries. One particular area where the use of AI can present unique challenges is in the administration of justice more broadly, through the use of AI in a variety of ways connected to the justice system, with data mining algorithms showing the potential to perform tasks traditionally performed by human agents in the context of administrative and judicial decision-making as well as legal counselling. These challenges are heightened in the case of criminal justice in particular, which is notable for its far-reaching grip on the individual.

AI can be of particular use to predictive policing and criminal justice – yet it is evident that the law in Greece has not quite caught up with the implications of this potential. While certain steps have been taken towards harnessing AI in law enforcement databases, smart policing devices, and surveillance mechanisms, the legislative framework still mostly approaches AI in more abstract terms, falling back onto broader rules related to human rights, data protection, and general criminal law principles. The use of AI in predictive function within the Greek criminal justice system has not yet drawn sufficient attention. This report seeks to close this gap by examining the current and potential use of AI and the risks it poses in the administration of justice in the Greek legal order.

The first part of this report focuses on predictive policing and the second on predictive justice, taking turns to explore the national practices on the ground, provide a comprehensive overview of the relevant normative framework, and showcase and reflect on the relevant general principles of law. In the third part, it moves on to explore the impact of AI on evidence law within the criminal justice system, and more specifically regarding evidence gathered through, produced by, and assessed through AI.[1] In doing so, it also illustrates the relevant risks posed to the robustness of the criminal justice system and its safeguards for the individual.

[*] Maria Kaiafa Gbandi (corresponding author), Professor in Criminal Law, School of law, Aristotle University of Thessaloniki, Greece, kaiafagb@law.auth.gr.

* Athina Sachoulidou (co-author), Assistant Professor in Criminal Law, CEDIS, NOVA School of Law, Universidade Nova de Lisboa, Portugal, athina.sachoulidou@novalaw.unl.pt.

* Dafni Lima (co-author), Assistant Professor, Durham Law School, Durham University, UK, dafni.lima@durham.ac.uk.

[1] The structure of this report corresponds to the structure of and the questions included in the questionnaire on AI and criminal justice Professor Juliette Lelieur drafted on behalf of the International Association of Penal Law.

2 Predictive policing

2.1 National practices

Greek law distinguishes between *administrative* police investigations that aim at crime prevention (Arts. 74 (15), 93 (1), 94, 96, 99 Presidential Decree 141/1991) and those that are repression-oriented and, thus, pertain to the *criminal procedural mechanism* (Art. 93 (2), 95 Presidential Decree 141/1999). The latest Sectoral Development Programme (SDP) of the Hellenic Ministry of Citizen Protection encompasses, *inter alia*, actions of targeted policing by means of a systematic analysis of statistical crime data that enables the creation of prediction models.[2] The focus seems to lie on criminality trends and the so-called "hot spots", but there is no explicit reference to *predictive policing*, a term that has not yet been defined, nor used extensively, in the domestic legal order. [3] The Greek legislator has only adopted rules in a neighbouring area, namely the use of audio and video recording surveillance systems in public spaces (Presidential Decree 75/2020).

According to the existing sources of information, Geographic Information System (GIS) infrastructure is available at the IT Directorate of the Hellenic Police Headquarters. This includes a Web-Application GIS Server, on which *CrimeView* (a software extension to ArcGIS developed and maintained by Esri)[4] is also installed, and a Geodatabase Server, which hosts a geographical database (Oracle 10g) and a software enabling the interface and the synchronisation between the CrimeView application and the Record of Offences and Incidents. *CrimeView* enables cartographical mapping of crime location, provides for search filters per offence type, geographical or administrative entity, date or similar information, visualises the crime density map by geographical entity, the map of recurring calls, diagrams and timetables of offences, and creates reports encompassing details and the timing of incidents. [5] According to reports in the press, *CrimeView* was employed in the period between 2008 and 2011 and was withdrawn afterwards.

There are, however, some recent developments indicating the intention of the Greek state to invest in automated law enforcement. In 2019, the Hellenic Police Directorate of the Ministry of Citizen Protection signed a 4-million contract with Intracom Telecom in the context of the 'Smart Policing' project. According to the technical specifications documents published by the Hellenic Police, this is a project aiming to facilitate the identification and verification of citizens' identity when stopped by the police, enhance security and reduce the risk of offenders absconding. The handheld electronic "smart phone" type devices are intended to be used by police officers to take a close-up photograph of the individual under inspection and to collect his/her fingerprints.[6] The respective data will be compared to that stored in databases held by national and international authorities, including Interpol, the US Federal Bureau of Investigation (FBI), the Hellenic Ministries of the Interior, Transport, and Foreign Affairs as well as Teiresias, a credit bureau offering its services in Greece. As regards the implementation of this project, the available information suggests that the procurement of all subsystems for the program was accomplished on 5 September 2021 (see Section 2.1.3).[7] Regarding further plans of employing

[2] Sectoral Development Programme (SDP) of the Ministry of Citizen Protection 2021–2025, Government Gazette 3630/6.8.2021.

[3] Greek scholars usually refer to predictive policing using definitions suggested in international scholarly works or policy reports. E.g., Grigoris Tsolias, 'Personal data processing by law enforcement agencies: between privacy and safety' [in Greek] (2020) 4 DITE 573, 575–576.

[4] ESRI ArcGIS <https://www.esri.com/en-us/arcgis/about-arcgis/overview> accessed 4 May 2023.

[5] Hellenic Police, 'Technical specifications in the context of the implementation of the action "Smart Policing" of the Internal Security Fund's (ISF) Programme 2014-
2020' [in Greek] (2018) <http://www.astynomia.gr/images/stories/2018/prokirikseis18/26052018texnikesprodiagrafes.pdf> accessed 4 May 2023, 12.

[6] Hellenic Police, 'Technical specifications' (n 5); Intracom Telecom 'Intracom Telecom Undertakes a "Smart Policing" Project' (2020) <http://www.intracom-telecom.com/en/news/press/press2019/20190702.htm> accessed 4 May 2023; Eleftherios Chelioudakis, 'Greece: Technology-led policing awakens' (2020) <https://aboutintel.eu/greece-policing-border-surveillance/> accessed 4 May 2023.

[7] Hellenic Police, 'Response to "Letter by Ms. LAMA Fakih regarding the Hellenic Police's new "smart policing" program"' (2022) <https://www.hrw.org/sites/default/files/media_2022/01/Letter%20from%20Hellenic%20Police_EN.pdf> accessed 4 May 2023.

means of automated law enforcement, it is also worth noting that Greece is represented in various research consortia of this kind (e.g., SPIRIT,[8] COPKIT,[9] ANITA,[10] and CONNEXIONs[11]).[12]

Access to information about the technical features of the existing infrastructure and the devices that are currently under development or the data those (will) process or the general framework of their (planned) use is rather limited. The existing information allows the following categorizations:

2.1.1 CrimeView

The input data consists of the type (What), the location (Where) and the timing (When) of the offence; in a word: historical crime data.[13] There is, however, no publicly accessible information as to where this software has been (or is) employed or whether its use has been (or is) limited to specific criminal activities. No safe conclusion can be reached as regards the public perception of its use inasmuch as we detected just a single reference to it in the Greek media, where the presentation of the software has been rather neutral, including just a brief comment as to the chances associated with its use for improving law enforcement. [14]

2.1.2 Audio and video recording surveillance systems

The Presidential Decree 75/2020 encompasses the rules that shall govern the use of audio and video recording surveillance devices, whether fixed or portable, in public spaces (Art. 1), *irrespective of their technical specifications*. These devices may be installed and deployed for preventing and repressing the criminal offences listed in Art. 14 (1) lit. b–d Act 3917/2011; that is, treason, offences against the public order, violent crimes, drug trafficking, common endangerment offences, crimes against road safety, and crimes against property (Art. 3 lit. a). Besides this, they may serve traffic control purposes (Art. 3 lit. b). Such devices may be used by the Hellenic Police, the Hellenic Fire Service and the Hellenic Coast Guard (Art. 4). When employed for traffic control purposes, image data processing is to be limited to identification of car templates and categories (Art. 7 (1)). Audio data recording and processing shall be disabled, unless there is a duly justified decision of the data processor that needs to be approved by the competent prosecutor – with the aim of detecting and identifying individuals involved in the commission of the aforementioned crimes (Art. 7 (2)).

The use of surveillance systems of this kind in public spaces has been scrutinised by the Hellenic Data Protection Authority (Hellenic DPA) prior to the adoption of the Presidential Decree 75/2020, in order to ensure the compliance of the respective provisions with fundamental rights. The intervention of the Hellenic DPA has been welcomed by Greek scholars, who highlighted the need to strike the right balance between the extensive use of surveillance for law enforcement purposes and the protection of citizens.[15] Today, the information available at the website of the Hellenic Police dictates that the latter already make extensive use of video and audio recording surveillance systems. There is, however, no information available as to whether and to what extent the use of such systems has led to concrete changes in policing methods.

2.1.3 Smart policing devices

The smart policing devices funded by the EU Commission's Internal Security Fund and manufactured by Intracom Telecom for the Hellenic Police[16] are designed to collect biometric data, namely scan people's faces and

[8] Spirit <https://www.spirit-tools.com/> accessed 4 May 2023.
[9] COPKIT project <https://copkit.eu/> accessed 4 May 2023.
[10] ANITA project <https://www.anita-project.eu/index.html> accessed 4 May 2023.
[11] CONNEXIONs project <https://www.connexions-project.eu/main/project-overview> accessed 4 May 2023.
[12] Eleftherios Chelioudakis 'Greece/Research' in Fabio Chiusi, Sarah Fischer, Nicolas Kayser-Bril and Matthias Spielkamp (eds), *Report Automating Society* (AlgorithmWatch GmbH and Beterlsmann Stiftung 2020) <https://automatingsociety.algorithmwatch.org/> accessed 4 May 2023, 131–140, 133–135.
[13] Hellenic Police, 'Technical specifications' (n 5) 12.
[14] Panagiotis Spyropoulos 'Crime View, a useful GPS for combating crime' [in Greek] (2017) <https://www.thetoc.gr/koinwnia/article/crime-view-ena-xrisimo-gps-gia-tin-pataksi-tis-egklimatikotitas/> accessed 4 May 2023.
[15] E.g., Elisavet Symeonidou-Kastanidou, 'Remarks on the Hellenic DPA's Opinion 3/2020' [in Greek] (2020) 8-9 Poiniki Dikaiosini 957–961.
[16] Intracom Telecom announced on 15 July 2022 that the project 'Smart Policing' was awarded a prize, after ranking first in the 'Best Implemented Idea' category in the 'Security of Citizens' thematic area, by the General Secretariat of Digital Governance and Process Simplification of the Ministry of Digital Governance as part of the annual Digital Governance Competition. See Intracom Telecom,

fingerprints.[17] Under this programme, the device users should also be enabled to scan vehicle licence plates.[18] According to the information provided by the Hellenic Police Directorate regarding the system's functions, the operator of each device should perform searches mainly by scanning valid travel identification documents or by typing data – with the 'Smart Policing' project aiming to digitalise already existing procedures for checks on persons, vehicles and objects. The biometric data gathered through these devices are to be compared, as mentioned above, with data already stored in existing national and European criminal databases, to which Greek law enforcement authorities have access, and in the Greek citizen identity card file record, but not –pursuant to the same information– with data stored in biometric databases of third parties or other private-public databases.[19] Besides this, the Hellenic Police inform that the biometric data collected during a check on a person is to be deleted in an automated way as soon as the search begins and is not to be stored in any database of theirs even in cases where there is a match.[20] Next, they list three safeguard measures: 1) the exclusive use of the devices by uniformed personnel in the performance of their duties, 2) built-in security measures that prevent unauthorised use of the system's resources and ensure their rational use, and 3) recording of all end-user actions in a special log file under the direct supervision and control of the competent national bodies.[21] According to further information available in the press, the smart policing devices are intended to be used across the country and without any limitation as regards the kind of criminal activity at stake.[22] Notwithstanding the above, it has been argued that the identification of individuals violating national migration laws will be prioritised giving, thus, rise to discrimination concerns[23] – with the Hellenic Police responding that it is only identification data (e.g., surname, name, data of birth, travel document number) that will serve as a criterion for performing a search on persons and not the racial characteristics thereof or his/her religious, political or other beliefs.[24]

The purchase of this new equipment, the actual use of which could not be confirmed based on the publicly available information, is linked to the expectation of efficient law enforcement, rapid and reliable identification of individuals, vehicles and other objects. [25] This is aligned with the overall plan of Hellenic Police's modernisation that includes the use of new technologies with the aim of preventing and repressing crime successfully, safeguarding public peace, increasing the resilience of the Greek society towards crisis and disaster as well as contributing to social welfare and the country's development.[26] In this context, the main characteristics of the internal security and borders management system the Hellenic Police aims to develop include: 1) information-based, intersectoral administration and decision-making procedures; 2) a comprehensive model of dangerousness assessment that will enable police officers to take appropriate preventive and repressive measures; 3) the horizontal standardisation of service operation on a three-fold basis: *prediction* (analysis of information for detecting tendencies, hot spots, days and times of increased danger per region) – *prevention* (targeted policing on the basis of prediction models) – *response* (intervention and pre-trial investigation); and 4) situational awareness and common operational picture enabled by networks of sensors (cameras, radars, portable technologies, telematics), including interfaces with other authorities and interconnected infrastructures, and reliable ICTs. [27]

The modernization of Hellenic Police, including but not limited to the (future) use of predictive policing software or smart policing equipment, is placed within the overall context of the transition from the Information Era to

'Distinction for the "Smart Policing" Project in Greece that was developed by Intracom Telecom' (2022) <https://www.intracom-telecom.com/en/news/press/press2022/2022_07_15.htm> accessed 4 May 2023.

[17] Chelioudakis, 'Greece' (n 6).

[18] Hellenic Police, 'Technical specifications' (n 5) 26–31.

[19] Hellenic Police, 'Response' (n 7) 2.

[20] *Ibid*.

[21] *Ibid*.

[22] Spyropoulos (n 14).

[23] Corina Petridi, 'Flush with EU funds, Greek police to introduce live face recognition before the summer' (2021) <https://algorithmwatch.org/en/greek-police-live-facial-recognition/> accessed 4 May 2023; Human Rights Watch, 'Greece: New Biometrics Policing Program Undermines Rights. Risk of Illegal Racial Profiling and Other Abuses' (2022) <https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights> accessed 4 May 2023.

[24] Hellenic Police, 'Response' (n 7) 2–3.

[25] Hellenic Police 'Contract for the Purchase of Smart Policing Systems' (2019) <http://www.astynomia.gr/images/stories/2019/prokirikseis19/14122019anakoinosismartpolicing.pdf> accessed 4 May 2023.

[26] Sectoral Development Programme (SDP) of the Ministry of Citizen Protection 2021–2025, Government Gazette 3630/6.8.2021, 48270–48271.

[27] *Ibid*, 48286-48287.

that of AI. More specifically, the main objectives pursued by employing new technologies in the realm of law enforcement are the reduction of operational costs, the rational use of human resources and the increase of efficiency. The question of whether the stated objectives are different from those actually pursued cannot be addressed without access to reliable empirical data about the actual use of such technologies by the Hellenic Police.

Irrespective of this, it is important to stress that the civil society has already reacted to the 'Smart Policing' project. In March 2020, Homo Digitalis, a national, non-profit digital rights advocate, filed a request for opinion to the Hellenic DPA with respect to the implications of the contractual agreement between the Hellenic Police and Intracom Telecom for privacy and data protection.[28] The main claim was that biometric data processing shall be authorised by Union or Member State law, be strictly necessary and subject to appropriate safeguards for the rights and freedoms of the individuals concerned as provided for in the Directive (EU) 2016/680 (known as the Law Enforcement Directive (LED)) – with none of these criteria being fulfilled in this case.[29] The focus particularly lay on the lack of a legal basis for collecting biometric data during police stops, the adequacy of the existing means and procedures for identifying individuals and offenders and the high risks to the rights and freedoms of data subjects that make a prior data protection impact assessment (DPIA) and the consultation of the national DPA necessary.[30] The Hellenic DPA addressed the aforementioned request in *August 2020* by informing Homo Digitalis that the Hellenic Police was requested to provide information about the smart policing contract, the legal basis for the intended processing of biometric data, the data retention period, and the information to be provided to data subjects.[31] Further information has been requested as to whether the Hellenic Police has conducted a DPIA – with the national DPA highlighting that a DPIA is to be conducted not only prior to the operation of the new devices, but also prior to their supply, in order to ensure compliance with privacy-by-design requirements.[32] On 11 October 2022, the Hellenic DPA confirmed that it was reviewing the 'Smart Policing' programme.[33] To date, there is no publicly accessible information as to the outcome of this review.

2.2 Normative framework

Personal data processing for preventing future crime falls into the scope of administrative police investigations (Arts. 74 (15), 93 (1), 94, 96, 99 Presidential Decree 141/1991).[34] The LED, as transposed by Act 4624/2019 (Chapter 4), provides for personal data processing of this kind – with Art. 70 (1) lit. b Act 4624/2019 referring to persons for whom there are substantial reasons to believe that they are about to commit a criminal offence in the future. This implies that preventive measures in the kind of personal data processing may be taken before the commission of a crime.[35]

As regards predictive policing *per se*, there are *no specific legal rules*. The Presidential Decree 75/2020, which was adopted to govern the use of audio and video recording surveillance systems in public spaces, does not address AI-based surveillance systems. However, this possibility was discussed by the Hellenic DPA when commenting on the respective draft legislation. More specifically, the Hellenic DPA noted that the future installation and use of additional equipment, including software enabling further audio and video processing, may make independent and individual data processing of different kinds (compared to the data processing activities originally envisaged) possible. This could be the case, should facial recognition software or other AI systems be deployed. In such a case, data processing principles, the principle of legality and the requirements set out in Arts. 7–8, 52 (1) CFR and Art. 8 ECHR are to be met.[36]

---

[28] Homo Digitalis, 'Request for the Greek DPA's opinion on the Greek Police Agreement on Smart Policing' (2020) <https://www.homodigitalis.gr/en/posts/5381> accessed 4 May 2023.
[29] Chelioudakis, 'Greece' (n 6).
[30] *Ibid*.
[31] Homo Digitalis, 'The Greek DPA investigates the Greek Police' (2020) <https://www.homodigitalis.gr/en/posts/7684> accessed 4 May 2023.
[32] *Ibid*.
[33] Human Rights Watch (n 23).
[34] Cf. Tsolias (n 3) 575.
[35] *Ibid*.
[36] Hellenic Data Protection Authority (DPA), 'Legal Opinion 3/2020' (2020) <https://www.dpa.gr/sites/default/files/2020-07/gnomodotisi%2032020.pdf> accessed 4 May 2023, 17.

As to the *future plans* to adopt rules to govern predictive policing, Greece is in the process of developing its national AI strategy – an effort coordinated by the Hellenic Ministry of Digital Governance (MDG).[37] The latter has also published the 'Digital Transformation Bible 2020-2025', which highlights, *inter alia*, the medium-term goal of employing AI in the field of public administration and creating an AI and machine learning platform, and presents various plans for this purpose (e.g., AI-driven mechanisms for supporting public audit institutions to combat tax evasion and to control public procurement).[38] Despite the great variety of the scheduled actions, there is *no concrete reference* to plans of employing predictive policing AI systems or similar.

Irrespective of the current lack of regulation, should the Proposal for an EU Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act (AIA))[39] be adopted, Greece will be obliged to comply with the rules the latter includes when shaping the respective national legal framework. It is worthy to mention that AI systems intended to be used for predictive policing purposes have been classified as 'high-risk' in this context (Art. 6 (2); Annex III 6 lit. a and e EU AIA).[40] To place such systems on the market and use them, it will be mandatory to assess their compliance with a set of requirements included in the EU AIA (Arts. 8–15). On the contrary, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement shall be prohibited, 'unless and in as far as such use is strictly necessary' for the law enforcement objectives that are listed exhaustively in Art. 5 (1) lit. d EU AIA.

Besides this, to date, there are no (publicly accessible) memos, ministerial recommendations or other normative instruments that address the topic of AI-supported predictive policing. Soft-law sources or private sector regulations of this kind could not be detected either. The same applies as regards references of the national criminal justice system to international or regional normative instruments issued in this area. This is not surprising, considering the scarce (if any) use of *CrimeView* by the Hellenic Police and the level of progress of the 'Smart Policing' project. Similarly, there is no case law regarding the use of AI systems for predictive policing purposes; that said, Greek scholars often refer to foreign jurisprudence when seeking to discuss predictive or smart policing.[41]

Nevertheless, there are two decisions of the Hellenic DPA that may impact on the future use of AI systems for predictive policing purposes. *First*, on 16 October 2018, the Hellenic DPA issued a list encompassing the types of data processing activities that presuppose a DPIA in accordance with Art. 35 (4) Regulation (EU) 2016/679, known as the General Data Protection Regulation (GDPR)[42].[43] The suggested criteria are divided into three categories: 1) kind and purpose of data processing; 2) type of data and/or categories of data subjects; and 3)

---

[37] European Commission and OECD, 'AI Watch. National Strategies on Artificial Intelligence. A European perspective. 2021 Edition – a JRC-OECD report' (2021) <https://publications.jrc.ec.europa.eu/repository/handle/JRC122684> accessed 4 May 2023, 70.

[38] Hellenic Ministry of Digital Governance (MDG), 'Digital Transformation Bible 2020-2025' (2021) <https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digitalstrategy.pdf> accessed 4 May 2023, 165.

[39] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM (2021) 206 final.

[40] The classification of predictive policing as high-risk AI remained intact after the release of the latest compromise text (19 October 2022) and the Council's General Approach to EU AIA (25 November 2022). See Council, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Fourth Presidency compromise text' (2022) <https://data.consilium.europa.eu/doc/document/ST-13102-2022-INIT/en/pdf> accessed 4 May 2023; Council, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach' (2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> accessed 4 May 2023. On the other hand, the European Parliament's Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs have recently voted in favour of a ban on predictive policing AI systems. See Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs, 'Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)) Rapporteurs: Brando Benifei & Ioan-Dragoş Tudorache' <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence> accessed 23 May 2023.

[41] E.g., Kyriakos Kotsoglou, 'Smart Policing? Prevention – Repression – Human Rights' [in Greek] (2021) 143 Synigoros 48, 51–52.

[42] 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).

[43] Hellenic Data Protection Authority (DPA) 'Decision 65/2018' (2018) <https://www.dpa.gr/el/enimerwtiko/prakseisArxis/katalogos-me-ta-eidi-ton-praxeon-epexergasias-poy-ypokeintai-stin> accessed 4 May 2023.

additional characteristics of or means deployed for data processing.[44] The combined use of these criteria implies that data processing by means of an AI-based predictive or smart policing system would require a DPIA on the part of the data controller according to Art. 35 GDPR. *Second*, as mentioned above, the Hellenic DPA issued Opinion 3/2020 regarding the use of audio and video recording surveillance systems in public spaces, where it states that AI-driven data processing for policing purposes shall meet the requirements set out by Arts. 7–8, 52 (1) Charter of Fundamental Rights of the EU (CFR) and Art. 8 European Convention on Human Rights (ECHR).

As particularly regards the guarantees of reliability, impartiality and effectiveness, it should be stressed again that, in Greece, there is no specialised legal framework governing the use of AI systems for (predictive) policing purposes. Even in the case of the Presidential Decree 75/2020, these guarantees are not addressed expressly. The latter only stipulates that the person responsible for and those participating in the respective data processing activities are obliged to take appropriate technical measures, so that the transmitted pictures may not be tampered in a non-identifiable way (Art. 9 (2)). Similarly, there is no provision setting out explicitly the legal obligation for AI predictive policing systems to be certified or labelled. Nevertheless, the Technical Specifications for the 'Smart Policing' project refer to, *inter alia*, the *basic principles*, according to which the respective devices shall be designed: security; integrity; scalability; maintenance of the authentication and authorisation points; reliability.[45] The same document provided for a *Monitoring and Delivery Committee*, responsible for, among other things, approving, certifying and accepting the project deliverables. [46] As particularly regards the portable smart policing devices, the certification shall meet the FBI requirements (Image Quality Standards): PIV Certified Single Finger Sensor or Appendix F.[47]

As to the obligation to monitor and adjust AI systems of this kind continuously, the only available information can be found in the document including the technical specifications for the smart policing devices, according to which the *Monitoring and Delivery Committee* will monitor and control the software-equipment and the applications to be designed or upgraded.[48] During the warranty period, which has already kicked off, and after the project is completed successfully, the same committee may check: the hardware-software-use licences, the technical manuals, and the project deliverables; the proper function of hardware-software; the harmonious cooperation between the various parties; the installation-configuration and the successful testing and function of the portable devices. Besides this, it will carry out any other controls that may be necessary to examine whether the supplied goods comply with the technical specifications.[49]

Although the smart policing devices have already been delivered by the contractor, namely Intracom Telecom, no specific rules setting out concrete transparency safeguards could be detected. Notwithstanding, trade secrets related claims may be addressed in the light of Recital 63 GDPR. The latter dictates that the right of access to personal data should not adversely impact the right and freedoms of others, including trade secrets, *but such considerations should not amount to a refusal to provide all information to the data subject*. Besides this, there are no specific rules governing the production of AI systems. Accountability related questions are usually addressed in

[44] *Ibid*, 7. It is mandatory to conduct a DPIA when at least one of the criteria of the first or the second category is met or when at least one of the criteria of the third category is met and the data processing falls into the scope of the first category or/and the data to be processed or the data subjects concerned fall into the scope of the second category (*ibid*). *As to the first category*, data processing purposes include among others: the systematic evaluation, rating, prediction, prognosis and profiling, particularly regarding (among other things) aspects related to the behaviour of data subjects; the systematic data processing that aims at automated decision-making that has a legal effect for the data subject or impacts on him/her significantly and may lead to exclusion or discrimination against natural persons; and the systematic and large-scale data processing for surveiling, monitoring or controlling natural persons by means of data collection empowered by systems of video-surveillance or networks or any other means in public, publicly accessible or private spaces accessible to an unlimited number of persons, including surveillance, whether real-time or not, of movements or geographic location of identified or identifiable natural persons (*ibid*, 7–9). *As to the second category*, the focus lies on large-scale processing of special categories of personal data (including biometric data) as listed in Art. 9 (1) GDPR as well as personal data of particular importance or special character, ranging from electronic communication data to data collected or produced by IoT devices (*ibid*, 9). *As to the third category*, of particular importance is, *inter alia*, the use of new technologies involving new types of data collection and use that are likely to result in a high risk to the rights and freedoms of natural persons – with AI-based applications being one of the examples mentioned expressly in the respective decision of the Hellenic DPA (*ibid*, 10).

[45] Hellenic Police, 'Technical specifications' (n 5) 36.

[46] *Ibid*, 47.

[47] *Ibid*, 83.

[48] *Ibid*, 45.

[49] *Ibid*, 46–47.

the realm of civil law (contracts and torts) and consumer law, as Greek criminal law does not provide for the liability of legal persons.

The Hellenic Police, which will be the principal public authority using such systems for law enforcement purposes in the future, are obliged to organise their actions in accordance with the Act 2800/2000, the Act 4249/2014 and Presidential Decree 141/1991. As particularly regards accountability matters, the Hellenic Police fall in the subjective scope of Art. 105 Presidential Decree 456/1984, according to which public authorities are liable to compensation for unlawful acts or omissions of public officials in the exercise of the public authority vested in them, unless the act or omission in question was committed in breach of a provision existing for purposes of public interest. State liability to compensation arises from issuing an unlawful administrative act or failing to issue such an act *as well as* from unlawful material acts or omissions of State organs, provided that those are associated with the organisation and the operation of public services. In addition, the State is liable, when special duties and obligations that are specific to the particular service and are determined by law in general, common experience and the good faith principle are violated (Council of State 2669/2015, 4133/2011, 1019/2008, 2741/2007, 2796/2006). In such a case, there is no need to establish the fault of the State organ (Council of State 1413/2006). Nevertheless, the existence of a causal link between the unlawful act or omission or the material act or omission of the State organ and the damage suffered is required (Council of State 473/2011, 322/2009, 334/2008, 1024/2005, cf. Supreme Court (*Areios Pagos*) 425/2006).

2.3 General principles of law[50]

To begin with the example of automated facial recognition (AFR) in terms of a technology already deployed as part of the 'Smart Policing' project presented above, the biometric data to be extracted by means of, *inter alia*, a digital photograph will be compared to the data available in other national and international criminal databases – with this comparison expected to lead to the so-called matching followed by the calculation of the similarity score. The limits, against which the similarity score is compared, are determined by individuals and, thus, are based –at least to a certain degree– on subjective criteria. Applying these limits may lead to false positives (when the limit is higher than it should be) or false negatives (when the limit is lower than it should be). This implies that AFR is not only susceptible to errors, but also speculative inasmuch as the calculations do not refer to concrete individuals, but to groups of individuals presenting similar characteristics.[51] Besides this, data processing of this kind may reflect discriminations on the grounds of, among others, racial or national origin.[52] Discrimination related concerns are also raised in relation to historical crime data stored in national and international databases, which do not necessarily depict the full spectrum of criminality, as the reporting rates may vary considerably depending on the crime category.[53] Access to data that corresponds to crimes with a higher reporting rate (e.g., crimes against property) that are usually associated with certain demographics and neighbourhoods, turns the spotlight onto individuals presenting certain characteristics or residing in specific neighbourhoods.[54] These individuals are exposed to the stigma associated with future coercive measures based on predictive policing outcomes. Besides this, predictive policing may lead to over-policing and community deprivation.[55] For instance, in the case of software identifying areas of heightened criminality, increased police patrols may turn these areas into *de facto* "hot spots of crime" and result in their social and economic degradation.[56]

[50] While there is rich international scholarship on predictive policing, this section, being a component of the Greek report on automated policing and criminal justice, takes into account predominantly works of Greek authors.
[51] Kotsoglou (n 41) 50–51.
[52] Tsolias (n 3) 576.
[53] Cf. European Union Agency for Fundamental Rights (FRA) 'Getting the future right. Artificial intelligence and fundamental rights' (2020) <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights> accessed 4 May 2023, 69–73.
[54] *Ibid*, 70; cf. Gloria González Fuster, 'Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. Study requested by the LIBE Committee' (2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf> accessed 4 May 2023, 40–42.
[55] See Athina Sachoulidou 'Going beyond the "common suspects": to be presumed innocent in the era of algorithms, big data and artificial intelligence' (2023) Artificial Intelligence and Law <https://link.springer.com/article/10.1007/s10506-023-09347-w> accessed 4 May 2023; Francesca Palmiotto, 'The black box on trial: The impact of algorithmic opacity on fair trial rights in criminal proceedings' in Martin Ebers and Marta Cantero Gamito (eds) *Algorithmic governance and governance of algorithms* (Springer 2021) 49, 63.
[56] Tsolias (n 3) 579–580.

Next, Greek scholars have addressed predictive policing's implications for privacy primarily in the light of foreign jurisprudence[57] and of the case law of the Court of Justice of the European Union (CJEU), and particularly of post-Digital-Rights-Ireland CJEU judgements.[58] Similarly, as part of examining the general legal framework of personal data protection, which should govern the use of surveillance systems, the Hellenic DPA stated expressly that audio and video recording by means of collecting, maintaining, storing, accessing and transmitting personal data, even in public spaces, amount to data processing that interferes with the right to privacy (Arts. 9 Greek Constitution (GrC); 7 CFR; 8 ECHR) and the right to data protection (Arts. 9A GrC; 8 CFR) and aligned its opinion with the respective case law of the European Court of Human Rights (ECtHR) and of the CJEU.[59] The latter dictates that access to, maintenance and use of personal data, whether sensitive or not, publicly accessible or not, for law enforcement purposes shall be governed by national law that provides for *objective criteria for controlling and monitoring the respective measures*.[60] These criteria encompass, *inter alia*, the existence of suspicion against individuals that plan the commission of, commit or have already committed a serious crime or are implicated in one way or another in the commission of such a crime,[61] provided that the law specifies clearly how the persons concerned are linked to and included in this specific data subject category – with a mere reference to 'other persons involved in a criminal offence' deemed to be insufficient.[62] Furthermore, the Hellenic DPA pays particular attention to the case law of Greek supreme courts (cf. Council of State (Plenary Session) 3665/2005) and the aforementioned international courts as regards derogations and limitations in relation to the protection of fundamental rights and the right to respect for private and family life in particular. Measures imposing such restrictions shall be provided for in national legislation, serving the purposes referred to in Art. 8 (2) ECHR (e.g., public safety), and comply with the principle of proportionality in a democratic society.[63] The possibility of compensating the data subjects in case of unlawful access to and use of their personal data has not been addressed expressly.

Regarding the need to protect the right to liberty and security of persons against AI systems intended to be deployed for predictive policing purposes, Greek scholars first stress that a legal order determines not only which kind of behaviours shall be punished, but also confers the competence to carry out preventive controls upon specific public authorities. Only the decisions reached by the latter are valid; any other opinion expressed by an unauthorised body –let alone the algorithmic output– does not produce legal effects.[64] This implies the legal and practical necessity of human intervention in terms of a meaningful contribution and not a mere confirmation of the algorithmic result.[65] Notwithstanding the above, it remains questionable to what extent human intervention actually serves as a guarantee, when police officers do not possess the knowledge and the skills required to challenge the algorithmic output.[66] It is equally important to avoid arbitrariness as a structural element of the rights enshrined in Art. 5 (and 8) ECHR (as the ECtHR has stressed on several occasions).[67] Proportionality of predictive policing measures or automated law enforcement in general, procedural safeguards against arbitrariness and consistent application of measures ensuring that like cases are treated alike and unlike cases are treated differently, will ultimately determine the outcome of a future appeal before the ECtHR.[68]

The need to safeguard proportionality may have not been addressed with regard to the use of AI systems for predictive policing purposes in the Greek scholarship, but has been part of a neighbouring debate, namely the debate on the use of surveillance systems in public spaces and its impact on fundamental rights, such as the right

[57] E.g., Kotsoglou (n 41) 52.
[58] E.g., Tsolias (n 3) 574.
[59] Hellenic DPA, 'Legal Opinion 3/2020' (n 36) 7.
[60] Cf. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB C-203/15 and Secretary of State for the Home Department* (2016) ECLI:EU:C:2016:970, para 118
[61] Cf. *ibid*, para 119; *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) para 260.
[62] Hellenic DPA, 'Legal Opinion 3/2020' (n 36) 8. Cf. *Iordachi and Others v Moldova* App no 25198/02 (ECtHR, 10 February 2009) para 44; *Roman Zakharov v Russia* (n 61) para 245.
[63] Hellenic DPA, 'Legal Opinion 3/2020' (n 36) 8–10.
[64] Kotsoglou (n 41) 51.
[65] *Ibid*, 52
[66] *Ibid*.
[67] Cf. *S., V. and A. v Denmark* App nos 3553/12, 36678/12 and 36711/12 (ECtHR, 22 October 2018); *McKay v the United Kingdom* App no 543/03, (ECtHR, 3 October 2006).
[68] Kotsoglou (n 41) 52.

to informational self-determination, the inviolability of communication or the freedom of assembly. These rights may not be absolute, but the respective restrictions have to be justified by overriding reasons of public interest, be manifestly and reasonably related to this purpose, be appropriate, suitable and necessary for achieving the objective pursued and must not interfere with the core of the right at stake or grant the administration wide discretionary powers (Council of State (Plenary Session) 3665/2005). Against this backdrop, Art. 5 (1) Presidential Decree 75/2020 states expressly that the installation and the use of surveillance systems in public spaces is allowed inasmuch as this is necessary and when the goal of preventing or repressing criminality and controlling traffic cannot be achieved by using milder means. In doing so, it reflects the principles of necessity and appropriateness, core components of the principle of proportionality.[69]

Furthermore, the need to respect proportionality arises in respect to data retention in the case of individuals suspected of planning to commit or committing a crime in the future (cf. Arts. 3, 8 (2) Presidential Decree 75/2020). As part of this proportionality test, it is necessary to delimit the notion 'suspect' and explain what the term 'committing a crime in the future' stands for. [70] In the case *P.N. v Germany*, the ECtHR has found the criteria of the nature, the gravity and the number of the offences for which the data subject has been convicted or prosecuted in the past as compliant with Art. 8 ECHR. [71] The lack of such criteria may pave the way for classifying everyone within the reach of surveillance systems as a suspect on the basis of unclear, subjective probabilistic judgments – making it impossible to examine the legality of the respective measures, including their compliance with the principle of proportionality.[72] The latter requires that the affected individuals know in advance upon which criteria they may be classified as suspects and their data may be retained.[73] Against this backdrop, Art. 8 (2) Presidential Decree 75/2020 adopts the aforementioned criteria as regards previous convictions and prosecutions and requires that reasonable suspicion as to the future commission of crimes arises from testimonies or information, the movements and the contacts of the individual concerned.

Procedural legality related questions have also been addressed with respect to the use of surveillance systems in public spaces. The installation and the use of such systems require the existence of reasonable suspicion that specific crimes (Art. 3 Presidential Decree 75/2020) are committed or will be committed in a specific place. This suspicion is to be substantiated by means of reference to factual evidence, such as *statistical or empirical data*, studies, reports, testimonies, information about the frequency, the kind and the special characteristics of the criminal offences committed in a specific place as well as the potential expansion or transfer of criminality to another public space (Art. 5 (1) Presidential Decree 75/2020). This should not mean that there is no need to safeguard procedural legality of predictive policing by means of specific rules – particularly, should the Hellenic Police start employing software that targets the so-called likely wrongdoers.[74] Instead, it should be safeguarded that personal data processing of this kind will comply with the principle of proportionality and will be based on strict and objective criteria, in order to avoid the ostensible classification of individuals as future criminals.[75]

Lastly, predictive policing may give rise to feelings of constant surveillance and reduce anonymity in public spaces and, thus, have a chilling effect on further fundamental rights, such as the *freedom of assembly and association* (Arts. 11 GrConst; 12 CFR; 11 ECHR) and the *freedom of expression* (Arts. 5 (1) GrC; 11 (1) CFR; 10 ECHR).[76] Equally problematic may be the use of materials collected by means of predictive policing in judicial settings. This may amount to a violation of the *right to a fair trial* (Arts. 20 (1) GrC, 47 CFR; 6 (1) ECHR), the *presumption of innocence* (Arts. 71 Greek Code of Criminal Procedure (GrCCP); 48 CFR; 6 (2) ECHR), including the burden of proof for establishing the guilt, combined with the defence's *right to present (counter)evidence*,[77] or initiate a debate on the

[69] Cf. Hellenic DPA, 'Legal Opinion 3/2020' (n 36) 23.
[70] Cf. *Tele2 Sverige AB C-203/15 and Secretary of State for the Home Department* (n 60) para 110.
[71] *P.N. v Germany* App no 74440/17 (ECtHR 11 June 2020) paras 77–83.
[72] Hellenic DPA, 'Legal Opinion 3/2020' (n 36) 35.
[73] *Ibid*.
[74] Tsolias (n 3) 579.
[75] *Ibid*.
[76] Cf. Tsolias (n 3) 579; Kotsoglou (n 41) 53; Athina Sachoulidou 'OK Google: is (s)he guilty?' (2022) 30 Journal of Contemporary European Studies 284–296.
[77] Cf. Recital 22 Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings.

admissibility of AI-generated evidence that may lead to insurmountable resources asymmetry between the prosecution and the defence.[78]

3 Predictive justice

3.1 National practices

Greek law does not provide for, nor defines, predictive justice (also known as algorithmic or automated justice) in criminal matters (or in general). Seeking to explore this judicial practice, Greek scholars usually use the definition included in the European Ethical Charter on the use of AI in judicial systems and their environment, which was drafted by the European Commission for the Efficiency of Justice (CEPEJ) under the umbrella of the Council of Europe.[79] In the Greek Digital Transformation Bible 2020-2025 (DTB), justice is listed as one the key areas where digital transformation will be promoted with the aim of improving efficiency and quality of public services.[80] The respective digitalisation projects include, *inter alia*, the extension and the upgrade of information systems in the judicial sector, the development of a system for collecting and processing statistical data of justice, the digitisation of court decisions, the creation of a single, interoperable judicial environment, AI applications for processing court files and drafting court decisions (chatbot) to be uploaded on the e-Justice platform as well as for anonymising and pseudonymising court decisions.[81] This list does not entail any predictive justice project.[82]

That said, there is no obligation, nor possibility, for the judicial authorities to use AI systems at any stage of adjudicating a criminal case. The Hellenic Standing Scientific Committee that was set up by virtue of the Ministerial Decision 8056/2019 with the mandate of examining the implications of the use of AI for the justice system (HCAI) noted that AI *may* be employed to address systemic and organisational problems the domestic judicial authorities face.[83] As particularly regards predictive justice, the possibility of creating a database of court decisions and trial documents that will provide information as to how a particular case was resolved has been examined as a means to improve alternative dispute resolution mechanisms *in civil matters* and to achieve speedy and high-quality administration of justice.[84] A similar comment is to be found in the Committee's report regarding the use of open data in the realm of administrative justice.[85] No such reference could be detected with respect to criminal justice. Notwithstanding the above, Greek scholars have already brainstormed on political and socio-economic incentives for automatising criminal justice – placing emphasis on the goals of eliminating discrimination and strengthening impartiality, enhancing the respect for criminal procedural rights (due process by design), promoting speedy administration of justice and minimising the operational costs thereof.[86] As part of the respective political debates and within the context of HCAI in particular, the focus rather lies on the digitalisation of court records.

---

[78] Tsolias (n 3) 580; Sachoulidou, 'Going beyond the "common suspects"' (n 55).

[79] The definition included in the Charter reads as follows: 'Predictive justice is the analysis of large amounts of judicial decisions by artificial technologies in order to make predictions for the outcome of certain types of specialised disputes […].' Council of Europe, European Commission for the Efficiency of Justice (CEPEJ) 'European Ethical Charter on the use of artificial intelligence in judicial systems and their environment' 2018 <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> accessed 4 May 2023, 74.

[80] MDG (n 38) 286.

[81] *Ibid*, 287–294.

[82] The DTB refers extensively to the use of AI for public governance purposes. The main message it conveys is that the use of AI is not an end in itself and that it is necessary to understand emerging technologies, the benefits and risks associated therewith, in order to assess properly their future integration in areas of public policy. The drafters of the DTB advocate a strategy of gradual use of AI systems in the public sector starting with pilot applications in areas that do not raise privacy, discrimination or bias concerns. For instance, this is the case with systems trained by means of open data, ruled-based AI systems or systems that provide for human supervision as a prerequisite for automated legally-binding decisions. Among the pilot applications included in the DTB, there are some that may impact on the administration of criminal justice (e.g., employing machine learning to investigate cases of fraud and to tackle financial crime).

[83] Hellenic Standing Scientific Committee for Examining the Implications of the Use of Artificial Intelligence for the Justice System (HCAI), 'Online Meeting Report 10 June 2021' [in Greek] (2021) <https://www.ministryofjustice.gr/wp-content/uploads/2021/10/Praktiko-Synedriasis-10-Iouniou-2021.pdf> accessed 4 May 2023, 19 [Comment of the Committee's President].

[84] *Ibid*, 27–28 [Presentation of Lymperopoulos]; 39–40 [Presentation of Toula].

[85] *Ibid*, 35 [Presentation of Papanikolaou].

[86] Konstantinos Kakavoulis, 'Judicial decision-making by means of artificial intelligence: A scenario of a total overthrow of the classical model of criminal trial?' (2021) 8-9 Poiniki Dikaiosini 1172, 1173.

Although predictive justice remains a rather theoretical concept in the Greek legal order, concerns have already been verbalised as regards the possibility of supporting legal reasoning or demystifying the behaviour of trial parties by means of AI systems particularly in criminal justice settings.[87] The challenges Greek scholars have pointed out vary depending on the phenomenology into question: For instance, in the case of an *AI-driven justice administration model that would progressively eliminate human intervention*, major concerns are formulated with respect to the compliance of such as model with the right to a fair trial and the right to access to a human judge, the requirements governing the justification of court decisions, the independence of the judiciary, and the right to appeal in criminal matters.[88] In the case of *algorithmic risk assessment* and recidivism algorithms in particular, the focus lies on compliance of their use with human dignity, the principle of guilt and the principle of equality.[89] Further challenges are identified with respect to the accuracy and the completeness of the data the algorithm is supplied with, the bias potentially inherent in the databases employed to design, train and operate the algorithm, the validation of the algorithmic output and the ways of safeguarding transparency in the realm of criminal justice as well as of enabling the exercise of the right to effectively participate in a criminal trial, to defend oneself and to be presumed innocent.[90]

3.2 Normative framework

As mentioned above, there is no special legal framework governing predictive justice, whether in general or in criminal matters in particular. The stakeholders involved in the debate as to the possibility of employing AI in judicial settings usually refer to the set of rules providing for the protection of fundamental rights (Arts. 4–25 GrC; CFR; ECHR) and data protection in particular (GDPR and LED as transposed by Act 4624/2019) as well as the rules governing the punishment of criminal conduct: Criminal Code (Act 4619/2019) and Code of Criminal Procedure (Act 4620/2019). Besides this, the only available source of *soft law* is the CEPEJ Ethical Charter on the use of AI in judicial systems and their environment, which was translated in Greek and was uploaded on the website of the Hellenic Ministry of Justice. This explains how AI systems may be deployed in judicial settings and adopts five core principles to govern the use of AI in this context: 1) the principle of respect for fundamental rights; 2) the principle of non-discrimination; 3) the principle of quality and security; 4) the principle of transparency, impartiality and fairness; and 5) the principle 'under user control'. The national criminal justice system has not yet formally referred to the CEPEJ Ethical Charter or another international or regional normative instrument of this kind.

In the absence of predictive justice projects, questions related to the authorization of such AI systems prior to their use or the need to certify/label them have not yet been addressed in the Greek legal order. The need to train the professionals that will be employing such systems in the future has been underlined only in the context of the respective scholarly discourse. In particular, it is noted that, if employing AI, judges should be educated accordingly and trained on a regular basis throughout their career following the system updates (the same way they are expected to keep pace with legislative amendments). This is necessary, in order to reach an informed decision when taking into account the algorithmic output – the same way they are expected to filter critically the expert opinions presented to them.[91] Transparency related questions have also been addressed in a scholarly (and not a legislative) context. It has been highlighted that, when employing AI systems in judicial settings, transparency requires either establishing technical standards that enable *ex ante* reverse engineering or setting review models that offer *ex post* validation of the algorithmic output.[92] This requires a close cooperation between the designer, the manufacturer and the end-user of the AI system as well the "translation" of the algorithmic output, including the way the latter has been calculated, in a language the affected individual understands.[93]

---

[87] HCAI (n 83) 38 [Presentation of Toula]

[88] Kakavoulis (n 86) 1175–1176.

[89] Georgios Papadimitrakis, 'Big data and algorithmic risk studies. New challenges in the area of penology' [in Greek] (2019)10 Poiniki Dikaiosini 1045, 1053–1054; Maria Kaiafa Gbandi, 'Algorithmische Justiz in Strafsachen: eine zulässige Wahl für den Rechtsstaat?' in Beatrice Brunhöber, Christoph Burchard, Klaus Günther, Matthias Jahn, Michael Jasch, Jesús-María Silva Sánchez and Tobias Singelnstein (eds) Strafrecht als Risiko. Festschrift für Cornelius Prittwitz zum 70. Geburtstag (Nomos 2023) 693, 699 *et seq*.

[90] Sachoulidou, 'OK Google' (n 76); *id*. 'Going beyond the "common suspects"' (n 55).

[91] Sachoulidou, 'Going beyond the "common suspects"' (n 55).

[92] Serena Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings – A Framework for a European Legal Discussion* (Springer 2020), 93; Sachoulidou, 'Going beyond the "common suspects"' (n 55); Kaiafa Gbandi (n 89) 705.

[93] Sachoulidou, 'Going beyond the "common suspects"' (n 55).

Additionally, in order to safeguard transparency and to respect the fair trial principle, the affected individuals should be informed as to 1) whether, at which stage(s) of the criminal procedure and to what extent an AI system has been deployed; 2) how and where to request explanations; and 3) how to contest the underlying decision.[94]

Neither the Greek legislator nor Greek scholars have dealt with accountability related questions expressly. As regards AI producers, such issues will be addressed most likely in the realm of civil law (contracts and torts) and consumer law,[95] considering that Greek criminal law does not provide for the liability of legal persons. Besides this, in the absence of specific rules to govern the use of AI systems intended to be employed by public authorities for predictive justice purposes, accountability issues of this kind may be examined in the broader context of State liability in case of harmful actions performed by the judiciary. In the Ruling 1501/2014, the Council of State recognised explicitly the State liability for damage caused by actions, whether illegal (cf. Art. 105 Presidential Decree 456/1984) or legal, of State organs *and the judiciary*. This case-law has recently been overturned with the Council of State holding by majority that Art. 105 Presidential Decree 456/1984, despite its broad wording, does not apply to cases of damage, whether material or immaterial, caused by State organs when acting in their judicial capacity. As long as the conditions for the reparation of such damage are not defined by law and there are no rules as to the competent jurisdiction for the settlement of such disputes, the respective damage cannot be repaired by invoking Art. 4 (5) GrC. The State obligation to repair damages suffered by citizens as a result of a breach of Union law caused by a decision of a national court of last instance (cf. Council of State (Plenary Sitting) 799/2021) does not apply analogously. Hence, in the absence of a provision establishing specifically the State liability for damages caused by the judiciary, Art. 105 Presidential Decree 456/1984, which, among other things, is not appropriate for safeguarding the constitutional principles of independence, validity and proper administration of justice, is not applicable (see Council of State 800-803/2021; 1360-61/2021). In the context of the respective rulings, some members of the Council of State argued that Arts. 533–545 GrCCP, which provide for a system of compensation to be granted to those detained and subsequently acquitted, may be applicable.

Irrespective of the lack of rules concerning the use of AI systems in criminal justice settings, Greece will be obliged to comply with the EU AIA (once adopted) when shaping the respective national legislation. The latter already classifies 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' as 'high-risk' (Art. 6 (2); Annex III 8 lit. a)[96].[97]

3.3 General principles of law[98]

The implications of the use of AI in judicial settings for the right to equality and non-discrimination have been placed at the centre of attention in the Greek scholarship. Major concerns are associated with the fact that, in societal contexts, where discriminatory policies are well-spread or inequalities beyond the control of those suffering them simply exist, the data collected to "feed" the algorithm will reflect these policies or practices, unless one de-biases successfully these datasets. AI systems that deploy such data may reproduce and entrench bias, discrimination and inequality, particularly as far as minorities and disadvantaged groups are concerned[99] – giving rise to the so-called algorithmic bias.[100] The transition from human to algorithmic bias is associated with further challenges related to the assessment of criminal liability itself.[101] Criminal liability shall be shaped on the basis of past conduct driven by factors *within the individual's control*. That said, variables, such as gender,

[94] Cf. FRA (n 53) 76; Sachoulidou, 'Going beyond the "common suspects"' (n 55).

[95] Being an EU Member State, Greece will have to transpose the Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) into domestic law, should the respective Proposal be adopted. See European Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' COM/2022/496 final.

[96] In its General Approach to the EU AIA, the Council (n 40) amended point 8 of Annex III as follows: 'AI systems intended to be used by a judicial authority or on their behalf to interpret facts or the law and to apply the law to a concrete set of facts'.

[97] Cf. Vassilis Karkatzounis, 'Artificial Intelligence in justice and the EU Proposal for a Regulation on high-risk [AI] systems' [in Greek] (2021) 2 DITE 234–236.

[98] While there is rich international scholarship on predictive justice, this section, being a component of the Greek report on automated policing and criminal justice, takes into account predominantly works of Greek authors.

[99] Cf. FRA (n 53) 69; *id*, 'Bias in algorithms - Artificial intelligence and discrimination' (2022) <https://fra.europa.eu/en/publication/2022/bias-algorithm> accessed 4 May 2023; CEPEJ (n 79) 55.

[100] Sachoulidou, 'Going beyond the "common suspects"' (n 55);

[101] Papadimitrakis (n 89) 1053–1054; Sachoulidou, 'Going beyond the "common suspects"' (n 55); Kaiafa Gbandi (n 89) 706 *et seq*.

education or family background, which are originally considered inappropriate to bring into the assessment of criminal liability,[102] may "intrude" judicial reasoning, particularly when employing algorithmic risk assessments. Besides this, these variables are interpreted differently in the context of (criminal) justice and that of computer science, where taking, for instance, gender into consideration may not signal a discrimination risk, but rather promote the accuracy of the prediction. The lack of a common "mindset" may allow biases to slip into the design of the algorithm and the interpretation of its output, even before the latter reaches the courtroom.[103]

Safeguarding judicial independence (cf. Arts. 87 (2) GrC; 6 ECHR) is presented as another great challenge the Greek legal order will have to address, should AI systems be deployed to replace human judges. It is argued that an AI system cannot reach any decision independently, as the "cognitive" tasks it performs are based on the data the programmer or the user thereof supplies it with.[104] The threshold for safeguarding judicial independence appears to be equally high in less extreme scenarios, that is, when the judge is "solely" assisted by the AI system. In this case, independence is tightly linked to the ability to reflect critically on the algorithmic output. Besides judicial independence, Greek scholars have also underlined the implications for the right of access to a human judge. According to Art. 8 GrC, no one shall be deprived of the judge assigned to them by law against their will. The term 'judge' refers to a natural person that is a member of a court (cf. Art. 87 (1) GrC) adjudicating a particular case on the basis of predetermined, general and impersonal criteria. Against this backdrop, AI systems cannot be subsumed under the term 'judge' and, thus, cannot replace the judiciary.[105] As regards AI systems intended to assist the judiciary, one should distinguish between the different tasks such a system may take over The interpretation of facts and law as well as the application of the law to concrete cases are complex cognitive procedures the outcome of which may have an important impact on the individuals concerned and their legal interests – making compliance with the right of access to a human judge questionable. A similar conclusion may be reached –at least at first sight– in the case of AI systems employed for research purposes, considering that judges may over-rely on the algorithmic output without cross-checking its validity or completeness. Nevertheless, Greek judges already employ (less sophisticated) tools of research that may not be based on AI, but can lead to inaccurate or incomplete results without such tools being controlled as regards their accuracy or transparency.[106]

Next, considerable concerns arise as regards the burden of proof (Arts. 6 (1) Directive (EU) 2016/343; 178 (2) GrCCP) as a component of the presumption of innocence (Arts. 6 (2) ECHR; 48 CFR, 2 Directive (EU) 2016/343; 71 GrCCP).[107] The presumption of innocence would be infringed, if the burden of proof were shifted from the prosecution to the defence – without precluding, however, 'the use of presumptions of fact [. . .] concerning the criminal liability of a suspect or accused person' (Recital 22 Directive (EU) 2016/343). Such presumptions should be confined within reasonable limits, be rebuttable and in any event be used only where the rights of the defence are respected (*idem*). In the case of AI systems that establish, for instance, a correlation between the defendant's background and the alleged crime in terms of a presumption of fact, it remains questionable how and to what extent the affected individual will be able to rebut such a presumption without having access to equally sophisticated tools.[108] The resources asymmetry *per se* is not synonymous to a reversal of the burden of proof. However, the affected individual has to contest *de facto* the AI system's output, in order to prove his/her innocence.[109]

Besides the right to be presumed innocent, the right to a fair trial (Arts. 6 ECHR, 47–48 CFR; cf. Art. 20 GrC) includes the right 'to be informed promptly, in a language which [one] understands and in detail, of the nature and cause of the accusation against him/her' (Art. 6 (3) lit. a ECHR) and the right 'to examine or have examined

---

[102] Danielle Kehl, Priscilla Guo and Samuel Kessler, 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing', Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School (2017) <https://dash.harvard.edu/handle/1/33746041> accessed 4 May 2023, 23.

[103] Aleš Završnik, 'Algorithmic justice: Algorithms and big data in criminal justice settings' (2021) 18 European Journal of Criminology 623; Sachoulidou, 'Going beyond the "common suspects"' (n 55).

[104] Kakavoulis (n 86) 1176.

[105] *Ibid*, 1175–1176.

[106] Karkatzounis (n 97).

[107] See Kaiafa Gbandi (n 89) 708.

[108] Cf. Sachoulidou, 'Going beyond the "common suspects"' (n 55).

[109] *Ibid*.

witnesses against him/her' (Art. 6 (3) lit. d ECHR). The term 'witness' is interpreted broadly encompassing documentary evidence and computer files.[110] Irrespective of the limitations the protection of these rights may be subject to,[111] informing a defendant that has been classified as high-risk, charged or convicted by means of an AI system presupposes a certain level of disclosure[112] as to, for instance, the kind of data that system assesses or which rules underlies its function.[113] However, achieving transparency is not enough without granting the affected individual adequate time *and facilities* to organise his/her defence (Art. 6 (1) lit. b ECHR) against an AI-supported finding or judgement.[114] Additionally, the link between the burden of proof and the defence right to submit counterevidence as components of the right to fair trial should be taken into consideration. This particularly refers to the rather limited chances of defence to present persuasive evidence –*with a view to influencing the court's decision*–[115] when contesting the algorithmic output that is already surrounded by scientific objectivity and a sense of security.[116]

The implications for the right to appeal have been addressed rather marginally with some Greek scholars arguing that, in the case of using AI systems both on first instance and at appeal level, the parties would be effectively deprived of their 'right to have their conviction or sentence reviewed by a higher tribunal' (Art. 2 (1) 7th Additional Protocol to ECHR).[117] This implies that there would be no distinction between the courts/tribunals that would employ a similar –if not the same– AI system to reach a decision. Besides this, there has not been any significant scholarly debate as to how to challenge an AI calculation before a criminal court or how to ensure the judicial review of an AI-supported decision on the basis of a concrete set of rules. Instead, the focus of Greek scholars rather lies on the obstacles arising as to the general possibility to do so without access to equally sophisticated tools or equally large datasets – highlighting, that way, the impact of the use of AI on the equality of arms in the realm of criminal justice.[118]

Next, Greek scholars turned the spotlight on the implications for criminal punishment as such.[119] The latter is tightly linked to the personal responsibility of the defendant and the decisions (s)he deliberately makes. According to Arts. 1 and 14 GrCC and Art. 7 GrC, one may only be punished for a wrongful act that can be attributed to him/her. The so-called moral liability originates from Arts. 2 and 5 GrC that mandate that an individual has value by virtue of this status and, hence, his/her life choices shall be respected. This implies that an individual may not be punished for reasons beyond his/her control, such as membership in a certain social group. That is, however, a risk associated with the use of recidivism algorithms for predictive justice purposes.[120] Individuals may be objectified, when the algorithmic output focuses on the average member of a certain group instead of the particular person and his/her chances to get involved in criminal conduct. This may even increase racist tendencies, as algorithmic risk assessments reinforce the belief that, regardless of their personal characteristics, members of a specific social group (will) behave in the same way and, thus, are to be treated in the same way.[121] In this context, equally considerable may be the impact on the principle of equality (Art. 4 GrC). Additionally, even when the AI system allows individualised decision-making, the selection of the input data may be problematic. For instance, the consideration of data related to the defendant's lifestyle may result in his/her stricter punishment not because of the severity of his/her acts, but because of his/her less conventional ideas. This equally violates fundamental tenets of Greek criminal law and the principle of personal liability in particular.[122]

---

[110] Cf. *Mirilashvili v Russia* App no 6293/04 (ECtHR, 11 December 2008) paras 158–159; *Papageorgiou v Greece* App no 59506/00 (ECtHR, 9 May 2003) para 37.
[111] E.g., *Al-Khawaja and Tahery v the UK* App nos 26766/05 and 22228/06 (ECtHR, 5 December 2011) paras 118, 152.
[112] Aleš Završnik 'Criminal justice, artificial intelligence systems, and human rights' [2020] 20 *ERA Forum* 567-583, 577.
[113] Sachoulidou, 'Going beyond the "common suspects"' (n 55).
[114] *Ibid*.
[115] Cf. *Brandstetter v. Austria*, ECtHR, 28 August 1991, para 67.
[116] Cf. Kelly Hannah-Moffat 'Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates' (2019) 23 Theoretical Criminology 453–470.
[117] Kakavoulis (n 86) 1176.
[118] Cf. Sachoulidou, 'OK Google' (n 76); *id*, 'Going beyond the "common suspects"' (n 55).
[119] Kaiafa Gbandi (n 89) 706–709.
[120] Papadimitrakis (n 89) 1053.
[121] *Ibid*, 1054.
[122] *Ibid*.

The use of AI in judicial settings for decision-making purposes has also been examined in the light of Art. 93 (3) GrC that, *inter alia*, dictates that '[e]very court judgement must be specifically and thoroughly reasoned'.[123] It is questionable whether and to what extent an AI-supported judgement complies with this principle, considering that the "cognitive" procedure a computer system follows to reach a conclusion cannot (always or fully or at least for the time being) be described in a way that is comprehensible to the trial parties and/or the defence. The judgement of a criminal court that does not meet the reasoning requirements, though, cannot fulfil its purposes; that is, it does not restore the idea of justice, nor establishes social peace for the sake of and among the citizens.[124]

When examining more far-reaching scenarios, such as that of replacing legal reasoning with mathematical calculation, it remains questionable whether and to what extent an algorithm could reach a conclusion that would comply with the normative decisions reached in the realm of (Greek) criminal law – in the sense of matching the material and mental elements of criminal liability and addressing the codified or otherwise recognised grounds upon which the wrongfulness of an act can be excluded or the liability itself can be excluded, aggravated or mitigated.[125] Developing appropriate calculation criteria for this purpose appears to be a great challenge, considering the multitude and the complexity of the variables shaping criminal liability as well as the lack of a universal approach to crime and criminal liability compared to the universal approach to mathematics and computer science. Even if such criteria are designed successfully, there are still parameters that may shape the legal reasoning, but cannot be measured, such as leniency, human values and social perceptions.[126]

Lastly, there has not yet been a major public debate on the possibility of privatising criminal justice (or parts thereof) through the development of LegalTech applications. It has only been underlined that the EU AIA is not clear as to the classification of AI systems deployed by law firms or LegalTech companies as 'high-risk', despite the fact that it is mainly these companies (and not public authorities) that deploy AI.[127] Questions related to the equality of litigants have not yet attracted the attention of Greek scholars either. Special emphasis is placed, however, on the role of the legal counsel in criminal trials. The legal counsel has multiple roles, including the assessment of the facts presented to him/her, discovering and revealing the truth *and* protecting the interests of his/her clients, and participates independently in the administration of justice. Using an AI system to provide legal guidance (and to replace lawyers in the future) would deprive the defendant of the possibility to object through his/her counsel, as that system would most likely operate on the basis of a similar –if not the same– algorithm the system employed by the judicial authorities is equipped with. This would automatically invalidate the institutional status of the legal counsel[128] and establish a regime of inequality in cases where one party may have access to legal counsel, whereas the other may only afford AI-supported counselling services.

Against this backdrop, it is no coincidence that the HCAI has primarily focused on the possibility of employing AI systems in *civil matters* and, particularly, in the context of the small claims procedure or that of online dispute settlement.

4 Evidence law

4.1 Evidence gathered through AI systems

The Forensic Science Department[129] and the Cyber Crime Department[130] of Hellenic Police are entrusted with the task of gathering evidence by means of modern technical equipment that enables, *inter alia*, the extraction of data from mobile devices. Nevertheless, there is no (publicly accessible) information as to whether and to what extent their staff (or the staff of another public authority) employs AI systems for this purpose and which exactly those systems may be. Similarly, Greek law firms appear to increasingly rely on new technologies, but there is no

[123] Cf. Kaiafa Gbandi (n 89) 708–709.
[124] Kakavoulis (n 86) 1176.
[125] Cf. Quattrocolo (n 92) 214–215.
[126] Kakavoulis (n 86) 1176; Kaiafa Gbandi (n 89) 707.
[127] Karkatzounis (n 97).
[128] Kakavoulis (n 86) 1174–1175.
[129] See more information here <https://www.astynomia.gr/hellenic-police/special-services/hellenic-police-forensic-science-division/?lang=e> accessed 4 May 2023.
[130] See more information here <https://www.astynomia.gr/hellenic-police/special-services/cyber-crime-division/?lang=en> accessed 4 May 2023.

information as to whether and to what extent they may use AI systems for the purposes of gathering evidence on behalf of their clients.

As regards the future use of AI systems in law enforcement settings, it is worthy to remind that the Hellenic Police have already acquired smart policing devices that enable, *inter alia*, facial recognition for the purpose of identifying individuals during on-site controls (see Section 2.1.3). Furthermore, the Sectoral Development Programme of the Ministry of Citizen Protection 2021–2025 emphasizes the need to standardise the evidence trail (identification – collection – management throughout the lifecycle of evidence and until its use before courts). There is, however, no information as to the specific technologies that will be developed or are already deployed to attain this goal.

To date, there is no special legal framework to govern the use of AI systems for the purpose of gathering evidence. Instead, Art. 265 GrCCP (cf. Art. 19 Council of Europe (CoE) Convention on Cybercrime)[131] only provides for the rules to govern the seizure of digital data.[132] Similarly, Greek law does not set out any specific procedural safeguards for the cases where the Greek authorities may resort to AI to gather evidence. Nonetheless, in combination with the provisions of the Greek Constitution and core international human rights instruments (e.g., CFR, ECHR), the GrCCP provides for a set of criminal procedural rights, which include, *inter alia*, the defendant's right to receive copies of the case file and to ask for adequate time for preparing his/her defence and which should be employed in a future scenario of gathering evidence through AI systems. These copies could include information regarding the particular system used to gather evidence. As regards the possibility of challenging the way in which such evidence was collected, the defendant would have the right to ask the public prosecutor to call witnesses, to introduce documentary evidence, and to comment on the evidence submitted in the course of the trial.

4.2 Evidence produced by AI systems

As already mentioned, the Hellenic Police has acquired smart policing devices that enable, *inter alia*, facial recognition for the purpose of identifying individuals during on-site controls (Section 2.1.3). It remains unclear, however, what the procedural use of this output may be beyond the identification purposes. As regards the framework, within which AI-generated evidence may be used in the future, both pre-trial and trial proceedings are governed by the principle of free assessment of evidence, while the use of illegally obtained evidence is explicitly prohibited (Art. 177 GrCCP). Any means of evidence may be allowed (Art. 179 GrCCP) – with circumstantial evidence, autopsy, expert opinions, the confession of the accused person, witnesses and documents being classified as the main means of evidence under Greek law (Art. 178 GrCCP). Against this backdrop, the use of AI-generated evidence cannot be excluded *in abstracto*. Irrespective of this, there is no special legal framework governing the use of such evidence (or express plans to introduce such rules in the future), nor a wide scholarly debate on this topic. The current debate is rather focused on the use of electronic evidence in criminal matters.[133]

Similarly, Greek law does not provide for any special procedural safeguards for those (for the moment, hypothetical) cases where AI-generated evidence may be used. Pursuant to the laws in place, the defendant would be entitled to the exercise of procedural fundamental rights as enshrined in the GrCCP and the applicable international and EU law (e.g., CFR, ECHR). As mentioned above, the defendant has, *inter alia*, the right to ask

[131] For a comprehensive overview of the Greek laws that transposed the CoE Convention on Cybercrime see Theocharis Dalakouras, 'Substantive and procedural provisions of the Council of Europe Convention on Cybercrime (Act 411/2016)' in Theocharis Dalakouras (ed) *Cybercrime. Substantive and procedural perspectives* [in Greek] (Nomiki Vivliothiki 2023) 1 et seq.

[132] See Ioannis Naziris, 'The seizure of digital data (PART B: The rules of the new Code of Criminal Procedure)' [in Greek] (2021) 3 Poiniki Dikaiosini 355, 360 *et seq*; Marianna Koudeli, 'Issues related to seizure of digital data pursuant to article 265 of the Greek Code of Criminal Procedure' in Theocharis Dalakouras (ed) *Cybercrime. Substantive and procedural perspectives* [in Greek] (Nomiki Vivliothiki 2023) 523 *et seq.*

[133] Cf., for instance, Ioannis Naziris, 'The seizure of digital data (PART A: Conceptual and broader regulatory framework)' [in Greek] (2021) 2 Poiniki Dikaiosini 178–194; Athina Sachoulidou, 'The key elements of the LIBE Committee's compromise proposal on e-evidence: a critical overview through a fundamental rights lens' (2021) Global Affairs 777–793; Vasileios Katos, 'Digital evidence' in Theocharis Dalakouras (ed) Cybercrime. Substantive and procedural perspectives [in Greek] (Nomiki Vivliothiki 2023) 399 *et seq.*; Alexandros-Ioannis Kargopoulos, 'Digital data in the current procedural framework: judicial pivots and concerns' in Theocharis Dalakouras (ed) Cybercrime. Substantive and procedural perspectives [in Greek] (Nomiki Vivliothiki 2023) 419 *et seq.*

the public prosecutor to call witnesses, to introduce documentary evidence, and to comment on the evidence submitted in the course of the trial.

The question of whether AI-generated evidence falls into a specific category of evidence has not yet been addressed in the Greek scholarship. The current discourse rather focuses on the notion of electronic data (compared to that of corporeal objects) and its use in criminal proceedings.[134] However, the Greek legislator has not yet classified expressly electronic evidence as a distinct type of evidence,[135] nor has (s)he scrutinised the admissibility of information provided by AI systems used by non-investigative authorities. Notwithstanding the above, in the latter case, one may resort to the existing scholarship as regards the use of DNA samples collected privately. Besides this, in the absence of a special legal framework, the constraints arising from the protection of human dignity and the principle 'nemo tenetur se ipsum accusare' should be taken into account. Within the context shaped by these principles, AI-generated evidence should remain subject to the court's free assessment.

Additionally, Greece has ratified the CoE Convention on Cybercrime (Law 4411/2016), which provides for the search and seizure (Art. 19), real-time collection of digital data (Art. 20) and the respective mutual assistance procedures (Art. 25 et seq.).[136] According to Art. 27 (3) of the Convention, 'mutual assistance requests […] shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party'. This provision, which primarily aims at ensuring the admissibility of evidence in the requesting country, relates to the obligation to respect technical procedural requirements and not fundamental procedural protections (Explanatory Report – Budapest Convention, para 267). Additionally, Greece has recently signed (but not yet ratified) the Second Additional Protocol to the CoE Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, which, *inter alia*, paves the way to the direct cooperation with private service providers for the purpose of cross-border access to electronic evidence in criminal matters.

As regards the EU initiatives in this area of regulation, of particular importance are the Directive (EU) 2014/41 on the European Investigation Order (EIO) and the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters.[137] Despite the fact that Art. 82 (2) TFEU refers expressly to the possibility of establishing minimum rules as regards, among other things, mutual admissibility of evidence between Member States, the rules governing the collection, use, and admissibility of evidence (regardless of its kind) are still left to the laws of national criminal procedure only.[138] Neither the EIO Directive nor the aforementioned Proposal (or the Final Compromise Text of the Regulation[139]) include rules on evidence admissibility or evidentiary exclusionary rules (with the exception of the specific context of immunities or privileges).[140] The shift to the 'forum regit actum' principle (cf. Art. 4 2000 EU MLA Convention; 9 (2) EIO Directive) is just a partial solution to divergent national rules.[141] Similarly, the ECHR does not entail any rules on admissibility of evidence in criminal trials, while the respective case law of the ECtHR rather focuses on the criterion of the overall fairness of the proceedings without having developed comprehensive common standards for evidence admissibility.[142] Against this backdrop, the aforementioned regional and international agreements do not have a direct impact on the admissibility of (AI-generated) evidence in Greece.

---

[134] E.g., Naziris, 'The seizure of digital data (PART A)' (n 133) 180–183.
[135] Cf. Naziris, 'The seizure of digital data (PART B)' (n 132) 373.
[136] See Dalakouras (n 131) 1 *et seq*.
[137] European Commission, 'Proposal for a Regulation of the European Parliament and the Council on European Production and Preservation Orders for electronic evidence in criminal matters' COM (2018) 225 final. In early 2023, the Council confirmed agreement with the European Parliament on new rules to improve cross-border access to electronic evidence (see more information at <https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidencecouncil-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-borderaccess-to-e-evidence/> accessed 4 May 2023). For a brief overview of the negotiations on the adoption of the Regulation see Athina Sachoulidou, 'Cross-border access to electronic evidence: is there any light at the end of the tunnel?' (2023) <https://trace-illicit-money-flows.eu/cross-border-access-to-electronic-evidence-is-there-any-light-at-the-end-of-the-tunnel/> accessed 4 May 2023.
[138] Katalin Ligeti, Balázs Garamvölgyi, Anna Ondrejová and Margarete von Galen, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 *eucrim* 201, 202.
[139] Available at <https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf> accessed 4 May 2023.
[140] Ligeti *et al* (n 138) 205.
[141] *Ibid*, 204-205.
[142] *Ibid*, 205-206.

Lastly, while there is no significant scholarly debate regarding the use of AI systems for generating evidence and the admissibility of such evidence before national courts, there are scholars who advocate technological neutrality. In the case of electronic data, it is underlined that the legislative choices should not be tailored to a particular technology (such as the AI) and the specificities thereof. Otherwise, constant technological developments may render the law obsolete – with the legislator lagging behind technology or –in the worst-case scenario– with the courts applying rules that no longer correspond to the technological context. Hence, a certain level of generalisation is required so that the law can go beyond the technology in question.[143]

4.3 Evidence assessed through AI systems

To date, according to the information publicly available, Greek judicial authorities do not employ any AI systems to assess evidence. Irrespective of this, Greek judges are not obliged to abide by concrete rules on evidence assessment. Instead, they shall reach a decision following their conscience voice and be guided by the impartial judgement concerning the factual truth, the credibility of the witnesses and the value of other evidence. Court rulings shall be reasoned as to, *inter alia*, the use of specific incriminating or exonerating evidence (Art. 177 (1) GrCCP). The GrCCP does not entail any rules concerning the probative value of different means of evidence – with evidence that has been lawfully acquired being subject to the court's free assessment irrespective of the kind and/or the origin thereof. This implies that, in theory, Greek judges could deploy an AI system to assess evidence in criminal matters, provided that they fully justify their conduct. It is questionable, however, to what extent such practice would comply with the presumption of innocence. The latter is a fundamental tenet of Greek criminal law (Arts. 6 (2) ECHR, 48 CFR, 71 GrCCP) that encompasses various meta-rules: The burden of proof lies with the prosecution and the defendant is not under an obligation to disclose evidence as to the claims formulated in favour of his/her interests (Arts. 6 (1) Directive (EU) 2016/343, 178 (2) GrCCP). Moreover, the accused or suspected person benefits from any doubts regarding his/ her guilt (Arts. 6 (2) Directive (EU) 2016/343, 178 (3) GrCC). Should an AI system be deployed to assess the criminal liability of an individual, it is questionable whether the individual concerned will be able to contest this assessment effectively, unless (s)he has access to information as to the calculation methods and the training data this AI system employs and/or access to equally sophisticated tools to prove otherwise.[144] As mentioned above, the resources asymmetry *per se* is not synonymous to a reversal of the burden of proof. Nevertheless, the affected individual has to address *de facto* the AI system, the findings of which may already be surrounded by an increased level of objectivity.[145]Additionally, in a context, where the principle 'in dubio pro reo' dictates that the costs of false positives are higher than those of false negatives, there is no guarantee that the judge will use this margin of appreciation, nor certainty as to the notion of doubt (and the threshold thereof) in AI times.[146]

As regards future steps, once the EU AIA is adopted, Greece will be obliged to comply with the choices of the EU legislators when shaping the respective national legislation.

5 Conclusions

While the development of AI and the expansion of its potential within everyday applications is being carried out at an increasingly rapid pace, its integration within the criminal justice process is far from comprehensive or substantial. Under Greek criminal law and procedure, AI applications have not yet been harnessed in a consistent manner. However, the potential of AI to produce meaningful change in terms of law enforcement and the administration of criminal justice is particularly prominent in the context of predictive policing and justice, as well as evidence law. Its relevance remains limited within the Greek legal order, where AI is seldom addressed directly in the legislative framework and where insufficient empirical data exists on the use of AI for predictive policing or predictive criminal justice purposes, terms that have not even been defined under domestic law. Similarly, the Greek judiciary has not yet engaged with AI in the context of criminal trials. Instead, AI is mainly being dealt with in the context of the development of the country's digital agenda and within broader policy and

[143] Naziris, 'The seizure of digital data (PART B)' (n 132) 187.
[144] Cf. Sachoulidou, 'OK Google' (n 76); *id*, 'Going beyond the "common suspects"' (n 55).
[145] *Ibid*.
[146] Cf. Kaiafa Gbandi (n 89) 708.

legal considerations, such as in data protection. The work of the HCAI and of the Hellenic DPA are important in this regard.

Even though the up until now practical relevance of AI for Greek criminal justice has been limited, Greek scholars have raised concerns in terms of its potential application and the effects not only on the criminal justice system, but also on fundamental rights more broadly. Cautionary tales about the potential for algorithmic bias can prove especially harmful in the broader context of the devastating effects that the wrong or biased decision is made with regard to an individual who is faced with the powerful toolkit of criminal repression.

It is also notable that the impact of AI does not relate only to the judicial determination of guilt or acquittal. It stretches further into the beginnings of the criminal justice system, as it can be deployed in policing and determining potential suspects and hotspots of criminality, as well as in the pre-trial stage during the gathering of evidence and the decisions related to detention and bail. In addition, its reach ranges over to the end product of the criminal trial: the determination of the sentence, as well as the decisions made during serving that sentence, notably those related to parole. Lastly, the criminal trial itself and the decision on guilt can be heavily influenced by AI and its potential to assist -or replace- the human agent in producing and assessing evidence related to the commission of a crime.

These far-reaching possibilities make this discussion particularly crucial, despite its limited practical application. By expanding the scope of the debate to analyse what risks lie in the intersections of AI and criminal justice, criminal law scholars, practitioners, and policy makers alike can be better prepared to employ the necessary safeguards as and when needed. Only by keeping our attention firmly focused in this rapidly changing landscape of AI, will we be able to come up with solutions that strike the right balance between reaping the benefits of AI and taking into account the unique position and purpose of criminal law within the broader legal system. For now, it is crucial to shed light on the principles that will guide the way, including respect for fundamental rights, non-discrimination, transparency, security, privacy, and involving users in the control of their own data.

References

Al-Khawaja and Tahery v the UK App nos 26766/05 and 22228/06 (ECtHR, 5 December 2011)

Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs, 'Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)) Rapporteurs: Brando Benifei & Ioan-Dragoş Tudorache' <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence> accessed 23 May 2023

Council, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Fourth Presidency compromise text' (2022) <https://data.consilium.europa.eu/doc/document/ST-13102-2022-INIT/en/pdf> accessed 4 May 2023

—— 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach' (2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> accessed 4 May 2023

Chelioudakis E, 'Greece: Technology-led policing awakens' (2020) <https://aboutintel.eu/greece-policing-border-surveillance/> accessed 4 May 2023

—— 'Greece/Research' in Chiusi F, Fischer S, Kayser-Bril N and Spielkamp M (eds), *Report Automating Society* (AlgorithmWatch GmbH & Beterlsmann Stiftung 2020) <https://automatingsociety.algorithmwatch.org/> accessed 4 May 2023

Council of Europe, European Commission for the Efficiency of Justice (CEPEJ), 'European Ethical Charter on the use of artificial intelligence in judicial systems and their environment' (2018)

<https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> accessed 4 May 2023

Dalakouras T, 'Substantive and procedural provisions of the Council of Europe Convention on Cybercrime (Act 411/2016)' in Dalakouras T (ed) *Cybercrime. Substantive and procedural perspectives* [in Greek] (Nomiki Vivliothiki 2023)

Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings

Directive (EU) 2016/680 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, and repealing Council Framework Decision 2008/977/JHA

European Commission, 'Proposal for a Regulation of the European Parliament and the Council on European Production and Preservation Orders for electronic evidence in criminal matters' COM (2018) 225 final

—— 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM (2021) 206 final

—— 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' COM/2022/496 final

—— and OECD, 'AI Watch. National Strategies on Artificial Intelligence. A European perspective. 2021 Edition – a JRC-OECD report' (2021) <https://publications.jrc.ec.europa.eu/repository/handle/JRC122684> accessed 4 May 2023

European Union Agency for Fundamental Rights (FRA), 'Getting the future right. Artificial intelligence and fundamental rights' (2020) <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights> accessed 4 May 2023

—— –
– 'Bias in algorithms - Artificial intelligence and discrimination' (2022) <https://fra.europa.eu/en/publication/2022/bias-algorithm> accessed 4 May 2023

Fuster GG, 'Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights' (2020) <https://www.europarl.europa.eu/thinktank/en/document/IPOLSTU(2020)656295> accessed 4 May 2023

Hannah-Moffat K, 'Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates' (2019) 23 Theoretical Criminology 453

Hellenic Data Protection Authority (DPA), 'Decision 65/2018' [in Greek] (2018) <https://www.dpa.gr/el/enimerwtiko/prakseisArxis/katalogos-me-ta-eidi-ton-praxeon-epexergasias-poy-ypokeintai-stin> accessed 4 May 2023

—— 'Opinion 3/2020' [in Greek] (2020) <https://www.dpa.gr/sites/default/files/2020-07/gnomodotisi%203_2020.pdf> accessed 4 May 2023

Hellenic Ministry of Digital Governance (MDG), 'Digital Transformation Bible 2020-2025' [in Greek] (2021) <https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digitalstrategy.pdf> accessed 4 May 2023

Hellenic Standing Scientific Committee for Examining the Implications of the Use of Artificial Intelligence for the
Justice System (HCAI), 'Online Meeting Report 10 June 2021' [in Greek] (2021) <https://www.ministryofjustice.gr/wp-content/uploads/2021/10/Praktiko-Synedriasis-10-Iouniou-2021.pdf> accessed 4 May 2023

Hellenic Police, 'Technical specifications in the context of the implementation of the action "Smart Policing" of the Internal Security Fund (ISF) Programme 2014-2020' [in Greek] (2018) <http://www.astynomia.gr/images/stories/2018/prokirikseis18/26052018texnikesprodiagrafes.pdf> accessed 4 May 2023

—— – – 'Contract for the Purchase of Smart Policing Systems' [in Greek] (2019) <http://www.astynomia.gr/images/stories/2019/prokirikseis19/14122019anakoinosismartpolicing.pdf> accessed 4 May 2023

—— —— 'Response to "Letter by Ms. LAMA Fakih regarding the Hellenic Police's new "smart policing" program"' (2022) <https://www.hrw.org/sites/default/files/media_2022/01/Letter%20from%20Hellenic%20Police_EN.pdf> accessed 4 May 2023

Homo Digitalis, 'Request for the Greek DPA's opinion on the Greek Police Agreement on Smart Policing' (2020) <https://www.homodigitalis.gr/en/posts/5381> accessed 4 May 2023

—— —— 'The Greek DPA investigates the Greek Police' (2020) <https://www.homodigitalis.gr/en/posts/7684> accessed 4 May 2023

Human Rights Watch, 'Greece: New Biometrics Policing Program Undermines Rights. Risk of Illegal Racial Profiling and Other Abuses' (2022) <https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights> accessed 4 May 2023

Intracom Telecom, 'Intracom Telecom Undertakes a "Smart Policing" Project' (2019) <http://www.intracom-telecom.com/en/news/press/press2019/2019_07_02.htm> accessed 4 May 2023

—— —— 'Distinction for the "Smart Policing" Project in Greece that was developed by Intracom Telecom' (2022) <https://www.intracom-telecom.com/en/news/press/press2022/2022_07_15.htm> accessed 4 May 2023

Iordachi and Others v Moldova App no 25198/02 (ECtHR, 10 February 2009)

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB C-203/15 and Secretary of State for the Home Department* (2016) ECLI:EU:C:2016:970

Kaiafa Gbandi M, 'Algorithmische Justiz in Strafsachen: eine zulässige Wahl für den Rechtsstaat?' in Braunhöber B, Burchard C, Günther K, Jahn M, Jasch M, Silva Sánchez JM and Singelnstein T (eds) *Strafrecht als Risiko. Festschrift für Cornelius Prittwitz zum 70. Geburtstag* (Nomos 2023)

Kakavoulis K, 'Judicial decision-making by means of artificial intelligence: A scenario of a total overthrow of the classical model of criminal trial?' [in Greek] (2021) 8–9 Poiniki Dikaiosini 1172

Kargopoulos AI, 'Digital data in the current procedural framework: judicial pivots and concerns' in Dalakouras T (ed) *Cybercrime. Substantive and procedural perspectives* [in Greek] (Nomiki Vivliothiki 2023)

Karkatzounis V, 'Artificial Intelligence in justice and the EU Proposal for a Regulation on high-risk [AI] systems' (2021) 2 DITE 234

Katos V, 'Digital evidence' in Dalakouras T (ed) *Cybercrime. Substantive and procedural perspectives* [in Greek] (Nomiki Vivliothiki 2023)

Kehl D, Guo P and Kessler S, 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing' (2017) Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School <https://dash.harvard.edu/handle/1/33746041> accessed 4 May 2023

Kotsoglou K, 'Smart Policing? Prevention – Repression – Human Rights' [in Greek] (2021) 143 Synigoros 48

Koudeli M, 'Issues related to seizure of digital data pursuant to article 265 of the Greek Code of Criminal Procedure' in Dalakouras T (ed) *Cybercrime. Substantive and procedural perspectives* [in Greek] (Nomiki Vivliothiki 2023)

Ligeti K, Garamvölgyi B, Ondrejová A and von Galen M, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 eucrim 201

McKay v the United Kingdom App no 543/03, (ECtHR, 3 October 2006)

Mirilashvili v Russia App no 6293/04 (ECtHR, 11 December 2008)

Naziris I, 'The seizure of digital data (PART A: Conceptual and broader regulatory framework)' [in Greek] (2021) 2 Poiniki Dikaiosini 178

—— 'The seizure of digital data (PART B: The rules of the new Code of Criminal Procedure)' [in Greek] (2021) 3 Poiniki Dikaiosini 355

P.N. v Germany App no 74440/17 (ECtHR 11 June 2020)

Palmiotto F, 'The black box on trial: The impact of algorithmic opacity on fair trial rights in criminal proceedings' in Ebers M and Cantero Gamito M (eds) *Algorithmic governance and governance of algorithms* (Springer 2021)

Papageorgiou v Greece App no 59506/00 (ECtHR, 9 May 2003)

Papadimitrakis G, 'Big data and algorithmic risk studies. New challenges in the area of penology' [in Greek] (2019) 10 Poiniki Dikaiosini 1045

Petridi C, 'Flush with EU funds, Greek police to introduce live face recognition before the summer' (2021) <https://algorithmwatch.org/en/greek-police-live-facial-recognition/> accessed 4 May 2023

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)

Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015)

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

S., V. and A. v Denmark App nos 3553/12, 36678/12 and 36711/12 (ECtHR, 22 October 2018)

Sachoulidou A, 'The key elements of the LIBE Committee's compromise proposal on e-evidence: a critical overview through a fundamental rights lens' (2021) Global Affairs 777

—— 'OK Google: is (s)he guilty?' (2022) 30 Journal of Contemporary European Studies 284

—— 'Going beyond the "common suspects": to be presumed innocent in the era of algorithms, big data and artificial intelligence' (2023) Artificial Intelligence and Law <https://link.springer.com/article/10.1007/s10506-023-09347-w> accessed 4 May 2023

—— 'Cross-border access to electronic evidence: is there any light at the end of the tunnel?' (2023) <https://trace-illicit-money-flows.eu/cross-border-access-to-electronic-evidence-is-there-any-light-at-the-end-of-the-tunnel/> accessed 4 May 2023

Sectoral Development Programme (SDP) of the Ministry of Citizen Protection 2021–2025, Government Gazette 3630/6.8.2021

Spyropoulos P, 'Crime View, a useful GPS for combating crime' [in Greek] (2017) <https://www.thetoc.gr/koinwnia/article/crime-view-ena-xrisimo-gps-gia-tin-pataksi-tis-egklimatikotitas/> accessed 4 May 2023

Symeonidou-Kastanidou E, 'Remarks on the Hellenic DPA's Opinion 3/2020' [in Greek] (2020) 8–9 Poiniki Dikaiosini 957

Tsolias G, 'Personal data processing by law enforcement agencies: between privacy and safety' [in Greek] (2020) 4 DITE 573

Završnik A, 'Criminal justice, artificial intelligence systems, and human rights' (2020) 20 ERA Forum 567

—— 'Algorithmic justice: Algorithms and big data in criminal justice settings' (2021) 18 European Journal of Criminology 623