TURKISH REPORT ON AI AND ADMINISTRATION OF JUSTICE

By Irmak Erdoğan, Selin Çetin Kumkumoğlu* and Ahmet Kemal Kumkumoğlu**

I. PREDICTIVE POLICING

1. National practices

There is no legal definition for predictive policing in Turkey. However, in doctrine, there are several discussions with regard to predictive policing. Alkan/Karamanoğlu define predictive policing as 'the use of analytical techniques by law enforcement agencies to make statistical predictions about potential criminal activity'. Predictive policing generally involves predicting probable events (i.e., predicting when and where crimes may occur) or likely people (e.g. victims or perpetrators of crimes). Thus, rather than relying on an officer's 'hunch' in an area, 'predictive policing uses the power of "big data" to detect patterns[1]. Secondly, Turan focuses on 'proactive policing', which aims at the prevention of crime and underlines the duty of the police to hinder the occurrence of the crime[2]. Finally, Erdoğan defines the term of predictive policing as 'the use of analytical techniques to solve both past and future crimes through statistical predictions based on data mining'[3].

In Turkey, there is no information disclosed to the public that AI-based systems are used or planned to be used in the near future within the framework of predictive policing activities. Therefore, there are no studies in which the reliability, impartiality and effectiveness of the use of these technologies are discussed.

At the national level, the National Artificial Intelligence Strategy ("NAIS") was published in 2021 by the Presidency Digital Transformation Office. NAIS determines the measures to shape Turkey's efforts in the AI field on the common ground between 2021-2025 and proposes a governance mechanism to implement these measures[4]. The goals foreseen are to be reached in 2025, which is the end of the implementation period of NAIS. They include political or socio-economic incentives such as increasing the contribution of AI to GDP up to 5% and the regulatory studies and standardization processes of international organizations in the field of trustworthy and responsible AI and cross-border data sharing[5].

On the other hand, another goal is to generate value from data through AI applications at institutions and at the sectoral level, to carry out AI projects effectively, and to increase the maturity level of Turkey's AI ecosystem within the framework such as carrying out activities addressing ethical and legal aspects of AI applications by creating regulatory sandboxes and test-beds, the development, and testing. The commercialization processes will

[*] Postdoctoral researcher, KU Leuven, Center for IT and IP Law

[*] Attorney at Law, Istanbul Bar Association

[*] Attorney at Law, Turkish Penal Law Association

[1] Nurettin Alkan & Yunus Emre Karamanoğlu, 'Öngörüye Dayalı Kolluk Temelinde Önleyici Kolluk: Rusya Federasyonu'ndan Örnekler' (2020) 9 Güvenlik Bilimleri Journal 387.

[2] Turan Atlı, 'Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi' (2019) 2 Necmettin Erbakan University Law Faculty Journal 4.

[3] Irmak Erdoğan, *Yapay Zekâ ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri* (1st edn, Seçkin Publishing 2022) 44.

[4] The Republic of Turkey Ministry of Industry and Technology / Presidency Digital Transformation Office, 'Ulusal Yapay Zeka Stratejisi'(2021) 7,<https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>, accessed 07.02.2022.

[5] Ibid.

be facilitated for start-ups; in addition, structural support will be provided and workforce transformation of public institutions and private sector organizations will be established in line with the developments in AI.[6]

The Eleventh Development Plan (2019-2023), published by the Presidency of Strategy and Budget, includes several goals regarding AI systems. According to this plan, technology suppliers will be encouraged to develop applications and services that can be offered on the industrial cloud platform such as AI, advanced data analytics, simulation and optimization, product lifecycle, and production management systems. Furthermore, the use of this platform by companies will be encouraged and supported for digital transformation[7]. Additionally, the Ministry of Industry and Technology published the 2023 Industry and Technology Strategy on 18 September 2019[8]. Moreover, several other public initiatives have been launched to foster the AI capacity of Turkey[9]. At the local level, various municipalities are running technology support and training programs, including AI[10].

One of the goals set within the framework of the 2021 Human Rights Action Plan published by the Ministry of Justice is the Protection of Human Rights in the Digital Environment Against Artificial Intelligence Applications. In this context;

- The legislative framework and ethical principles concerning the field of AI will be established in line with international principles, and human rights-compliant measures will be applied.
- AI applications will be used in the judiciary in conformity with the principles and recommendations of the Council of Europe and without prejudice to the protection of legal guarantees[11].

Some of the goals on strategy documents, action plans, and development plans have already been implemented. For example, an Artificial Intelligence Institute has been established within the Scientific and Technological Research Council of Turkey ('TUBITAK'), which started to carry out related studies[12][13].

In addition, there are institutional structures related to AI in the public sector. For example; the "Big Data and Artificial Intelligence Applications Branch" has been established under the General Directorate of Information Processing within the Ministry of Justice[14].

However, it is not possible to monitor concrete outputs and examine if the indicated goals are met. Monitoring and evaluation reports have not been shared with the public until now.

[6] Ibid.

[7] The Presidency of Strategy and Budget of the Turkish Republic, Eleventh Development Plan (2019-2023) 76, <https://www.sbb.gov.tr/wp-content/uploads/2021/12/On_Birinci_Kalkinma_Plani-2019-2023.pdf,> accessed 07.02.2022.

[8] For more information: Republic of Turkey Ministry of Industry and Technology, '2023 Sanayi ve Teknoloji Stratejisi'(2019), p. 40, <https://www.sanayi.gov.tr/2023-sanayi-ve-teknoloji-stratejisi>, accessed 07.02.2022; Republic of Turkey Ministry of Industry and Technology, p. 73; Republic of Turkey Ministry of Industry and Technology / Presidency Digital Transformation Office, p. 41; KOSGEB, 'KOBİ Teknolojik Ürün Yatırım Destek Programı', <https://www.kosgeb.gov.tr/site/tr/genel/destekdetay/6443/kobi-teknoyatirim-kobi-teknolojik-urun-yatirim-destek-programi>, accessed 07.02.2022.

[9] For more information: Republic of Turkey Ministry of Industry and Technology, p. 73; Republic of Turkey Ministry of Industry and Technology / Presidency Digital Transformation Office, p. 41.

[10] For example, Istanbul Metropolitan Municipality ("IMM") opens Technology Workshops to contribute to the training of individuals who will make technological breakthroughs in Istanbul, see https://teknolojiatolyeleri.ibb.istanbul/; also "Artificial Intelligence Education and Research Branch Directorate" has been established within Gaziantep Metropolitan Municipality, see https://www.gaziantep.bel.tr/tr/haberler/buyuksehir-belediyesi-bir-ilke-daha-imza-atti.

"Artificial Intelligence Education and Research Branch Directorate" has been established within Gaziantep Metropolitan Municipality.

[11] For more information: Republic of Turkey Ministry of Justice, 'İnsan Haklari Eylem Plani ve Uygulama Takvimi' (2021) 120, <https://rayp.adalet.gov.tr/resimler/1/dosya/insan-haklari-ep02-03-202115-14.pdf >, accessed 07.02.2022.

[12] For more information: TÜBİTAK, Yapay Zekâ Enstitüsü, <https://yze.bilgem.tubitak.gov.tr/>, accessed 09.02.2022.

[13] On the other hand, concrete supports are provided by TUBITAK itself. TUBITAK has provided 1.7 billion TL (at 2020 prices) finance to approximately 1,715 R&D and innovation projects carried out in the last 10 years. AI projects in this area account for 18% of the total supported AI project budget. See Republic of Turkey Ministry of Industry and Technology/ Presidency Digital Transformation Office, 46.

[14] Republic of Turkey Ministry of Industry and Technology / Presidency Digital Transformation Office, 40.

There was no discussion in the national media regarding the use of AI-based systems for predictive policing. On the other hand, there is an increase in academic studies on the subject and some non-governmental organizations focus on this issue[15].

In that regard, on the website of DIGICRIMJUS, a strategic education partnership is established by the University of Szeged, the University of Konstanz, and Istanbul University with the support of European Union Erasmus+, where there are articles on digital technologies and law, as well as evaluations on predictive policing practices. Some of these evaluations focus on the data used in the development of algorithms for predictive policing. In this context, the authors warned against the processing of data that are not directly related to crime or criminal procedure processes and its possible consequences, especially for socio-economically disadvantaged groups. Thus, the doctrine underlines the use of such data that reflect social inequalities may cause the algorithms to produce "prejudiced" or "biased" results, which may lead to unfair and discriminatory practices[16].

On the other hand, the Artificial Intelligence Working Group within the body of the Istanbul Bar Association Informatics Law Commission makes publications in the monthly bulletins entitled "Law in the Age of Artificial Intelligence", where they tackle the current developments in predictive policing. The opinion letter in the November 2020 bulletin elaborates particularly on the lack of transparency in algorithms used in the context of predictive policing. The use of "black box" algorithms, which hinders the explainability of the results, is a serious challenge in predictive policing practices, as they transform the law enforcement actions that should be justified by a reasonable suspicion[17].

In the Artificial Intelligence Working Group's 2021 report, Dr. Zafer İçer explained the broader definition of "Artificial Intelligence-Based Preventive Legal Mechanisms" as a broad concept that includes the administrative, criminal procedure, and execution law measures that aim to prevent a person from committing or recommitting a crime[18]. These preventive mechanisms also include AI-based predictive applications that assist the judicial authorities in taking various judicial actions and decisions. On the other hand, AI applications may produce erroneous results and are prone to attacks against the system, such as data manipulation, which in turn may cause weaknesses in the fight against crime[19]. The Istanbul Bar Association focuses further on predictive policing activities and the Human Rights Center of the Association recently organized a conference on "The Implications of New Technologies in Law Enforcement Crime Prevention Activities for the Fundamental Rights and Freedoms" which tackled the risks regarding fundamental rights[20].

[15] For example, some of the published academic articles are as follows: Bacaksız, Pınar & Sümer, Seda Yağmur, *Robots, Artificial Intelligence and Criminal Law* (Adalet Publishing House 2021); Gökhan Erdoğan, Yapay Zekâ Ve Hukukuna Genel Bir Bakış, (2021) 134 Adalet Journal <https://dergipark.org.tr/tr/download/article-file/1778256>; Irmak Erdoğan, *Yapay Zekâ ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri* (1st edn, Seçkin Publishing 2022); Murat Balcı & Hüseyin Aydın, 'European Parliament Resolution on Criminal Liability of Artificial Intelligence', Artificial Intelligence in Criminal Law and Its Use by Law Enforcement and Judiciary Authorities in Criminal Cases, Translated by Murat Balcı & Sinem Turan (Adalet Publishing House 2021); Yunus Emre Karamanoğlu, 'Öngörüye Dayalı Kolluk: Jandarma 4.0' (2020), Jandarma Journal 12 <https://www.jandarma.gov.tr/kurumlar/jandarma.gov.tr/Jandarma/Jandarma_Dergisi/Jandarma_Dergisi_156_k.pdf> accessed 07.02.2022; Nurettin Alkan and Yunus Emre Karamanoğlu, 'Öngörüye Dayali Kolluk Temelinde Önleyici Kolluk: Rusya Federasyonu'ndan Örnekler' (2020) 9 Güvenlik Bilimleri Journal 2.

[16] Eren Sözüer, 'Öngörücü Kolluk Uygulamaları (Predictive Policing) ve İnsan Hakları' (2020), DIGICRIMJUS, <https://www.digicrimjus.com/2021/04/20/ongorucu-kolluk-uygulamalari-predictive-policing-ve-insan-haklari/>, access 07.02.2022.

[17] For more information: Eren Sözüer, 'Öngörücü Kolluk Uygulamaları (Predictive Policing) ve İnsan Hakları'(2020), Artificial Intelligence Working Group, November 2020, p.4, <https://www.istanbulbarosu.org.tr/komisyonlar.aspx?ID=1&DESC=BILISIM-HUKUKU-KOMISYONU-YAPAY-ZEKA-CALISMA-GRUBU>, accessed 07.02.2022; Zafer İçer, Yapay Zekâ Temelli Önleyici Hukuk Mekanizmaları - Öngörücü Polislik, Artificial Intelligence Working Group, annual report of 2021, p.30, <https://www.istanbulbarosu.org.tr/files/komisyonlar/yzcg/2021yzcgyillikrapor.pdf >, access 07.02.2022.

[18] İçer (2021), p. 32.

[19] İçer (2021), p. 41.

[20] Istanbul Bar Association, Human Rights Center, 'Conference on the Implications of New Technologies in Law Enforcement Crime Prevention Activities for the Fundamental Rights and Freedoms', 17 December 2021.

According to another view advocated in the doctrine, stigmatizing the neighborhoods as risky by AI systems will cause directing law enforcement to certain areas, which may result in excessive police surveillance of the residents in these areas. Accordingly, the police will detect more crimes and misdemeanors in these areas. As a result, the residents in certain regions may be treated as potential criminals and face practices that routinely interfere with their rights and freedoms[21].

2. Normative framework

The criminal justice system regulates coercive measures via explicit laws. However, the new methods, which are applied in preventive policing and using smart tools, are not yet regulated distinctively. On the other hand, the Turkish Constitution, the Law on Police Duties and Entitlements no. 2559 (Police Code), the Criminal Procedures Code no. 5271 (CPC), the Personal Data Protection Law no. 6698 (PDPC) set limits to the use of measures via law enforcement.

Predictive policing interferes intrusively with the right to personal data protection. In this context, it is frequently reminded in the doctrine that a regulation limiting the processing of personal data for preventing, detecting, investigating, and prosecuting law enforcement, as within the Directive (EU) 2016/680 must be stipulated in Turkey[22]. In this context, the National AI Strategy emphasizes that artificial intelligence systems should be developed in a way that fulfils the PDPC rules. Particularly while using such systems, data processors must inform transparently and meaningfully from whom and how personal data is obtained and how the decisions based on such data will affect the relevant person.[23]

In Turkish law, there are no specific regulations concerning the use of AI-based systems for predictive policing. However, Article 90 of the Constitution provides that if international conventions in the field of fundamental rights and freedoms are in contradiction with domestic law provisions on the same matter, the provisions of international agreements shall prevail. As this norm prioritises the international conventions, Turkey will be bound by how the European Court of Human Rights interprets the European Convention on Human Rights about policing. Furthermore, The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) is also binding regarding the processing of personal data while using the tools for predictive policing.

Substantive guarantees

a) Norms Regarding Impartiality of AI technologies

If the use of artificial intelligence technologies during predictive policing is based on discriminatory data or the software is designed in a way that causes discrimination, or if the use of these technologies leads to inequality among different groups, one must refer to the equality clause of the Turkish Constitution. Accordingly, such technologies infringe Article 10 of the Constitution which ensures equality before the law without any discrimination due to language, race, political opinions, philosophical beliefs, religion, sect, and similar reasons.

There are also special laws in different regulations regarding equality and impartiality. Turkish Penal Code (TPC) Article 3 is also directly relevant to predictive policing, as it stipulates that penal laws will be applied equally to everyone and states that punishment and security measures must be proportional to the criminal act they committed. Therefore, within the framework of predictive policing, this article should be considered when new

[21] Irmak Erdoğan, p. 47, Gökhan, p.144.

[22] See Volkan Dülger & Onur Özkan, 'Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunması: "Unutulan" Direktifin Kapsamlı ve Karşılaştırmalı Analizi', (2020) 15 Ceza Hukuku Derneği 85, Baran Kızılırmak, 'Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi' (2019) 7 Kadir Has University Law Journal 225.

[23] Republic of Turkey Ministry of Industry and Technology / Presidency Digital Transformation Office, 'Ulusal Yapay Zekâ Stratejisi' (2021) 60, <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>, access 07.02.2022

technologies are enforced during judicial law enforcement activities or when individuals are subjected to measures, which has an equivalent impact as criminal sanctions, or security measures. Therefore, while determining sanctions or similar intrusive measures, the decisions cannot be based solely on the characteristic traits of the possible perpetrators, or on directly or indirectly discriminatory factors such as the place of residence or political views. Pursuant to article 3, once a criminal act is detected, data indicating the relationship between this act and the perpetrator should be collected, and criminal law shall be enforced proportionately to the act committed.

b) Norms Regarding Reliability and Effectiveness of AI technologies

There is no clear regulation on the effectiveness of AI technologies used in predictive policing. However, the effectiveness of these technologies in achieving the desired purpose is related to the principle of proportionality. This principle is stated in Article 13 of the Constitution, stating that the restrictions on fundamental rights and freedoms 'cannot be contrary to the wording and spirit of the Constitution, the democratic social order, the secular Republic, and the principle of proportionality'. While evaluating the proportionality of a measure or restriction taken by public authorities, it is crucial that the authorities have a legitimate purpose and that the measure taken is convenient and necessary to achieve it. Moreover, even if these tools are necessary, they should not interfere with the rights of individuals disproportionately. Therefore, while auditing compliance with the principle of proportionality, the suitability, necessity, and proportionality of the applied measure will be examined[24]. For this reason, it is imperative to evaluate whether the technologies used are suitable for achieving the legitimate aim, in this case, the prevention of crime. In order to protect individuals from arbitrary public power, the use of tools that are not suitable for preventing or detecting crime should not be allowed. In cases where there is more than one convenient means of achieving a legitimate aim, the less restrictive means of rights and freedoms should be selected. Therefore, in accordance with the principle of proportionality regulated in Article 13, predictive law enforcement activities must be effective and thus appropriate and necessary.

Within the European Union, Article 27 of the Law Enforcement Directive 2016/687 requires risk analysis of the effects of modern technologies on the rights and freedoms of individuals, before law enforcement process personal data with such tools. However, in Turkey, the scope of PDPC is not applicable to many preventive activities of law enforcement. Moreover, unlike Article 28 of the Law Enforcement Directive, the PDPC does not require consulting the Personal Data Protection Authority before using such predictive technologies in law enforcement.

In terms of data security, PDPC art. 12 stipulates the responsibility of data controllers to prevent the unlawful processing of data and illegal access to the processed data. The same provision regulates the obligation to take all kinds of technical and administrative measures to establish the security of retained data. Even if there are obligations for ensuring data security while processing personal data, there is no regulation that foresees risk assessment for these technologies, which endangers fundamental rights and freedoms.

It is not publicly known which authorities use AI-based systems for predictive policing, or whether they are using them. There is no binding or non-binding legal regulation on this matter. On the other hand, when it comes to the use of AI-based systems, public authorities often deal with the issue in line with their own internal procedures and can act to constantly monitor and adapt them.

On the other hand, in accordance with the principles in article 4 of the PDPC, each data controller, including public authorities, who process personal data; must comply with the principles of lawfulness and fairness, accuracy, purpose limitation, data minimization and storage limitation.

[24] Metin Yüksel, 'Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük İlkesi Evrensel Bir Anayasal İlke Midir?', (2017) 7 Süleyman Demirel University Law Faculty Journal 1.

In this respect, the authorities using AI-based systems should make the necessary updates and adaptations in the processes of processing personal data, especially by acting in accordance with the principle of "being accurate and kept up to date when necessary".

c) Norms Regarding the Liability and Compensation in Case of Breach of Substantive Guarantees

As per the liability for compensation, the PDPC, CPC, and the general liability principles of the administrative code should be taken into consideration. Article 18/1 (b) of the PDCP stipulates administrative fines ranging from 15,000 Turkish liras to 1,000,000 Turkish liras shall be imposed on those who fail to fulfil their data security obligations[25]. According to the article 18/1 (c) of the PDPC, an administrative fine from 25,000 Turkish liras to 1,000,000 Turkish liras shall be imposed in case the data processors and controllers fail to fulfil the decisions made by the Data Protection Authority[26]. Within the CPC, article 141 is relevant to predictive policing activities. The article regulates unlawful apprehension, arrest, search, and seizures. In such cases, the victim of such measures can request compensation for the material and moral damages from the State. In this context, it will be possible for people to claim compensation if AI technologies used during predictive policing activities lead to ineffective or erroneous arrest, detention, or search.

According to the general principles of administrative law, if public administration leads a poor and untimely service, or does not fulfil its duties such as securely processing personal data, the aggrieved person can apply accordingly for administrative compensation. In this context, faulty service of the public administration in the context of predictive policing requires also material or moral compensation. For example, if the personal data is shared disproportionately via AI technologies or if the necessary technical measures are not taken to ensure to prevent sensitive data leakage, the administration is liable[27]. In such cases, the concerned person can file a suit following Articles 12 and 13 of the Administrative Procedures Code.

Even if the administration acts responsibly and uses data anonymization while collecting data, there is still a possibility of harm to individuals. Especially during predictive activities, the administration's strict liability may arise. The concept of strict liability is the responsibility arising from the execution of an activity that contains risk, such as cyber-attacks. Thus, in cases where necessary precautions were taken while employing new technologies, it is still possible to demand compensation under the strict liability of public administration[28].

d) Norms Regarding Transparency of AI Systems in Turkish Law

As stated above, there is no regulation specific to AI-based systems in Turkey. However, institutions that develop and/or use these systems (regardless of the public or private sector) are obliged to comply with the obligations stipulated under the PDPC.

In addition, pursuant to clause 11 of the PDPC, natural persons whose personal data are processed, have the right to demand information as to if his/her personal data have been processed; to learn the purpose of the processing of his/her personal data and whether these personal data are used in compliance with the purpose; to know the third parties to whom their personal data are transferred within the country or abroad; to request the rectification of the incomplete or inaccurate data, if any; to request the erasure or destruction of his/her personal data under the conditions referred to in Article 7; to request reporting of the operations carried out[29] (to third parties to whom his/her personal data have been transferred); to object to the results in their disfavor based solely on data analysis

[25] The current amounts of the relevant fines after annual increases are as follows: 89,571 to 5.971.990 Turkish Liras

[26] The current amounts of the relevant fines after annual increases are as follows: 149,301 to 5.971.990 Turkish Liras

[27] Halil Altındağ, 'Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu', (2019) 18 Istanbul Kültür University Law Faculty Journal 387.

[28] Halil Altındağ, p. 396.

[29] "Pursuant to sub-paragraphs (d) and (e)"

by automated systems; to claim compensation for the damage arising from the unlawful processing of his/her personal data.

Individuals can use these rights against the data controller if their personal data are processed through AI-based systems. Although there are no explicit provisions regarding the principle of transparency in the PDPC, the general principles of data protection within Article 4 of the PDPC, the disclosure obligation of the data controller under Article 10, and the rights of data subjects within Article 11 provide mechanisms to ensure transparency. Moreover, Article 14 of the PDPC foresees a right to complain with the Personal Data Protection Authority, in case the controller refuses to respond to a request, provides an insufficient answer, or does not respond to within the specified period[30]. Therefore, the foretold provision can be a barrier to preventing the use of non-explainable software models while processing data.

However, the legislation on the protection of personal data may not provide complete protection against black box algorithms. As Özçelik stated[31] in case it is not possible to comprehend how these types of algorithms reach conclusions, it will be challenging to determine the fault after system-related damage occurs. Thus, it will be hard to detect the basic elements of legal responsibility, which are causation and fault. Therefore, there is an urgent need for legislation for explainable and transparent AI systems which ensure liability and consumer protection. With that perspective, the Human Rights Action Plan, published in April 2021, tackles a legal framework for AI systems[32].

As per trade secrets, different regulations involve provisions on a trade secret. For example, Article 73 of the Banking Law, Article 55 of the Turkish Commercial Code, Article 25 of the Law on the Protection of Competition, Article 6 of the Electronic Communications Law, Article 23 of the Law on Access to Information and Article 239 of the Turkish Penal Code contain provisions regarding trade secrets. However, these foretold regulations do not specifically address AI-based systems.

Nevertheless if, for example, during the purchase of a technology product, there is a request to obtain information about the working principles of that product and if it is protected under the Industrial Property Law, the company may refrain from disclosing the requested information to ensure the continuity of the benefit provided by this protection. On the other hand, the company may refuse to disclose how its products work, arguing that it is a trade secret.

Some sectoral regulations include strict provisions in terms of trade secrets, especially in transactions related to data sharing with third parties. These provisions can also apply to the transactions subject to AI systems. For example, the Regulation on the Sharing of Secret Information on sharing and transfer of bank secrets and customer secrets foresees that a bank secret or a customer secret can only be shared under exceptional circumstances. Exceptionally, such information may be shared with the authorities if explicitly authorized by law. In conclusion, if a request for an explanation from a company on how its products work does not comply with the exceptions specified in the Regulation, the Company may have the right to refuse this request to avoid a violation of the confidentiality obligation.

e) Norms Regarding the Liability of Companies Producing AI-Based Systems in Turkish Law

The liability of companies for the results of AI-based systems should be examined under legal and criminal liability. Since there is no specific regulation for AI-based systems, the existing criminal law and liability law

[30]According to Article 14 of PDPC, the data subject can complain to the Data Protection Board within thirty days after the data subject learns about the response of the data controller, or in any case within sixty days after the request is made to the data controller.

[31] Barış Özçelik, 'Legal Necessities Arising from Artificial Intelligence as Regards Data Protection, Civil Liability and Intellectual Property' 1 (2021) Adalet Journal, 87<https://dergipark.org.tr/tr/download/article-file/1778200 > accessed 10 February 2022.

[32] Ministry of Justice, p.120.

regulations will apply. In terms of legal liability, contractual liability and liability for negligence come to the fore. Since there is a limited number of principles in terms of strict liability, the responsibility of those who produce AI-based systems cannot be directly described as a state of strict liability. In terms of contractual liability, first of all, the relationship between the software developer and the manufacturer should be considered as an example. Parties entering into a contractual relationship are obliged to act in accordance with the rules of honesty (Principle of *Culpa in Contrehendo,* Turkish Civil Code, Art. 2)[33]. Within the scope of this obligation, it is required that the parties shall not act deceptively in the contract negotiations or the determination of its terms.

When the contract is concluded, one party may not fulfil its contractual obligation due to the failure or late performance of the contract by the other party. For example, if the software developer is late in her/his performance, the manufacturer may demand the performance or go before the court. On the other hand, if the manufacturer does not fulfil an obligation, the software developer can rely on the provisions of default of creditor or the provisions of breach of debt[34].

In terms of fault-based liability, there may be wrongful act when developing an artificial intelligence model and embedding this model into products. In the life cycle of AI, each stakeholder can cause damage with her/his faulty action. In this respect, as a rule, the person who acted wrongfully is responsible for the damage. The person who has suffered victimization and damage due to a wrongful act may demand compensation for the damage from the person or persons responsible for this action[35].

As per criminal liability, companies that produce AI-based systems do not have criminal liability.

According to the Turkish Penal Code, companies producing AI-based systems cannot be held liable. Pursuant to Article 20/2 of the TPC, only natural persons can be liable for criminal actions. Thus, no punitive sanctions can be imposed on legal entities. However, security measures can be imposed, if the law explicitly foresees it for the relevant crime. According to Article 60, the following security measures shall be imposed on legal entities only if the representatives or organs join the commitment of the crime and if the unfair advantage acquired by the perpetrator is provided to the legal entity:

According to Article 60, there are two measures, where specifically stated in the law: 1) If an intentional crime is committed for the benefit of a legal entity operating under a license granted by a public institution, and if an organ or a representative of the legal entity has participated in the crime and has misused the license for the commitment of crime, then the operating license shall be revoked, 2) Provisions pertaining to confiscation shall also apply to civil legal entities in case the offenses are committed for the benefit of such companies. On the other hand, according to Article 60/3, where the application of the foretold security measures results in disproportionate consequences to the offense itself, the judge may not impose such measures.

Thus, the imprisonment penalties and monetary sanctions in the TCC apply only to natural persons, who have committed a crime. If security measures are explicitly foreseen for a particular crime and if the commitment of such a crime creates an unlawful benefit to a legal entity, the security measures stipulated in Article 60 of TCC shall apply to such a legal entity.

In conclusion, security measures will be imposed on the legal entities if the conditions under Article 60 are met. It means when organs or representatives of the legal entity are actively involved in the crime as an accomplice and intentionally abuse their license to acquire benefits for the company, the revocation of the license of the company or the confiscation of its goods is possible.

[33] Kemal Oğuzman and M. Turgut Öz, *Borçlar Hukuku Genel Hükümler*, (16th edn, Vedat Publishing 2018), 77.

[34] Ibid, p. 355; Selin Çetin, Selin Çetin, 'Yapay Zekâ ve Hukuk ile ilgili Güncel Tartışmalar', the Report on Law in the AI Age, Istanbul Bar Association, 2019, <https://www.istanbulbarosu.org.tr/files/docs/Yapay_Zeka_Caginda_Hukuk2019.pdf>, accessed 07.02.2022, p. 60.

[35] Selin Çetin, 62.

f) Norms Regarding the Liability of Organisations Using AI-Based Systems in Turkey

Although there is no specific regulation to AI-based systems in Turkey, when the organisations process personal data, obligations stipulated under the PDPC shall apply.

At the same time, in accordance with Article 10 of the PDPC, the data controller or the person authorized by her/him is obliged to inform the relevant persons about the following during the processing of personal data: the identity of the data controller and of its representative, if any; the purpose of the personal data processing; to whom and for which purposes the processed personal data may be transferred; the method and legal basis of the collection of personal data; other rights referred to in Article 11.

Although the principle of transparency is not directly expressed in the PDPC, the above-mentioned obligations are included in the regulation to ensure transparency.

On the other hand, the relevant public institutions may include conditions for safeguarding transparency according to the goods and service procurement specifications.

Also, security measures can be applied to companies producing or using AI. Pursuant to 141/1 (a) of CPC, if a person is unlawfully arrested because of the use of AI technologies, this person may claim material and moral damages from the State. He/she further has the right to administrative and legal compensation.

g) Substantive Obligations of Police Authorities Using AI-Based Systems

The Police Code, CPC, and PDPC apply limit activities of law enforcement that involve the use of AI systems. As in most cases, AI-based systems interfere with the rights within the PDPC is particularly important in terms of transparency and accountability of law enforcement activities.

Article 28 of the PDPC stipulates a very complicated exclusionary clause. Accordingly, the PDPC does not apply to preventive activities regarding public security, public health, or public order. Article 28/2 (a) foresees further limitations for some rights regarding personal data in case the personal data is collected for crime prevention and investigation purposes. However, it should be noted that article 28/2 requires law enforcement to abide by the main principles and obligations within the PDPC. Accordingly, the personal data processed during predictive policing must have a legal basis, must be limited to a specific, legitimate, and explicit purpose; must be accurate, and up-to-date and must be processed for a limited time. Following Article 7 of the PDPC, law enforcement must fulfil the obligations regarding the deletion, destruction, or anonymization of personal data and follow the data transfer regime regulated in Articles 8 and 9, and ensure security of the processed data pursuant the Article 12[36]. In addition, the data subject can exercise the right to file a complaint to the Data Protection Authority and if his/her data is processed unlawfully, he/she has the right to compensation.

The Data Protection Authority (DPA) underlines all these abovementioned principles and obligations in its "Recommendation on the Protection of Personal Data in the Field of Artificial Intelligence" and emphasized that the protection of human rights and fundamental freedoms and the right to protect human dignity must be particularly safeguarded while employing AI technologies. In this recommendation, the DPA states that risk assessment for AI technologies is essential if there is a high risk of infringing the rights to data protection and privacy and such an assessment is a crucial indicator of the lawfulness of data processing[37]. The DPA also stresses in this recommendation that the purpose limitation is particularly relevant for such technologies, thus algorithms designed for a particular purpose should not be enforced for different purposes[38].

[36] Baran Kızılırmak, 252, 253.

[37] Türkiye Personal Data Protection Authority, 'Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler', <https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler>, Accessed 05.02.2022.

[38] Ibid, 12.

Therefore, before enforcing predictive policing tools, it is significant that the purpose for data processing is determined from the beginning, and the concerning tool is employed only for the determined purpose. Law enforcement activities aimed to prevent crime are, by their nature, different from activities for detecting and investigating crime. It should be also considered that once criminal procedures start, the principle of a fair trial will come into play. For these reasons, technologies deployed within the framework of predictive activities should not be used for crime investigation and prosecution purposes. In the Turkish law context, in the pre-crime area, primarily the Police Act applies, whereas with the investigation CPC provisions are applicable. In this context, additional Article 7/7 of the Police Code is crucial. According to the relevant provision, the data obtained for preventive purposes shall not be used for judicial purposes. Considering these prohibitions and the recommendation of the Data Protection Authority, the purpose set for AI tools changes the legal regime that applies and their use for other purposes would be unlawful.

3. General principles of law

a) Right to equality or non-discrimination

There are academic studies on the protection of the right to equality regarding AI-based systems used for predictive policing. These issues are also addressed in the academic studies listed in the "National Practice" part of this work. In this context, Sözüer stated that profiling algorithms in predictive policing will expose certain groups of people to extended law enforcement surveillance and intervention; which could result in different treatment of groups and discrimination[39].

İçer emphasizes that biased analysis is another weak point of the systems, as the reference datasets of facial recognition technologies are mainly based on white people; as a result, the system has difficulty recognizing other races and can produce erroneous results. Accordingly, these practices, which will be used to identify potential criminals and prevent crime, may produce biased results, and innocent people may be subject to various preventive and suppressive measures[40].

In addition, some public institutions focus particularly on non-discrimination and AI practices. In this context, the Human Rights and Equality Institution of Turkey organised an international symposium on "The Effects of Artificial Intelligence in the Context of the Prohibition of Discrimination" on 30 March 2022, where they stressed observing and preventing the discrimination risk in AI applications, including predictive policing activities[41].

b) Right to privacy

Before evaluating the protection of the right to privacy with regard to an AI-based system, the notion of privacy within Turkish law should be assessed. There are comprehensive discussions on the content, origin, and protection of the notion of privacy in Turkey. This right is referred to as "private life", "intimacy" and "secret space"[42]. Some doctrinal views underline that the scope of the right to privacy extends to all information that the person does not want to share and includes the protection of the inviolability of the belongings, communications, and residence, as well as the protection of the physical and mental immunity and intellectual freedom of individuals[43]. Some others argue this right also protects individuals against surveillance, monitoring, and harassment[44]. There are also discussions, which focus on the separation of the spheres of public life and private life and state that this dichotomy does not correspond to today's circumstances, which have drastically changed via AI technologies. On the contrary, it is pointed out that smartphones, smart homes, the internet of things, and

[39] Sözüer, 8.

[40] İçer, 41.

[41] Türkiye Human Rights and Equality Instutuion, 'Ayrımcılık Yasağı Bağlamında Yapay Zekâ Kullanımın Etkileri' (2022), https://www.tihek.gov.tr/ayrimcilik-yasagi-baglaminda-yapay-zeka-kullaniminin-etkileri-uluslararasi-sempozyumu/ Accessed 07.02.2022.

[42] Güçlü Akyürek, *Özel Hayatın Gizliliğini İhlal Suçu* (3rd edn, Seçkin Publishing 2021) 24.

[43] Ersan Şen '5237 sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar' (2005) 79 İstanbul Bar Association Journal 709, Akyürek, p. 37.

[44] Sultan Üzeltürk, *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı*, (1st edn Beta Publishing 2004) 169, Akyürek, p. 37.

computers have transformed the concept of "home", which is no more a private and intangible area. Thus, in the face of smart tools, the persons are deprived of a private space where they can think and act freely, shape their relationships without any concerns, establish their personalities, and do not have to abide by the expected roles[45].

There are several rights guaranteed regarding privacy within the Constitution, such as the right to privacy (art.20), inviolability of the home (art.21), and inviolability of communications (art. 22). The Constitutional Court safeguards these rights and ensures the compatibility of laws with the foretold articles, as well as legality, necessity, and proportionality of the enforced measure. On the other hand, predictive policing activities are not yet regulated with a foreseeable law, even if they interfere with the foretold rights.

If the law enforcement authorities are not empowered by law or act beyond the limits of their power, they can face sanctions foreseen by article 132 and the following within the TPC. For example, for law enforcement officers who violate the confidentiality of communication by not complying with the interception of communication procedures, the crime of violating the confidentiality of communication (art 132) applies. In Turkish law, there is no regulation that authorizes the law enforcement to use hacking or remotely accessing a person's IT system, thus such an act would also be considered as violation of article 131 (alongside with IT crimes). TPC article 133 regulates the intercepting and recording of non-public conversations between individuals. Furthermore, TPC article 135 stipulates illegal recording of personal data and TPC art. 136 further incriminates the unlawful transfer or seizure of personal data, and finally art. 138 regulates not destroying personal data within due time. Apart from these special provisions TPC art. 134 constitutes a more general provision protecting the right to privacy, thus violating the privacy of individuals was regulated as a crime. All these articles impose imprisonment. Therefore, the victim of these acts can initiate criminal proceedings against the perpetrators, or the public prosecutor can start an investigation ex-officio.

Additionally, pursuant to the PDPC, where personal data is processed, the concerned person may submit requests to the data controller. In compliance with article 13 of PDPC, the request must be answered within thirty days at the latest. If the request is rejected or the person concerned finds the response insufficient, pursuant to the article 14, it is possible for the data subject to apply to the Personal Data Protection Authority. Article 11 regulates the right to request compensation according to the PDPC; moreover, Article 14/3 stipulates the right to request compensation in courts.

However, among doctrinal discussions, it is often underlined that regulation regarding policing activities, particularly data processing via law enforcement falls short in the face of new predictive policing activities. Therefore, it is often underlined that there is a need for similar regulation to the (EU) Directive 2016/680[46].

c) Right to liberty and security

The use of AI-based systems for predictive policing interferes with the right to liberty and security, thus according to Article 19 of the Constitution on right to freedom and security, such systems must be regulated with an explicit law. However, currently, there is no regulation on the use of artificial-based technologies in Turkey.

Therefore, there are discussions on software models in Europe and America, such as COMPAS, Static 99, SyRI that detect possible perpetrators and affects the decisions on arrest, search, and bail. It is emphasized that such tools cannot be used by law enforcement without a legal basis. Moreover, as will be discussed further below, such software systems transform the threshold of suspicion in criminal law, and they shift the focus from the criminal act to the perpetrators. Furthermore, in legal doctrine and practice, it is emphasized that the coercive measures must meet the reasonable suspicion threshold, which requires individualised suspicion. However, such predictive tools evaluate certain groups as more prone to commit crimes than others and create non-individualized group profiles. For all these reasons, the use of such technologies for restricting the right to

[45] Irmak Erdoğan, p. 54.

[46] See Dülger&Özkan, p. 140, Kızılırmak, p. 258.

freedom and security, without a legal base or procedural guarantees constitutes an intrusive interference with Article 5 of the European Convention on Human Rights and Article 19 of the Turkish Constitution[47].

One of the most important prohibitions that guarantee the right to freedom and security, and human dignity is the prohibition of unlawful evidence. In Turkey, there is a strict exclusionary regime, meaning that any measure to collect evidence must comply with the Constitution, all applicable regulations, laws, international agreements, and the general principles of law. The Constitutional Court also confirms the strict exclusion of illegal evidence[48]. It means the use of preventive technologies must comply with all the applicable rules and regulations, or else their results cannot be used as evidence. For example, if personal data protection regulations are not followed while data processing, the results of predictive tools will be excluded as unlawful evidence. Pursuant the Article 206/2 (a) of CPC, illegally obtained evidence cannot be submitted to the court. The Article 217/2 of CPC stipulates further that unlawful evidence cannot be used as a basis for the decision, and thus cannot be used as proof of the facts. For this reason, it should be emphasized that the results obtained with AI-based systems, which lack legal basis or do not comply with the existing norms cannot be used as evidence.

d) Principle of proportionality

Due to the advancements in AI-based systems and big data, it has become possible to collect data indiscriminately which is far beyond necessary for establishing a link between the criminal act and the perpetrator. For safeguarding principle of proportionality, it is stated in the doctrine that it is necessary to investigate whether there are other measures, which could less intrusively interfere with the rights and freedoms of the individual. The doctrinal views also underline that if sensitive data is collected or revealed, law enforcement must guarantee that it does not lead to discrimination. Particularly, it is underlined that profiling technologies lead people to be included on heat lists or terrorist lists, which also has a chilling impact on the freedom of expression, assembly, and association, as well as affecting freedom of movement. Considering all the endangered rights, such tools are likely to violate the principle of proportionality[49].

Therefore, during the predictive policing, the article 13 of the Constitution must be considered, which imposes that any intervention with the personal rights and freedoms shall have a legitimate purpose, shall be in line with the word and spirit of the Constitution and the requirements of the democratic social order and fulfil the principle of proportionality. Such technologies should be applied only if they serve the predetermined purpose in the least intrusive way.

e) Procedural legality

Predictive policing can include the pre-crime or after-crime activities. If AI-based tools are enforced after the crime, meaning during the phases of investigation and prosecution, they must comply with the provisions of the CPC.

The provisions of the CPC apply when the public prosecutors learn about the commission of a crime through a complaint, request, or ex officio a crime has been committed. Thus, in case AI-based systems lead to disclosing a crime, the public prosecutor must be informed. Once an investigation starts based on facts that a crime has been committed, the law enforcement officers cannot act without consulting the prosecutor. To start an investigation, the suspicion must base on real facts or events[50]. Thus, assumptions, personal inferences, or criminalistic hypotheses cannot meet the threshold of the basic suspicion to initiate an investigation[51] Therefore, algorithmic

[47] Sözüer, 7.

[48] Turkish Constitutional Court, E:1999/2, K:2001/2, see Güçlü Akyürek, 'Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu' (2012) 102 Turkish Bar Association Law Journal 61.

[49] Irmak Erdoğan, 179

[50] İlyas Şahin, 'Türk Ceza Yargılaması Hukukunda Koruma Tedbirleri Bakımından Esas Alınan Şüphe Kavramının İncelenmesi', (2014) 20 Marmara University Law Faculty Journal 97

[51] Zehra Yılmaz, *Ceza Muhakemesi Hukukunda Şüphe*, Master Thesis (Selçuk University 2019) 83.

assumptions based solely on profiling data, such as analysis of the characteristics, social, economic conditions, and tendencies of individuals and groups could not per se initiate a criminal investigation.

As per applying coercive measures, the threshold for suspicion must be shown based on the criminal act. Resorting to coercive measures without fulfilling the threshold will constitute an unfair and unlawful interference with fundamental rights and freedoms[52]

There is not a common threshold for suspicion, which applies to all coercive measures under the CPC. Considering the intensity of the intervention via the relevant protection measure with the rights and freedoms, the threshold of suspicion is regulated separately for each measure. It varies from reasonable suspicion to probable cause; however, the simple doubt to start an investigation does never suffice to impose coercive measures, which restrict the rights of a suspect before a verdict.

The definition of reasonable suspicion in Turkish legislation is similar to the reasonable suspicion threshold stipulated in the ECHR, Europe, and the US. Accordingly, it must base on the information and facts that can convince an impartial person that a particular perpetrator may have committed a crime[53]

Therefore, the suspicion must be based on specific and objective facts. These facts should relate to the criminal act, hence not to the perpetrator. The facts and evidence in question must be obtained before the relevant measure is implemented. Personal qualities can be taken as a basis in the evaluation of all the circumstances of the event, but only if they are relevant to the criminal act in question, they will form a basis for suspicion. Therefore, if the actions and preferences of the person, which are not related to crime, are exposed by AI-based technologies, this information cannot be used in criminal proceedings to impose coercive measures.

Within the scope of the CPC, measures such as computer searches (Article 134), interception of communication (Article 135), and technical surveillance (Article 140) are explicitly regulated. To apply these measures, there must be an individualized, reasonable suspicion (for some measures probable cause) and an affirmative decision of the judge. The law enforcement authorities cannot implement AI tools in criminal procedures that are not specifically regulated in the CPC, and they cannot limit the rights and freedoms based on a collective and non-individualised suspicion, such as suspicion based on group profiling.

Predictive activities also can take place before a crime is committed. In this case, the provisions of the Police Act apply. The Police Act regulates explicitly the interception of the communications and technical surveillance in additional article 7. These activities in the pre-crime area must also be carried out under the supervision of a judge. Although such measures can be imposed without being based on any suspicion of a crime, there are some limitations foreseen within article 7. The judicial decision allowing the measure must be in written form; must include the identity of the person to whom the measure will be applied; the type of communication tool to be used must indicate the relevant phone number or internet connection address; the type, scope, and duration of the measure. The decision must also be reasoned. If the law enforcement does not enforce coercive measures but seeks to collect general information, Article 15 of the Police Act applies. Unlike the articles regarding coercive measures, this article stipulates the information gathering activities without imposing extra safeguards and limitations. However, Article 15 does not apply once a person is held as a suspect for a crime. If there is an individualised suspicion, which links an act to a particular person, the CPC regulations, hence the rights and safeguards for the suspects, shall apply.

f) Constitutional Principles Regarding the Use of AI-based Systems for Predictive Policing

[52] Yener Ünver & Hakan Hakeri, *Ceza Muhakemesi Hukuku* (15th edn, Adalet Publishing 2019) 685, Veli Özer Özbek, Koray Doğan & Pınar Bacaksız, *Ceza Muhakemesi Hukuku* (14th edn, Seçkin Publishing 2021) 258.

[53] Yılmaz, 91, 92.

Predictive policing aims to protect public order and prevent crime. However, to implement coercive measures against individuals, there must be a concrete danger of harm to public order. If AI-based systems are used after the crime has been committed, they must aim to establish the link between the suspect and the criminal act. Making associations between indiscriminate data that does not necessarily serve this purpose. Particularly if only certain groups are targeted via AI-based systems, it will constitute a violation of the principle of equality stipulated in Article 10 of the Constitution.

Approaching citizens as potential suspects and collecting their data indiscriminately also infringe the presumption of innocence pursuant the Article 38 of the Constitution. Furthermore, the principle of *nemo tenetur*, which is also protected under Article 38, must be considered, as no one can be compelled to make a statement or show evidence accusing himself. In this context, the Internet of Things allows revealing when a person entered/left the house, profiling tools show the suspect's habits, tendencies, personal connections and other information. Revealing all this information constitutes an interference with the right to remain silent and the right against self-incrimination. Therefore, the use of AI technologies must have limits, which would not infringe the essence of the constitutional rights of the suspects.

Article 38 of the Constitution stipulates individual criminal liability. If AI-based systems lead to suspicion by profiling certain groups as potential suspects, in this case, Article 38 will be breached. Finally, the Constitution m. 38 requires that all the information or data must be collected in compliance with the law, thus any breach of the current laws, regulations, the Constitution, international agreements, and the general principles of law while data collection would constitute illegal evidence. Thus, according to the Constitution such evidence must be excluded in criminal proceedings.

II. PREDICTIVE JUSTICE

1. National practices

There is no definition of predictive justice in Turkish legislation. However, there are several resources related to this subject. For example, the use of new and predictive technologies in the judiciary is discussed in the guide published within the scope of the Project on 'Increasing the Internship Efficiency and Effectiveness of Judge and Prosecutor Candidates'[54]. In addition, in public debates and literature, the terms such as 'use of artificial intelligence in the judiciary', 'predictive justice' or 'algorithmic justice' are used in close affinity with the concept of predictive justice. It is emphasized that artificial intelligence can be used in judicial applications in three ways: assisting the judge, preparing the decision drafts, and making the decisions. Thus, these systems must first have an ethical framework[55].

The Use of AI-based systems for predictive justice in Turkey

In Turkey, AI-based systems are not used for predictive justice. However, the Minister of Justice of the time in 2020 stated a branch was established within the Ministry, whose task is only to work on artificial intelligence. The Ministry aims of developing practices to speed up judicial proceedings and eliminate the possibility of errors, which could alleviate the workload in the current judicial system[56]. Although further news and statements on the subject appeared in the written and digital media[57], there is still no official framework that guides the method and scope of predictive justice practices.

According to the statements and the news in the media, it is seen that the main motivation for considering the use of AI-based systems for predictive justice is to expedite procedures in the judiciary and to increase the efficiency of the judicial process. In addition, one issue of the academic journal of the Ministry of Justice is specifically dedicated to the title of 'Artificial Intelligence and Law'[58]. It is further targeted to enhance the National Judicial Network Project of the Ministry of Justice (UYAP) with artificial intelligence-based systems and to make it more 'intelligent' to contribute to the Turkish judiciary[59].

In Turkey, there is no obligation and no regulation regarding the use of AI-based systems for predictive justice by judicial authorities at any stage of the criminal process. Thus, the doctrine warns that the lack of regulation on this issue will pose a problem in terms of investigations and prosecutions based on AI-based systems and there is an urgent need for detailed regulation. Thus, it is necessary to pay attention to compliance with legal and ethical principles in the development of related AI applications and to integrate them into the judicial system.

[54] Antoni Oliver and Rafael Fernández de Páiz, *Adalet Alanında Yeni Teknolojiler, Hâkim ve Savcı Adaylarının Staj Verimliliğinin ve Etkinliğinin Artırılması Eşleştirme Projesi* < https://adaylik.adalet.gov.tr/Resimler/221220201522adalet-alaninda-yeni-teknolojiler-modulupdf.pdf> accessed 16 July 2021.

[55] Oğuz Gökhan Yılmaz, 'Yargı Uygulamasında Yapay Zeka Kullanımı-Yapay Zeka Hakim Cübbesini Giyebilecek Mi?' (2021) Adalet Journal <https://dergipark.org.tr/tr/download/article-file/1779680> accessed 16 June 2021.

[56] Kıvanç El, 'Adalet Yapay Zekaya Emanet' (2020) Milliyet Newspaper < https://www.milliyet.com.tr/gundem/adalet-yapay-zekaya-emanet-6302654> accessed 16 July 2021.

[57]'Yargıda yapay zekâ uygulamaları kullanılacak' (2021) BT News <https://www.bthaber.com/yargida-yapay-zeka-uygulamalari-kullanilacak/>, 'Temyiz süreci kısalıyor, Yargıda yapay zeka dönemi' (2021) Akşam Newspaper <https://www.aksam.com.tr/guncel/temyiz-sureci-kisaliyor-yargida-yapay-zeka-donemi/haber-1232716> accessed 16 June 2021.

[58] Ministry of Justice, 'Adalet Degisinin 66. Sayısı "Yapay Zeka ve Hukuk" Dosyası Yayımlandı' (2021) <https://basin.adalet.gov.tr/adalet-dergisinin-66-sayisi-yapay-zeka-ve-hukuk-dosyasi-ile-yayimlandi>, accessed 16 June 2021.

[59] Emre Kıyak, 'Büyük Veri ve Yapay Zekâ Teknolojileri ile Adım Adım Zeki Uyap (Ulusal Yargı Ağı Projesi) Ekosistemine Doğru' (2020) 22 Dokuz Eylül University Law Faculty Journal 79 <https://doi.org/10.33717/deuhfd.704837>, accessed 16 June 2021.

On the other hand, there are private companies working on artificial intelligence applications that can be used in the judiciary in Turkey[60]. Nevertheless, there is no information that the applications developed by these companies are being used in the judiciary. Also, there is no scientific study that reveals the possible difference between the predictive justice practices and current judicial decisions, nor there is any information on the effect of such practices on the criminal justice system.

While there is no widespread discussion of the use of AI-based systems for predictive justice, there are some academic studies. For example, it is emphasized that artificial intelligence can be used in judicial practices in three ways: AI systems can assist the judges, prepare decision drafts, and take decisions. It is emphasized that all these systems must first have an ethical framework[61]. On the other hand, it is stated that determining whether the fairness of AI systems is particularly problematic when such systems are applied to alternative dispute resolution, and it is important to access a judge instead of an AI system for a request[62]. In parallel, it is emphasized that the use of AI systems in judicial activities may have positive effects such as speeding up access to justice and efficiency but may cause violations in the processing of personal data and that the system should undergo a human audit equal to the level of risk posed.

2. Normative framework

Law and soft law

In Turkey, there are no specific regulations or draft proposals concerning the use of AI-based systems for predictive justice. Also, there are currently no soft-law resources related to predictive justice.

The Human Rights Action Plan published in April 2021 targets to integrate the artificial intelligence applications in the judiciary in accordance with the principles and recommendations of the Council of Europe and in compliance with legal guarantees[63]. Although no detailed information is shared with the public, the above-mentioned statements of the Ministry of Justice officials and media posts show the intention to include AI-based systems in predictive justice in the near future.

Case law

In Turkey, only high court decisions are shared with the public. In this context, no decision has been found regarding AI-based systems used for predictive justice.

Substantive guarantees

a) Transparency and Right to Information

In Turkey, there is no specific regulation to inform the parties about the important results of AI calculation. However, in cases where personal data is processed through these systems, the rights, and obligations within the Personal Data Protection Code No. 6698 (PDPC) apply.

According to the article 11/1 (g) of the PDPC, data subjects have the right to object to the adverse legal effect concerning them, produced by solely automated analysis of data. Thus, data subjects have the right to object to the data controllers concerning the results provided by AI calculations.

[60] ODTÜ Teknokent, 'Kodex Bilişim'den Yargıtay davalarına yapay zekalı destek' <http://odtuteknokent.com.tr/tr/haber/kodex-bilisimden-yargitay-davalarina-yapay-zekali-destek> accessed 16 July 2021.

[61] Oğuz Gökhan Yılmaz, 'Yargı Uygulamasında Yapay Zeka Kullanımı-Yapay Zeka Hakim Cübbesini Giyebilecek Mi?' (2021) 66 Adalet Journal < https://dergipark.org.tr/tr/download/article-file/1779680 > accessed 16 June 2021.

[62] Gökhan Erdoğan, 'Yapay Zekâ ve Hukukuna Genel Bakış' (2021) 66 Adalet Dergisi 117 https://dergipark.org.tr/tr/download/article-file/1778256 > accessed 16 June 2021.

[63] Turkish Ministry of Justice, *Human Right Action Plan* (2021) <https://insanhaklarieylemplani.adalet.gov.tr/resimler/%C4%B0nsan_Haklar%C4%B1_Eylem_Plan%C4%B1_ve_Uygulama_Takvimi.pdf> accessed 16 June 2021.

Apart from the right foreseen within the PDCP, the general principles of adversarial jurisdiction and equality of arms apply. These principles require that in case AI-based systems are used during criminal proceedings, their results must be shared with the parties. They enable the parties to have the right of access the file (CPC art. 153) and examine the information and documents in the file that form the basis of the accusation.

Although certain limits may be imposed on the right to access to the file for not to endanger the investigation, during the trial phase, the publicity of the hearing is mandatory. To implement the principle of adversarial trial, witness testimonies obtained via the "letters rogatory" procedure, crime scene reports, and other information regarding the defendant must be shared and read during the trial. Otherwise, they cannot be accepted as evidence (CPC art. 209). Furthermore, the defendant and his counsel must have the right to challenge the presented documents (CPC art. 215). The judge may base his decision on the evidence brought to the hearing and discussed before him (CPC art. 217).

There is no special regulation, which foresees exceptions for the AI-based evidence; therefore, these systems and their conclusions must be shared with the victim and defendant, and the defence must be given the right to object. If the operation of these technologies requires technical knowledge or if there is doubt about their integrity, according to Article 63 of the CPC, they should be examined by an expert. Following Article 63/4, the report samples prepared by the expert should be shared with the public prosecutor, the participant, his/her lawyer, the suspect/the defendant, and his defence counsel during the hearing. If the report is considered erroneous or contradictory, it will be not accepted as sound and reliable evidence. In that sense, under Article 63/5, the parties have the right to object to the expert examinations and to request a new expert opinion. It is also possible for the parties to request an opinion from another expert to evaluate the results.

In the light of these rules, as AI-based evidence cannot be explained without experts, the Courts must request an explanation of the technical aspects of such tools and share the results with the parties. The defendant must be allowed to understand the basis of the allegations against him and challenge such results. He/she can ask for further examination by other experts.

b) Accountability

As a general rule, the convicted persons have the right to appeal pursuant the articles 267 and 286 of the CPC. In addition, if the conditional release is refused; the convicted person can oppose this decision in accordance with article 107/11 of the Code numbered 5275.

In case the AI-based system results are considered for the final decision, the court must examine the functioning of these systems and their results before reaching a conclusion. Apart from the general rules, no special remedies for AI systems are foreseen in Turkish law.

Third parties affected by the automatic decisions made by such technologies can enforce the rights within PDPC, particularly the right not to be subjected to adverse results of solely automated analysis pursuant the Article 11. Furthermore, if the personal data rights of the third parties are infringed, they can contest before the Personal Data Protection Authority.

However, the doctrine underlines the need for more specific rights for ensuring the right to a fair trial, particularly the transparency of the hearing, the right of defence and the equality of arms, and the right to defence in the case of the use of AI-based systems. Particularly, the doctrine insists that there must be a legal regulation that specifically foresees the obligation to expose which data are used and processed via an AI system and how the algorithm functions. Furthermore, the regulations must enforce testing the accuracy of the AI systems. In addition, doctrinal discussions propose that AI-based systems should be used in criminal justice only for crimes of a certain severity, and they must be exposed to regular auditing.

Finally, it is argued that AI systems reveal information about a person's past and process all the traces they left which they shared without knowing that they will be the subject of the investigation. It may infringe the right to remain silent and nemo tenetur, which are among the fundamental principles of a fair trial.

c) Independence of the Judges

The 2021 report of the Istanbul Bar Association Informatics Law Commission AI Working Group states that AI-based risk assessment tools may pose problems to the fair trial regarding the independence and impartiality of the judges. In order to ensure it, 'scientific, impartial and technological output' must be presented to judges, and he/she must conclude his/her decision on a conscientious opinion, based on such an impartial output. This report questions whether the evaluation will affect the independence and impartiality of the evaluation based on the data presented and states that the judges may have a tendency to automatically accept the suggestions of these systems in order to avoid any risks. It may in return lead to automated bias[64].

Although there are similar academic and practical discussions in Turkey[65], there are no special procedures or guarantees to ensure the independence of the judge when using AI-based systems.

d) The right of access to a human judge

There is no widespread discussion in Turkey regarding the need to recognize the right of access to a human judge, as it is not likely AI judges to completely replace human judges in the near future. However, this issue has been addressed in several academic articles. In the article titled 'Artificial Intelligence Assets and Criminal Law', Hakan Aksoy emphasizes the use of AI judges might be possible in civil cases, yet they cannot serve in criminal proceedings. In this context, according to Article 138 of the Constitution of the Republic of Turkey, judges shall make judgments 'according to the law and their conscientious convictions'. Similarly, Article 217/1 of CPC states that the judge can freely evaluate the evidence according to his conscience. Thus, judges in criminal procedures can decide only according to the conscientious opinion based on the evidence. Therefore, the possibility of artificial intelligence entities replacing judges and their conscientious opinion does not seem possible very soon, especially since cognitive characteristics such as the psychology of justice, risk-taking, and reasoning cannot be calculated mathematically[66].

e) The presumption of innocence

Some of the AI systems reach conclusions relevant to the facts of the case, such as traffic cameras recording and reporting the violation of speed limits. The other AI technologies, especially risk analysis tools, pave the way for obtaining all personal data of a person. Thus, in the short term or distant future, big data transform the whole life cycle of people into statistics.

This transformation shifts the focus from the criminal act towards the dangerousness of 'future' perpetrators. It leads everyone to defend themselves against allegations based on the acts that they have not yet committed. In criminal proceedings, the presumption of innocence implies that evidence should lead to the perpetrator, and for the criminal verdict; the judicial authority must establish the link between the criminal act and the perpetrator without a doubt. Turkish doctrine discusses that AI-based systems based on big data might reverse this process.

[64] Ozan Can Özbalçık, 'Artificial Intelligence-Based Risk Assessment Tools in Criminal Procedure and Its Legal Effects' (2021) Istanbul Bar Association AI Working Group <https://www.istanbulbarosu.org.tr/files/komisyonlar/yzcg/2021yzcgyillikrapor.pdf> accessed 16 July 2021.

[65] Istanbul Bar Association AI Working Group, 'Yapay Zekâ ve Ceza Hukuku' (2021) Annual Conference <https://www.youtube.com/watch?v=cgTtqj8kRl4&t=17s>, Istanbul Bar Assiciation, 'Ceza Muhakemesinde Yapay Zeka Kullanımı: Riskler ve Tavsiyeler' (2022) Monthly Online Education <https://www.youtube.com/watch?v=MdDqH_hZTbs> accessed 16 July 2021.

[66] Hakan Aksoy, 'Yapay Zekalı Varlıklar ve Ceza Hukuku' (2021) 4 International Journal of Economics, Politics, Humanities & Social Sciences <https://dergipark.org.tr/en/download/article-file/1293489> accessed 16 July 2021.

Hence, there is an inherent risk of using AI tools, as they automatically deem the suspect/defendant as dangerous, which causes them to turn into objects of the case who struggle against the 'presumption of guilt'[67].

f) The right to a fair trial

There are no examples of the use of AI tools within the scope of predictive justice yet. However, the doctrine is already discussing how to establish the principles of equality of arms and adversarial process in a predictive justice system. In this context, the right to object and to request an audit for the outputs of AI-based risk assessment tools is considered an indispensable component of the principle of equality of arms. Furthermore, if such risk results constitute the basis for judicial decisions, doctrinal discussions point out that there should be a specific right to contest the results of AI-based systems[68]. Nevertheless, there are still no specific regulations regarding the right to object to the use of an AI-based system in the framework of predictive justice. In that sense, general rules within Criminal Procedures Code apply to challenge the incriminating evidence.

The Turkish doctrine also concentrates on the black box problem arising out of the use of unexplainable AI systems. Accordingly, it will impair the suspect's right to defense if the suspect cannot learn what kind of data AI-based systems process and how such systems reach their conclusions. There is not yet an exemplary case where a protective measure has been applied or a judgment has been established against the accused based on an algorithmic calculation. For this reason, it is not yet clear whether the defendants will have equal means of defence in practice.

On the other hand, the processing of personal data for judicial purposes by the judicial authorities is completely exempted from the scope of PDPC. Thus when judicial authorities enforce algorithmic applications, the personal data protection regulations do not apply. Such a legal loophole makes the defendant more prone to the violation of the equality of arms principle during criminal proceedings. Even if the accused/defendant has the right to access and object to all the evidence and resources constituting an accusation against him/her, the doctrine emphasizes that the use of big data applications should be regulated by a separate law to enhance the individual's rights.

Turkish doctrine scrutinizes philosophical concepts such as justice as well as possible problems that may arise if human reasoning is converted into a mathematical calculation, such as losing flexibility, nuances, and essence of real-life situations[69]. Similarly, Muharrem Kılıç, President of the Human Rights and Equality Institution of Turkey, interprets this issue in his article titled 'Transhumanistic Representations of the Legal Mind and Onto-Robotic Forms of Existence' as 'legal singularity'. He predicts that the legal system based on this 'legal singularity' targets to eliminate the 'legal uncertainty'. However, the idea of 'legal singularity', which seeks 'uniformity, harmonization and integration' through a structural transformation in the legal system, ignores the domestic character of legal rules. The singularity ideal, which does not take into account the economic and cultural dynamics of the social structure, may lead to an 'apolitical social mechanism'. It implies that representative onto-robotic devices will not be able to establish 'justice, fairness, and conscience'. Therefore, considering the main principles of law, establishing criminal justice through mathematical reasoning raises some essential ethical-judicial concerns. [70]

Furthermore, the discussions on privatisation of criminal justice are also relevant to the fairness of the processes. In this context, the doctrine underlines that the private sector developing big data programs becomes more in charge of the process, while the public officials use such complex software programs without any technical knowledge. Thus, those who work in the justice service become just customers and passive users of these

[67] Irmak Erdoğan, 41.

[68] See Özbalçık, *Istanbul Bar Associaton IT Commission AI Working Group 2021 Report.*

[69] Öztürk ve Diğerleri, Dijital Ceza Muhakemesi Hukuku, p. 234, Seçkin, 2021.

[70] Muharrem Kılıç, 'Hukuksal Aklın Transhümanistik Temsilleri ve Onto-Robotik Varoluş Formları' (2021) 66 Adalet Journal < https://app.trdizin.gov.tr/publication/paper/detail/TkRZeU9EYzVPUT09> accessed 16 July 2021.

programs. The designers of software programs for automated decision-making and the users of such programmes within criminal justice are alienated from each other. Therefore, there is a risk that the criminal justice system transforms into a process in which experts from other professions will be in charge rather than judges, prosecutors, and lawyers. Those who write algorithms are mostly unfamiliar with the legal system and its principles, whereas those who implement it use these technologies automatically in the face of complexity and obscurity in algorithms. Hence, the arguments about privatization focus on all these factors that may indirectly harm the independence of the judiciary[71].

[71] Özgür Taşdemir, 'Ceza Adaletini Dijitalleştirmek, Büyük Veri Vicdani Kanaate Karşı', in Yaşar Bilge (ed.), *Sağlık Alanında Büyük Veri Analitiği ve Uygulamaları* (Türkiye Klinikleri 2021).

III. EVIDENCE LAW

1. Evidence gathering through AI-based systems

There is no judicial decision regarding evidence gathering through large quantities of documents and communications via AI-based systems. Under normal circumstances, it is possible for companies to integrate some filters for information security into their information systems. The companies try to prevent information leakage outside the company via these filters and tracking mechanisms. However; following and analyzing all employees of a company or all citizens of a state via artificial intelligence systems indiscriminately without concrete suspicion of a crime and a court decision that sets a certain limitation, would be contrary to the fundamental rights enshrined in the Turkish Constitution.

In the meantime, there has been a critical discussion recently. The leadership of the main opposition party claimed that the Information and Communication Technologies Authority, which is the authority of informatics and telecommunication in Turkey, confidentially demands "subscribe pattern" and "internet traffic log records" of all users within the country from service providers to process these big data set and profile citizens via AI systems unconstitutionally [72].

On the other hand, Information Technology Authority and National Cyber Security Incident Response Team, carry out AI-based intelligence activities on the internet to ensure national cyber security.

Also, public authorities of heavily regulated sectors like the Capital Markets Board, carry out AI-based follow-up and data analysis on public capital market transactions to prevent sectoral manipulation.

Finally, AI-based systems are used by experts that are appointed by court and prosecutors, police and gendarmerie criminal experts, and the Council of Forensic Medicine experts. Features and working models of AI systems are coded openly for the audit of expert reports.

2. Evidence produced by AI-based systems

a) Facial recognition and voice recognition via AI-based systems

Facial recognition systems are used within the framework of preventive law enforcement operations in high-crime-risk public places like airports. However, such applications are not shared with the public in detail.

The experts can examine high-resolution video recordings at ATMs or high-quality sound recordings, within the framework of criminal investigations and proceedings for acquiring evidence and report outputs of these examinations to the case file as expert report evidence.

b) Treaties and international agreements on the admissibility of digital evidence

The Council of Europe played a leading role as a regional organization in making international regulations on cybercrime. The works that started in the committees established in the mid-1980s became concrete with the work of the Cybercrime expert committee established in 1996, which at first became a draft contract, and then European Cybercrime Convention was opened for signature on 23 November 2001 in Budapest. The Convention has become a part of domestic law in Turkey with the "Law on Approval of the Convention on Crimes Committed in the Virtual Environment" numbered 6533, which has been published in the Official Gazette dated May 2, 2014.

[72] For claims of Onursal Adıgüzel see 'BTK'nın fişleme skandalı' (Politikyol, 12 December 2022) <https://www.politikyol.com/btknin-fisleme-skandali > accessed 16 December 2022.

For this reason, cybercrime regulations shall abide within the principles of the Convention to which Turkey is a party.

Criminal Procedure Code (CPC) Art.134, which corresponds to the Articles 18 and the Articles 19 of the Convention is the main regulation on forensic informatics in Turkish law. This Article is going to be analysed in detail, but it should also be noted that the CPC Art.134 is not a sufficient instrument for the fight against cybercrime and related AI-based applications.

3. Evidence assessed by AI-based systems

In Turkey, the principle of free evaluation of evidence applies following the Turkish Criminal Procedure Code. According to this principle, there are no rules, which require only certain types of evidence to support or refute the guilt. Thus, any evidence, which is legally obtained, can be used in court[73]. Therefore, the crime can be proved by a variety of evidence and judges can evaluate them freely[74]. Furthermore, all parties can contribute to finding evidence, thus the investigation authorities do not have a monopoly on evidence collection. Hence, no special restrictions and regulations apply to AI-based evidence.

However, all evidence, including AI-based evidence must fulfill some basic qualifications. Firstly, the results achieved with AI systems must be realistic. In other words, it must point to reality perceivable by the five senses[75]. In addition, the evidence must be rational. Only the evidence reached by rational reasoning and referring to material truth can be accepted. For this reason, the AI-based system should be scientifically sound and rational. In addition, the evidence must represent the facts of the case partially or comprehensively[76]. In that sense, any fact or information, which is not relevant to the facts of the case, has no evidential value. The relevance element is regulated within Article 206/2 (b) of CPC, which stipulates that evidence will be rejected if it does not contribute to the establishment of the facts of the case. In fact, including information, which is not related to the facts of the case, may create prejudice against the perpetrator and cast a shadow on the objective opinion. Therefore, data only referring to the personality of the suspect cannot be accepted as evidence, as it will affect the impartiality of the court. The representative character of the evidence also requires that the evidence is solid, thus, reliable. The robustness of the evidence is evaluated by itself and by considering it together with other evidence. Although the court has the discretion of deciding the reliability of the source, the claimant and defendant must participate in this process. Otherwise, if the defendant cannot contest the reliability of the accusatory evidence or lacks the information that allows him/her to object to it, the soundness of the evidence cannot be challenged. In this context, sharing the source data and other information regarding the evidence produced by AI-based systems is important for the equality of arms.

One of the most important traits of evidence in the Turkish Criminal Procedure system is that it should be challenged collectively. It is not sufficient that the evidence is accessed only by the judge. Allegation and defence also need to access the evidence and participate collectively in the assessment process. Therefore, the element of collectiveness serves as the basis of the right to defence and a fair trial. The Court of Cassation reverses first-instance decisions in case of breach of the collective aspect of evidence. Accordingly, for example, to use the interception of communication records as evidence, they must be presented in the case file and must be discussed during the hearings[77]. Furthermore, one cannot constitute a decision based on the evidence which was not read

[73] Ünver/Hakeri, 1453

[74] Cumhur Şahin and Neslihan Göktürk, *Ceza Muhakemesi Hukuku II* (11th edn, Seçkin Publishing 2021) 32.

[75] Birtek, 56, Şahin and Göktürk, *Ceza Muhakemesi Hukuku II*, 34. According to the Turkish Court of Cassation, the evidence must be "rational, in compliance with science, material truth, and legal norms" and the legal truth can only be established by the evidence which is "reasonable and represents facts of the case partially or comprehensively"; furthermore, all evidence should be assessed together, see Court of Cassation 6. CD, E. 2020/207, K. 2020/4968, T. 15.12.2020, <https://lib.kazanci.com.tr/> accessed 16.07.2021.

[76] Ünver/Haker, 1454, Yenisey/Nuhoğlu, 514.

[77] Court of Cassation, 10. CD, E. 2020/1651, K. 2021/3431, T. 11.03.2021 < https://lib.kazanci.com.tr/ > accessed 16 June 2021.

at the hearing and therefore was not challenged by the accused[78]. Finally using the evidence without letting the parties discuss its robustness before the court[79] constitutes a breach of evidence law.

In conclusion, the judge's power to freely assess the evidence is not limitless and pursuant the Article 217 of the CPC, the judge can base his conscientious opinion only on evidence, which was brought to trial and discussed before the court. The claimant, defendant, and judicial actors must be able to understand the content of the evidence. Otherwise, the right to defence could not be exercised effectively. Similarly, the Constitutional Court decided that the assessment of the reliability of digital evidence requires technical knowledge, thus using solely the law enforcement's report on digital evidence and not sharing it with the defence infringe the principle of equality of arms and the right to a fair trial[80].

Finally, the evidence must be obtained lawfully. Since there is an absolute prohibition of illegal evidence in Turkey, if AI systems breach any legal norm, they cannot be used as evidence. Thus, unlawful evidence cannot be taken as a basis for a verdict and the strict exclusionary rule applies to AI-based evidence as well. For this reason, the compliance of the AI system with the basic principles of law, international conventions, data protection norms, and the CPC is essential. Pursuant to Article 206/1 (a) of CPC, the evidence obtained illegally cannot be presented at the hearing and pursuant to Article 217/2 of the CPC such evidence cannot be taken as a basis for the final decision[81].

In the Turkish legal system, there are two main categories of evidence: direct evidence, which directly demonstrates the criminal act, and indirect evidence, which shows a combination of facts to infer the fact in issue. For example, if the traces of blood, hair, and semen at the crime scene match the data of a person in the database, there is indirect evidence that does not directly show that the accused committed the alleged crime but indicates that the accused was present at the crime scene[82]. Hence, in the doctrine, AI-based systems are mostly considered indirect or circumstantial evidence.

a) AI-based evidence as a witness

Risk assessment profiling technologies show similarities with personality testimony, which does not represent material events but refer to the character of the suspect. However, in the CPC system, such a witness, who conveys his/her subjective opinion about the personality, moral values, and lifestyle of the suspect/defendant shall not be used to prove the material event[83].

The doctrine also considers AI-based systems as anonymous witnesses if the information about the software is not shared by claiming intellectual property rights or if the results of this software are difficult to be analysed by humans due to black box algorithms.

In the CPC system, the court shall resort to secret witnesses as a last resort. Moreover, the court can seek such witnesses only for certain crime types and only if there is a real danger to the life and safety of the witness or his/her relatives.

In case there is an anonymous witness statement, there must be additional safeguards provided for the defence (CPC art. 58) and the court cannot make a judgment based solely on the statement of an anonymous witness (Witness Protection Law art. 9/8). However, no norms limit the use of AI-based systems to certain types of crimes

[78] Court of Cassation, 10. CD, E.2021/2849, K.2021/5922, T. 24.05.2021 <https://lib.kazanci.com.tr/ > accessed 16 June 2021.

[79] Court of Cassation, 14. CD, E. 2020/4256, K. 2021/2398, T. 25.3.2021 <https://lib.kazanci.com.tr/ > accessed 16 June 2021.

[80] Turkish Constitutional Court, Application No: 2014/253, 9.1.2015, para. 55, 76, 77, https://www.resmigazete.gov.tr/eskiler/2015/05/20150512-12.pdf > accessed 17 July 2021.

[81] Yenisey and Nuhoğlu, 532, Fatih Birtek, *Avrupa İnsan Hakları Mahkemesi, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat* (2nd edn, Adalet Publishing 2017) 70, Şahin and Göktürk, *Ceza Muhakamesi Hukuku II*, 35.

[82] Centel and Zafer, 260, Ünver and Hakeri, 1455.

[83] Irmak Erdoğan, 220-222.

and provide additional safeguards for defence. In this case, it would be incompliant with the CPC law to accept unexplainable AI tools or keep their functioning secret due to intellectual property rights.

b) AI-based evidence as digital evidence

AI-based systems can be considered electronic (digital) evidence. Electronic evidence is not a distinct type of evidence instead it constitutes either direct or circumstantial evidence. For example, the digital data on a CCTV recording of an event is direct evidence that represents the material facts, whereas finding digital traits in a hacked computer is circumstantial evidence[84].

In the CPC there are no strict rules for evidence, thus, screenshots and prints of digital evidence can also be presented to the court[85]. Nevertheless, the Court must compare such evidence to the original source and must verify it with further evidence. The Court must also prove that the extraction process did not alter the integrity and authenticity of the source; furthermore, the extracted data was taken from the allegedly original source. Particularly the authenticity of the printed and documented data must be verified. In order to fulfil these requirements, hash values shall be generated for the digital data. In case of a mismatch in hash values, such data is not accepted as evidence[86]. On the other hand, as AI-based systems rely on big data, it is harder to verify the authenticity of their resources and their integrity.

Furthermore, since digital data mostly do not represent the main facts, but rather constitute circumstantial evidence, they do not prove per se the relationship between the act and the perpetrator. For example, even if they point out that illegal activities have been carried out through a person's computer, they do not prove if the person concerned carried them out. Therefore, without further evidence, AI-based evidence alone will not be sufficient to form a conscientious conviction that the suspect has committed the concerned act.

Since the evaluation and analysis of such evidence require technical knowledge, an expert opinion must be sought, and the digital evidence must be explained using scientific methods. There are certain procedures to be followed while transforming the obtained electronic data into evidence. In exemplary cases, the Court of Cassation states that an expert must analyse the footage before and after the crime scene and the extraction report shall be read to all parties during the hearing so that they can understand its content and challenge it. The defendant must have the opportunity to make claims regarding the originality and integrity of the digital data produced by AI-based systems[87]. If there is doubt about the reliability of the data, the court must seek another expert opinion or consider the expert opinions presented by the parties. Otherwise using such data, as a basis of the verdict constitutes a breach of the right to a reasoned decision, the principle of equality of arms, and thus the right to a fair trial.[88]

c) AI-based evidence as scientific evidence

Some doctrinal views argue that AI systems can be considered per se as scientific evidence or expert witness. In Turkey, there are no special criteria for the acceptance of scientific evidence. The only limitation to the expert opinion is that the judge cannot consult an expert regarding legal issues. However, such reports and evidence must also fulfil the conditions of being rational, authentic, and scientific. The doctrine underlines in the case of

[84] Olgun Değirmenci, 'Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği', (2014) 9 Terazi Law Journal 14.

[85] Değirmenci, 19.

[86] Murat Özbek, 'Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları' (1st International Symposium on Digital Forensics and Security (ISDFS) 2013) < https://www.bilgisayardedektifi.com/adli-bilisim-uygulamalarinda-orijinal-delil-uzerindeki-hash-sorunlari/91> accessed 17 June 2021.

[87] Court of Cassation 1. CD, T. 16.01.2012, E. 2008/10249, K. 2012/48, see Arslan, 261.

[88] Constitutional Court, Sencer Başat and Others, App. No: 2013/7800, Decision Date: 18.06.2014, para. 69-72, <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/7800> accessed 30 July 2021.

using the black-box algorithms, it will be difficult to test the validity of such tools and the robustness of the data on which they are based.

4. Conclusion

In conclusion, there is no special regulation regarding the validity and acceptability and assessment of AI-based systems and their use as evidence. Regulations on digital evidence in the Turkish legal system, primarily CPC art. 134 and the following articles focus on the measures of computer search, technical surveillance, and interception of communications. However, there are no specific regulations on newly emerging measures such as the use of big data and their analysis by data mining. For this reason, for the measures including personal data processing, the PDPC provisions shall be taken into consideration. However, since the PDPC excludes judicial proceedings as well as data collection by police for national security and public order, there is an urgent need for special regulation in this area.

Considering the intrusiveness of the AI-based systems, using such tools cannot be considered within the framework of regular tasks of the police force. Thus, the doctrine insists on establishing specific laws, which foresee their limits. Particularly for safeguarding the authenticity of AI-based systems, there is a need for mandatory special procedures. Furthermore, there is a need for exclusionary rules for the use of risk analysis profiling tools in interim and final decisions in criminal proceedings, as they single out the future perpetrators but do not constitute evidence relevant to the facts of the case.