XXIst International Congress of Penal Law – ”Artificial Intelligence and Criminal Justice”.

Section III. Predictive Policing and Predictive Justice, and Evidence.

Finnish National Report

By Sofia SÖDERHOLM (Part I), Raimo LAHTI and Lauri LAHTI (Part II), and Juhana RIEKKINEN (Part III).

Part I. Predictive policing in Finland

Written by Sofia Söderholm[*]

1 National practices

Predictive policing in Finland is still in its infancy and there is no country-specific definition of the concept. In this report, the concept of predictive policing refers to the much-cited definition by Perry et al.: ‘Predictive policing is the application of analytical techniques – particularly quantitative techniques – to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions.’[1] In addition, essential elements of predictive policing technology are exploitation of big data[2] and AI. Hence, any AI-based solutions used for crime prevention by private companies, such as banks, have been excluded from the scope of this report.

The central administrative authority of the Finnish police, the National Police Board of Finland, has not announced the usage of AI-based predictive policing systems by either the local police departments or the National Bureau of Investigation (‘NBI’).[3]

[*] Sofia Söderholm is Doctoral Researcher, University of Helsinki, Faculty of Law, Finland (sofia.soderholm@helsinki.fi).

[1] Walter L Perry, Brian McInnis, Carter C Price, Susan C Smith and John S Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (1st edn, RAND Corporation 2013) 30.

[2] E.g., Elizabeth E. Joh, ‘Feeding the Machine: Policing, Crime Data, & Algorithms’ (2017) 26 *Wm. & Mary Bill Rts. J.* 287.

[3] Ministry of the Interior, *Finland’s Strategy on Preventive Police Work 2019–2023* (Publications of the Ministry of the Interior 2019:11) 37: ‘Major investments are being made in the development of automation and artificial intelligence in Finland and other countries and using such applications in different tasks is still in its initial stages.’

However, as a member of the European Union, Finland has implemented the Passenger Name Record ('PNR') Directive (EU) 2016/681[4] in the form of the Act on the use of Passenger Name Record data for the prevention of terrorist offences and serious crime (657/2019, 'PNR Act').[5] The PNR Act creates an obligation for air carriers to transfer PNR data to the Passenger Information Unit ('PIU'), which in Finland is formed by the Police, the Finnish Customs, and the Finnish Border Guard. The aim of analysing PNR data is to prevent, detect, investigate and prosecute terrorist offences and serious crime that are explicitly defined in the Criminal Code of Finland (39/1889) and the Annex II of the Directive. Analysing PNR data to identify people who were not suspected before and making them a target of policing activities based on the analysis provided by the PNR system, could be considered as a form of predictive policing.[6]

Limited information is available on the workings of the PNR system in Finland. The preparatory work of the Act is the only source to assess the nature of the system. According to the Government Proposal on the PNR Act, the PNR data should be used for the creation of threat assessments and risk profiles, which guides the authorities to target their activities towards the passengers that fit the profiles.[7] In order to identify 'the unknown suspects' the PIU has pre-defined evaluation criteria to which the PNR data is compared to. The proposal also suggests analysing customary travel models and the activities that differ from them. The proposal

<https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161343/SM_11_19_Strategy%20on%20preventive%20police%20work.pdf?sequence=1&isAllowed=y> accessed 27 December 2021. See also Vesa Syngelmä, 'Ennustamisteknologioiden hyödyntämismahdollisuudet osana ennakoivaa poliisitoimintaa' (Master's thesis, Tampere University, 2021) <https://trepo.tuni.fi/handle/10024/130523> accessed 27 December 2021 (concluding that predictive technologies are not currently in use in Finland).

[4] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[5] Finnish parliamentary acts are officially available in Finnish and Swedish. A collection of unofficial translations to other languages is available at Finlex, Translations of Finnish acts and decrees <https://www.finlex.fi/en/laki/kaannokset/> accessed 28 March 2022.

[6] European data protection supervisor, Request for an Opinion by the European Parliament, draft EU-Canada PNR agreement (Opinion 1/15) Hearing of 5 April 2016 Pleading notes of the European Data Protection Supervisor (EDPS) <https://edps.europa.eu/sites/default/files/publication/16-04-05_pleading_canada_pnr_en.pdf> accessed 27 December 2021; Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards. Executive summary. Council of Europe. The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-Pd) Strasbourg, 15 June 2015. <https://rm.coe.int/16806b1761> accessed 27 December 2021.

[7] Government Proposal on the PNR legislation (HE 55/2018 vp) 18 (law drafting documents are only available in Finnish and Swedish).

provides examples of suspicious activities: a cash payment for a last-minute booking or travelling without luggage.[8]

During the legislative procedure, the national data protection authority characterised the PNR system as 'an AI type solution' in its statements to the Parliament's Constitutional Committee and Administrative Committee.[9] The Administration Committee stated that by virtue of Section 24(1)(5) of the Act on the Openness of Government Activities (621/1999, 'Openness Act'), more detailed information on methods used in the analysis of PNR data is classified.[10] However, it should be noted that the Court of Justice of the European Union in its judgement on the PNR directive from summer 2022 stated that the wording of the directive precludes the use of self-learning AI systems in the evaluation process and especially when determining the evaluation criteria.[11] Thus, at least after the judgement it is safe to say that self-learning AI should not be used in the aforementioned context.

Although the usage of predictive policing in Finland is still in its infancy, there are several indications that the Finnish police force is interested in using AI in its crime prevention analysis. The role of *intelligence-led policing* (operating on knowledge analysed from criminal intelligence) has already been emphasised on many occasions by the police.[12] Based on recent reports provided by the police, using AI systems seems to be the goal and next step of the digitalisation of police operations. According to the National Police Commissioner, who is the head of the National Police Board of Finland, the Board is currently exploring the future technology the

[8] *ibid* 27.

[9] The expert opinion of the Data Protection Ombudsman for the Constitutional Law Committee on 10 September 2018 <https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-203144.pdf>; and the opinion of the senior officer for the Administrative Committee on 7 January 2019 <https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2019-AK-235519.pdf> (both accessed 29 December 2021).

[10] The Report of the Administrative Committee (HaVM 42/2018 vp). Section 24(1)(5) of the Openness Act: 'Unless specifically provided otherwise, the following official documents shall be secret: the documents containing information on the tactical and technical methods and plans of the police, the Border Guard, the Customs, the prison authorities and the Finnish Immigration Service if the access would compromise the prevention and solving of crime, the maintenance of public order and safety, the order of penal institutions, or the reliability of an assessment on a foreigner done by the Immigration Service.'

[11] Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministres* [2022] para 194.

[12] Mika Sutela, 'Tiedon, analyysin ja analytiikan hyödyntämisen tarve poliisissa – ilmeinen ja suuri?' (Official blog of the police, 15 September 2019) <https://poliisi.fi/blogi/-/blogs/tiedon-analyysin-ja-analytiikan-hyodyntamisen-tarve-poliisissa-ilmeinen-ja-suuri-> accessed 29 December 2021; The expert opinion of the National Bureau of Investigation on data processing in the police on 10 January 2019 <https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2019-AK-236903.pdf> accessed 29 December 2021.

police would be using in 2030.[13] However, so far, no material on the project has been made available to the public.

In 2018, the final report of the study project on the Status of Crime-prevention in Finland found the role of efficient IT systems in the analysis of data for crime prevention to be highly important. According to the report, the target level for storing, processing and aggregating data of the Finnish police should be at the same level as that of the Europol.[14] In addition, the usage of AI and big data in the analysis is emphasised.[15] The report states that the elements of big data and AI should be implemented in processing large datasets in *Vitja,* the police information system. It should be noted that *Vitja* includes *Poti,* the new intelligence system of the police and it is also used by other law enforcement authorities such as the Finnish Customs and the Finnish Border Guard.[16] Finally, the report suggests that the police should collect and analyse data on place, time, and results of breathalysing and use statistical analysis to predict where police officers should patrol to increase the likelihood of catching drivers with a blood alcohol level that exceeds the legal limit. In 2021, the National Police Board of Finland confirmed that data of this type is being collected and analysed to target policing activities, but more detailed information on this activity is not available.[17]

The Financial Intelligence Unit of the NBI undertook a project that explored the opportunities arising from the use of AI in the fight against money laundering and terrorist financing. The project was called *RANKKA*, and took place between 2020 and 2021.[18] According to the annual report of the Unit in 2020, the aim of the project

[13] Poliisiylijohtaja Seppo Kolehmainen muistutti poliisien valatilaisuudessa: Poliisin pysyttävä mukana muutoksessa <https://poliisi.fi/-/poliisiylijohtaja-seppo-kolehmainen-muistutti-poliisien-valatilaisuudessa-poliisin-pysyttava-mukana-muutoksessa> accessed 29 December 2021.

[14] Europol is the EU's law enforcement agency. The organisation and functioning of the agency are laid down in Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

[15] Rikostorjunnan tila -selvityshanke and Tero Kurenmaa, *Rikostorjunnan tila -selvityshankkeen loppuraportti* (The publication series of the National Police Board of Finland 1/2018) 45 <https://poliisi.fi/julkaisut/-/asset_publisher/Ga8MkKWl5ss3/content/rikostorjunnan-tila-selvityshankkeen-loppuraportti?_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_Ga8MkKWl5ss3_assetEntryId=43809202> accessed 29 December 2021.

[16] Poliisi panostaa rikosten ehkäisemiseen ja paljastamiseen <https://poliisi.fi/-/poliisi-panostaa-rikosten-ehkaisemiseen-ja-paljastamiseen> accessed 27 December 2021.

[17] Letter to the author on 17 November 2021 (POL-2021-127171). The opportunities of AI in data analysis are seen also in the final report of the study project on the status of monitoring and emergency activities of the police: Valvonta- ja hälytystoiminnan selvityshanke and Arto Karnaranta, *Valvonta- ja hälytystoiminnan tila -selvityshankkeen loppuraportti* (The publication series of the National Police Board of Finland 3/2019).

[18] Projects and top-up funding of the Police are available at <https://poliisi.fi/en/projects-and-complementary-funding>.

was 'to produce a study of technological solutions related to artificial intelligence and digitalisation in general that are applicable in the context prevention, detection and investigation of money laundering.'[19] Furthermore, the Ministry of Finance has set up a working group to develop digital tools to support national risk assessment work on money laundering and terrorist financing. The term of office of the working group is 13.10.2021–30.6.2024. According to the project description, 'the aim is to create two different tools to support national money laundering and terrorist financing risk assessment work: a digital data platform and a risk assessment tool for processing quantitative and qualitative data.'[20]

Finally, other law enforcement organisations, namely the Finnish Border Guard and the National Enforcement Authority Finland, have started to consider using AI in their activities. According to the Finnish Border Guard's 2020 annual report, it has initiated a development project of surveillance techniques called *RAVAKE*. The aims of the project are to modernise the surveillance systems of land borders and sea areas, and the solutions used in maintaining and managing situational pictures. In the second phase of the project (2022–2024) the aim is to replace the Border Guard Information System by introducing a centralised data warehouse, which is to be used for management, analysis, and exploitation of data. In addition, the opportunities created by AI are to be exploited effectively.[21] The National Enforcement Authority Finland has undertaken two projects called *RATKE* and *Harmaa*, the aim of which is to increase the efficiency of data acquisition, data processing and decision-making necessary for enforcement through robotics and data analytics.[22] With *RATKE*, the plan is to automate the enforcement process by automatically providing bailiffs with proposals for decisions and measures. The aim of the *Harmaa* project is to use data analytics to facilitate the identification of cases requiring special measures from the masses of cases and thus to target better investigative activities to find assets and income concealed by actors in the grey economy.

[19] *The Annual report of the Financial Intelligence Unit* (2020) 39 <https://poliisi.fi/documents/25235045/67733116/2020-Rahanpesun-selvittelykeskus-vuosikertomus-2020.pdf/e340331f-f04c-7eec-2756-111628ae368a/2020-Rahanpesun-selvittelykeskus-vuosikertomus-2020.pdf?t=1617010848853> accessed 29 December 2021.

[20] The project website <https://vm.fi/hanke?tunnus=VM141:00/2021> accessed 29 December 2021.

[21] *The Annual report of the Border Guard* (2020) 15 <https://raja.fi/documents/44957406/64377821/Tilinp%C3%A4%C3%A4t%C3%B6s_2020.pdf/d7f4c8ec-92ce-fe60-0825-b45e209fd4c1/Tilinp%C3%A4%C3%A4t%C3%B6s_2020.pdf?t=1615290408994> accessed 29 December 2021.

[22] Ulosottolaitoksen hankkeet RATKE ja Harmaa hyödyntävät uutta teknologiaa (21 December 2021) <https://ulosottolaitos.fi/fi/index/ulosottolaitos/ajankohtaista/verkkouutisetjatiedotteet/uutiset2021/ulosottolaitoksenhankkeetratkejaharmaahyodyntavatuuttateknologiaa.html> accessed 29 December 2021.

Public debate on predictive policing in Finland has been almost non-existent and academic research is still scarce.[23] This is most likely because predictive policing is not currently used in Finland in the prevention of crime, other than PNR analytics. More attention has been given to the willingness of the Finnish Security and Intelligence Service to widen its intelligence powers,[24] and the willingness of the NBI to widen the powers of the police to conduct intelligence without tangible suspicion of a crime.[25]

2 Normative framework

In Finland, there are no national legal rules, other normative instruments, or soft law sources specifically concerning AI-based systems for predictive policing. As regards case law on predictive policing, since predictive policing is not currently used in Finland, no decisions by judicial authorities, regulators, or courts have been issued.[26]

Although not specifically enacted for AI-based predictive policing, there is other national legislation that is worth noting to gain an understanding of Finland's national normative framework regarding policing in general, which would still be the starting point in the case the police would implement AI-based predictive policing systems. Firstly, the regulation on processing of personal data is essential for systems such as AI-based predictive policing. Secondly, since the police exercise public power, the requirements set for public authorities and their employees as government officials form another significant legislative framework that needs to be considered when using AI systems in public administration. Section 2(3) of the Constitution of Finland (731/1999) specifically states the principle of legality in public administration: The exercise of public power must be based on the law. The law must be strictly observed in all public activities.

Rights and obligations concerning the processing of personal data are provided at the national level in the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018, 'Act on the Processing of Personal Data in Criminal Matters'), which implements the Law

[23] Sofia Söderholm, *Potentiaalisen rikoksentekijän asema ja oikeus syyttömyysolettamaan ennakoivassa poliisitoiminnassa* (Legal Tech Lab 2020) <https://helda.helsinki.fi/handle/10138/331782> accessed 29 December 2021; and Syngelmä (n 3).

[24] Tuomo Pietiläinen, 'Supo haluaa lisää oikeuksia tiedustella salaa – laillisuusvalvojat täsmentäisivät nykyisiä tiedustelulakeja' *Helsingin Sanomat* (23 November 2021) <https://www.hs.fi/politiikka/art-2000008422934.html> accessed 29 December 2021.

[25] Tuomo Pietiläinen, 'Poliisi haluaa puhelinkuuntelun ja muita salaisia keinoja käyttöön ilman rikosepäilyä – sisäministeriö aloittaa esiselvityksen' *Helsingin Sanomat* (18 November 2021) <https://www.hs.fi/politiikka/art-2000008414156.html> accessed 29 December 2021.

[26] As Finland is a member of the European Union, the upcoming Artificial Intelligence Act will be applicable in Finland once in force.

Enforcement Directive ((EU) 2016/680, 'LED').[27] According to Section 1 of the Act, it applies *inter alia* to the processing of personal data by competent authorities in the context of preventing, detecting or investigating criminal offences or referring them for consideration of charges. The Act contains provisions on the principles relating to processing of personal data, obligations of the data controller and processor, rights of data subjects, data security, data protection officer, transfers of personal data to third countries and international organisations, supervisory authority, legal protection of individuals, compensation for damages and penal provisions. Additionally, the Act on the Processing of Personal Data by the Police (616/2019) complements its provisions.[28]

When it comes to the transparency of both the technological functioning of automated decision-making systems used by authorities and the transparency of policing practices, the applicable provisions are provided by the Openness Act,[29] which promotes and makes operational the principle of openness and the fundamental right to obtain information from authorities.[30]

In Finland, the transparency of the functioning of an IT system used in public administration has been approached as the transparency of the system's source code. The starting point is currently the interpretation that the code is considered to be an official document.[31] However, as mentioned above, Section 24(1) of the Openness

[27] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[28] The Border Guard, the Customs and the Defence Forces have their own *lex specialis* data processing acts: Act on the Processing of Personal Data by the Border Guard (639/2019), Act on the Processing of Personal Data by the Customs (650/2019) and Act on the Processing of Personal Data by the Defence Forces (332/2019).

[29] Further, the Act on Information Management in Public Administration (906/2019) contains provisions on management and processing of datasets of authorities to implement the principle of openness.

[30] Constitution of Finland, s 12(2): 'Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings.' Openness Act, s 3: 'The objectives of the right of access and the duties of the authorities provided in this Act are to promote openness and good practice on information management in government, and to provide private individuals and corporations with an opportunity to monitor the exercise of public authority and the use of public re- sources, to freely form an opinion, to influence the exercise of public authority, and to protect their rights and interests.'

[31] Niklas Vainio, Valpuri Tarkka and Tanja Jaatinen, *Arviomuistio hallinnon automaattiseen päätöksentekoon liittyvistä yleislainsäädännön sääntelytarpeista* (Publications of the Ministry of Justice 2020:14) 44 <https://api.hankeikkuna.fi/asiakirjat/ff3444f4-24c9-4ee8-8c9d-7bc581c0021a/e034bf5c-e2bd-4245-a626-9b679b2144ff/LAUSUNTOPYYNTO_20210609083824.PDF> accessed 29 December 2021. More on algorithmic transparency: Jenni Hakkarainen, Riikka Koulu and Kalle Markkanen, 'Läpinäkyvät algoritmit? lähdekoodin julkisuus ja laillisuuskontrolli hallinnon digitalisaatiossa' Edilex 2020/18 <https://www.edilex.fi/artikkelit/21042.pdf> accessed 29 December 2021; Riikka Koulu, Beata

Act contains provisions on secret official documents. These include documents containing information on the tactical and technical plans and methods of the police. The provision was interpreted in the context of PNR legislation in a way that classified the information on the PNR system source code.[32] Thus, it is likely that the Act would be interpreted in the same way in the context of AI-based systems for predictive policing. In any case, the openness of the system source code does not guarantee the actual transparency of the system's workings: first, it would not necessarily be enough to reveal the working of the AI system; second, it is unlikely that an ordinary citizen would understand the meaning of the code.[33] When it comes to policing practices in general, the provisions of Chapter 5 of the Openness Act on the duty of an authority to promote access to information are essential. Section 20 of the Act imposes obligations on authorities to produce and disseminate information, which includes producing publications on their activities.[34]

As the police officers are government officials, they work under official accountability. Like the principle of openness, official accountability has been enacted at the constitutional level. According to Section 118 of the Constitution, an official is responsible for the lawfulness of his or her official actions. In addition, an individual who has suffered an infringement or damage due to an unlawful act or omission by an official, has the right to seek imposition of a punishment on the relevant official and claim damages for the harm suffered.

Thus, police officers in Finland are obliged to comply with the legislation that applies to all government officials, e.g., the provisions of the Openness Act, but also the special duties of police officers in the Police Act (872/2011), the Coercive Measures Act (806/2011), the Criminal Investigation Act (805/2011) and all the other legislation applicable to policing. The Police Act contains provisions on general powers of police officers but the enacted powers can also be found elsewhere in the legislation. Violation of official duties is punishable in accordance with the Criminal Code of Finland and the liability for damages in accordance with the Tort Liability Act (412/1974).

Mäihäniemi, Vesa Kyyrönen, Jenni Hakkarainen and Kalle Markkanen, *Algoritmi päätöksentekijänä?: Tekoälyn hyödyntämisen mahdollisuudet ja haasteet kansallisessa sääntely-ympäristössä* (Government's publication series 2019:44) 122–123 <https://julkaisut.valtioneuvosto.fi/handle/10024/161700> accessed 29 December 2021; Tomi Voutilainen, *ICT-oikeus sähköisessä hallinnossa* (Edita 2009) 224; Hanne Hirvonen, 'Automatisoitu päätöksenteko julkisella sektorilla' (2018) *Oikeus* 47(3) 302–310, 306–308.

[32] See note 10.

[33] See Joshua A Kroll, Joanna Huey, Solon Barocas, Edward W Felten, Joel R Reidenberg, David G Robinson and Harlan Yu, 'Accountable Algorithms' (2017) 165 *University of Pennsylvania Law Review* 633, 638. <https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3> accessed 29 December 2021.

[34] For instance, The National Police Board has its own series for publishing studies, reports and working group reports. These publications are available at <https://poliisi.fi/en/publications>.

Although Chapter 1, Section 1 of the Police Act defines the duties of the police *inter alia* to secure the rule of law, maintain public order and security, and prevent, detect and investigate crimes, the policing activities must always be based on a specific provision of law when an officer intervenes in an individual's rights. This clarification has been stated in the Government Proposal on the Police Act and before that in the decisions of the supreme overseers of legality, that is the Parliamentary Ombudsman and the Chancellor of Justice.[35] Whether a police officer would intervene in the activities of individuals based on prediction provided by a predictive policing system, the officer would still need to have a specifically enacted power to do so. Additionally, the police officers have the obligation to announce the basis of their actions to the individual against whom the action has been taken.[36]

Currently, the Police Act does contain a provision on preventing an offence or disturbance based on the likelihood of a person's future behaviour. According to Chapter 2, Section 10(1) of the Police Act,

> A Police officer has the right to remove a person from a scene if there are reasonable grounds to believe on the basis of the person's threats or other behaviour, or it is likely on the basis of the person's previous behaviour, that he or she would commit an offence against life, health, liberty, home or property, or would cause a considerable disturbance or pose an immediate danger to public order or security.

In addition, according to subsection 2, 'A person may be apprehended if his or her removal is likely to be an inadequate measure and the offence cannot otherwise be prevented or the disturbance or danger otherwise removed.' The period of apprehension can last a maximum 24 hours. The Government Proposal from the year 2010 does not refer to using algorithmic tools when conducting this assessment. It seems clear that the wording of the Section and the Proposal refer more to an onsite evaluation by a police officer.[37] Thus, it can be argued that this provision would not be an adequate legal basis for the police to act based on a predictive policing prediction.

3 General principles of law

Respecting fundamental rights, such as rights to equality, privacy, and liberty and security are all regulated at the constitutional level. Furthermore, a significant constitutional right, the right to legal protection enacted in Section 21 of the

[35] Government Proposal on the Police Act (HE 224/2010 vp) 71; Decision of the Deputy-Ombudsman of the Parliament (EOA 1634/4/01) 18 December 2003 <https://www.oikeusasiamies.fi/r/fi/ratkaisut/-/eoar/1634/2001> accessed 29 December 2021.

[36] Police Act, c 1 s 7.

[37] Government Proposal on the Police Act (HE 224/2010 vp) 79.

Constitution constitutes a right to an effective remedy, fair trial, and good administration and is always relevant when exercising public power.[38] According to Section 22 of the Constitution, public authorities must guarantee the observance of basic rights and liberties and human rights. Thus, all public officials, including police officers, are obliged by the Constitution to guarantee the fulfilment of these rights in their activities.

Although there has been no discussion regarding the protection of fundamental rights specifically in the context of AI systems used for predictive policing, the question of equality in the context of automated decision-making in the private sector has been assessed in Finland by the National Non-Discrimination and Equality Tribunal in the context of assessing creditworthiness.[39] Section 6(2) of the Constitution provides the foundation for the right to equality. It states that without an acceptable reason, no one should be treated differently from other people on the grounds of sex, age, origin, language, religion, conviction, opinion, health, disability or other reason that concerns his or her person.

The Act on the Processing of Personal Data in Criminal Matters also contains provisions on discrimination. Section 11(3) of the Act prohibits profiling that results in discrimination against natural persons according to special categories of personal data.[40] Profiling means any automated processing of personal data consisting of the use of personal data to evaluate personal aspects relating to a natural person. These aspects can be about personal preferences, interests, reliability, behaviour, location or movements.[41] According to the related Government Proposal, this provision

[38] Constitution of Finland, s 21: '(1) Everyone has the right to have their case dealt with appropriately and without undue delay by a legally competent court of law or other authority, as well as to have a decision pertaining to his or her rights or obligations reviewed by a court of law or other independent organ for the administration of justice. (2) Provisions concerning the publicity of proceedings, the right to be heard, the right to receive a reasoned decision and the right of appeal, as well as the other guarantees of a fair trial and good governance shall be laid down by an Act.'

[39] Decision register number 216/2017, date of issue 21 March 2018. Short English summary available at <https://www.yvtltk.fi/en/index/opinionsanddecisions/decisions.html> accessed 29 December 2021. The whole decision is available only in Finnish: <https://www.yvtltk.fi/material/attachments/ytaltk/tapausselosteet/2SVkNzOWF/YVTltk-tapausseloste-_21.3.2018-luotto-moniperusteinen_syrjinta-S._L.pdf> accessed 29 December 2021. Generally, on the Tribunal, see <https://www.yvtltk.fi/en/index.html> accessed 26 December 2021.

[40] Act on the Processing of Personal Data in Criminal Matters, s 11(1): 'Special categories are personal data revealing ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or a natural person's sex life or sexual orientation.'

[41] Government Proposal on processing of personal data in Criminal Matters and in Connection with Maintaining National Security (HE 31/2018 vp) 37.

prohibits algorithm-based profiling that leads to persons belonging to a specific ethnic group being subject to stricter surveillance than others.[42]

When it comes to the right to privacy, Section 10 of the Constitution provides the foundation of the right to privacy but the aforementioned Act on the Processing of Personal Data in Criminal Matters and the Act on the Processing of Personal Data by the Police provide the provisions on the lawful processing of personal data in the context of preventing and detecting criminal offences. For instance, Section 13 of the Act on the Processing of Personal Data in Criminal Matters regulates automated individual decision-making: Unless otherwise provided by law, a decision will not be based solely on automated processing of personal data if the decision produces adverse legal effects concerning the data subject or otherwise significantly affects him or her. Since no predictive policing systems are currently used in Finland, the adequacy of the level of protection of privacy provided by the data protection legislation is difficult to assess.

The right to liberty and security has been enacted in Section 7 of the Constitution. According to Section 7(1) everyone has the right to life, personal liberty, integrity and security. In Section 7(3), the personal integrity of the individual must not be violated, nor should anyone be deprived of liberty arbitrarily or without a reason prescribed in an Act. As stated above, whether police officers would act based on predictive policing prediction, they still must have specific powers enacted by law for their activities. In addition to providing powers, the Police Act also contains principles that restrain activities of the police officers. Chapter 1 of this Act contains general provisions on the obligation to respect fundamental and human rights (Section 2), the principle of proportionality (Section 3),[43] the principle of minimum intervention (Section 4),[44] the principle of intended purpose (Section 5),[45] and postponing actions and refraining from taking actions (Section 9).[46]

Lastly, it should be noted that predictive policing could also be used, at least in theory, for the purposes to detect crime that has already happened. This possibility was also included in the predictive policing definition by Perry et al.[47] However, in Finland the reactive usage of predictive policing could be problematic from the

[42] *ibid* 42.

[43] Police action shall be reasonable and proportionate with regard to the importance, danger and urgency of the duty; the objective sought; the behaviour, age, health and other specifics of the person targeted by the action; and other factors influencing the overall assessment of the situation.

[44] The police shall not take action that infringes anyone's rights or causes anyone harm or inconvenience more than is necessary to carry out their duty.

[45] The police may exercise their powers only for the purposes provided by law.

[46] Police Act, c 1 s 9(1): 'The police have the right to refrain from taking an action if completion of the action could lead to an unreasonable conclusion compared with the outcome sought.'

[47] Perry et al (n 1).

legislative division of labour point of view and its impact on individuals' procedural rights.[48] Simply put, pre-crime police work is enacted in the Police Act and post-crime work in the Criminal Investigation Act and Coercive Measures Act. This also divides individuals into either non-suspects (if no crime has been committed) or suspects (if a crime has been committed), and further impacts what kinds of rights individuals have in the process. Criminal procedural rights, e.g., the right to be presumed innocent apply only after a criminal investigation has started.

The linear logic of the Criminal Investigations Act is that the police need to base their investigation on suspicion and not vice-versa. According to Chapter 1, Section 3(1) of the Criminal Investigation Act, the criminal investigation authority shall conduct an investigation when, on the basis of a report made to it or otherwise, there is reason to suspect that an offence has been committed. Thus, there needs to be a tangible act, which is suspected to be a crime before the police can start to investigate it. Before any tangible act has been observed, the applicable provisions come from the Police Act. As already noted above, according to the Police Act, one of the tasks of the police is to detect crime.[49] Using systematic screening of people to detect crime that might have been conducted could make the distinction between pre- and post-crime measures blurred if individuals would be targeted with algorithmic investigative measures without suspicion of a crime occurring first. However, as also stated, the police always need to have a specific provision that allows officers to intervene in individuals' rights. Hence, it can be argued that using predictive policing for reactive purposes would also require enacting it on the legislative level.

Part II. Predictive justice

Written by Raimo Lahti and Lauri Lahti[1]

[48] The procedural legality of predictive policing has been touched upon in the reporter's master's thesis from the Faculty of Law, University of Helsinki. See Söderholm (n 23).

[49] Police Act, c 1 s 1.

[1] Raimo Lahti is LL.D. and Professor (emeritus) of Criminal Law, University of Helsinki, Faculty of Law, Finland (raimo.lahti@helsinki.fi), and Lauri Lahti is Dr. Sc. (Tech.) and Postdoctoral Researcher at the Department of Computer Science, Aalto University School of Science, Finland (lauri.lahti@aalto.fi). Raimo Lahti has written the sub-chapter 1 (Predictive justice in Finnish legal system) and Lauri Lahti has written the sub-chapter 2 (Challenges of developing ethical artificial intelligence for identifying personal needs and risks).

1. Predictive justice in Finnish legal system

The main emphasis of the Finnish National Report concerning Section III is laid on the part I (Predictive policing) and the part III (Evidence law).[2] Therefore, the following presentation on the part II (predictive justice) is a short one and not following in detail the questionnaire by Juliette Lelieur.

The reason for the shortness is the fact that the role of artificial intelligence (AI) has so far been very limited or even non-existing in the Finnish criminal justice system. A similar parsimony is true also in relation to the ideology in which preventive justice and, in particular, preventive sentencing, are not in the fore front of the dominant criminal policy. Preventive justice is a wider concept, including i.a. preventive offences and counterterrorism laws, while preventive sentencing is concentrating on risk assessment in the criminal justice process and prevention of the dangerous.[3] There are examples of preventive justice and, to a limited extent, of preventive sentencing.

In a recent article I have described the development of life imprisonment and other long-term imprisonments in the Finnish criminal justice system in the 1970s:[4]

> "Among the most important results of the criticism during the 1970s were legislative reforms in Scandinavia which either abolished the special sanctions which were imposed for an indeterminate period or at least clearly limited their scope of application. Such kinds of sanctions were in the Nordic countries, as everywhere in the Western countries, introduced in the spirit of the dominant treatment or incapacitation ideology of the first half of the 20th century.
>
> The model for the individualization of the sanctions was primarily applied to special categories of offenders (as to dangerous offenders and/or mentally disordered offenders). It should be noted that in the Nordic countries the most common penal sanction imposed by the courts has traditionally been the fine (both Finland and Sweden

[2] See the partial reports of *Sofia Söderholm* (Part I. Predictive policing in Finland) and *Juhana Riekkinen* (Part III. Evidence law).

[3] See, e.g., Andrew Ashworth and Lucia Zedner, *Preventive Justice*, Oxford University Press, Oxford 2014; Jan W. de Keijser, Julian V. Roberts and Jesper Ryberg (eds.), *Predictive Sentencing. Normative and Empirical Perspectives*, Hart Publishing, Oxford 2019.

[4] Raimo Lahti, Life Imprisonment and Other Long-Term Sentences in the Finnish Criminal Justice System: Fluctuations in Penal Poliy, in Khalid Ghanayim and Yuval Shany (eds.), *The Quest for Core Values in the Application of Legal Norms. Essays in Honor of Mordechai Kremnitzer*, Springer, Cham 2021, pp. 201-217, at 204-205.

> make extensive use of the day-fine system). Furthermore, the sentences of imprisonment imposed in these countries are, by international standards, short: for common crime such sentences are usually at most a few months in length.
>
> It should also be noticed that the influence of the treatment or incapacitation ideology differed from one Scandinavian country to another. This influence was traditionally profound in Denmark and Sweden but relatively weak in Finland. For example, Finland never followed the Scandinavian model in the matter of establishing a special treatment institution for psychopathic offenders; such a Danish institution under the leadership of the psychiatrist Georg K. Stürup was internationally known.
>
> The most obvious and immediate effects of the described criticism against coercive treatment on legislative reforms in Finland consisted of the abolition of compulsory castration (in 1970) and an essential narrowing down of the conditions for the indeterminate incarceration of dangerous recidivists (in 1971)."

Nevertheless, the fluctuation in the climate of penal policy took place at the beginning of the 21st century: The reform work led to the new Prison Act (767/2005), which adjusted the prison law to fulfil the requirements of the new Finnish Constitution (731/1999) and human rights obligations as well as with the strengthened legal safeguards and transparency of prison administration. This reform also included the enactment of new provisions on the release of prisoners on parole (780/2005), and as a novelty, a regular release of prisoners serving a life sentence on parole by the decision of Helsinki Court of Appeals (781/2005).

The legislation on incarceration concerning dangerous offenders (preventive detention) was repealed and replaced by new provisions on prisoners serving their entire sentence in prison due to their dangerousness to the life or health of others as manifested in their criminal activity (780/2005). The application of these provisions presupposes multidisciplinary risk assessments of the offender, and it is a manifestation of the aim of incapacitation. As Tapio Lappi-Seppälä points out, there have been some indication of a return of risk-based, predictive sentencing, which was ruled out by the 1970s sanction reforms. However, the overall use of these risk-based measures has remained low in the Nordic countries.[5]

When the scope of preventive justice is expanding in many ways in the name of public protection and security, we scholars should be prepared to critically assess the foundations for this development. Michael Tonry summarizes the most recent research results by saying that "[p]redictive sentencing can thus be justified neither empirically nor morally", although "prevention concerns and prevailing emotionalism may make the elimination of preventive sentencing unachievable".[6]

In a critical evaluation of the described reforms on the long-term sentences, various values and interests of criminal policy as well as basic and human rights considerations must be balanced. In her recent doctoral thesis on the subject (2017) Annakaisa Pohjola summarizes that "evaluating the dangerousness of offenders is complicated, as it is necessary to weigh against each other the concrete elements of dangerousness, formal and substantive justice along the overall legal safeguards of the judicial system"[7].In a similar way, a recent study by a team of researchers from the University of Eastern Finland (2021) concluded that the timing of the assessment of the risk of danger should be reviewed, the consistency of the terminology and the assessments should be increased. and the quality of the assessments should be improved[8].

Although predictive sentencing is widely used, the accuracy of risk assessment instruments remains problematic, as the editors of the article collection "Preventive Sentencing" express their concern.[9] Two developments in relation t the technology of risk prediction, seem to Esther FJC van Ginneken be noteworthy: machine learning algorithms and neurological assessments. As to machine learning techniques, they have enabled the search for instruments that can detect more complex pattern than traditional regression-based instruments, although there is not

[5] T. Lappi-Seppälä, Life Imprisonment and Related Institutions in the Nordic Countries, in D. van Zyl Smit & C. Appleton (Eds.), *Life Imprisonment and Human Rights* (Hart Publishing, Oxford 2016), pp. 461-505, at 500.

6 M. Tonry, Sentencing and Prediction. Old Wine in Old Bottles, in *Predictive Sentencing. Normative and Empirical Perspectives* (*supra* note 3), pp. 269–298, at 290–291.

[7] A. Pohjola, *Vaarallinen rikoksentekijä?* [Dangerous Offender?] (A Study on Offender Risk Assessment within the Finnish Penal System). (Finnish Lawyers' Association, Helsinki 2017), *passim*, esp. pp. 409–411 (Abstract).

[8] Matti Tolvanen *et al.*, *Vaarallisuuden ja väkivaltariskin arvioiminen* [Assessment of the Risk of Danger and Violence]- Publications of the Government's analysis, assessment and research activities 2021:70, Helsinki 2021 (Abstract).

[9] J. De Keijser *et al.*, Introduction, in*: Predictive Sentencing. Normative and Empirical Perspectives (supra* note 3), pp. 1-8, at 2.

yet consensus on whether machine learning techniques are more accurate at predicting recidivism.[10]

In Finland, these new risk assessment instruments are not yet in use. It is predictable that these instruments reach the Finnish forensic expertise and juridical practice as helping methods, too. Then role of personal decision making will be retained. The normative framework and general principles of law are *mutatis mutandis* also then applicable.[11]

2. Challenges of developing ethical artificial intelligence for identifying personal needs and risks[12]

The questionnaire of Juliette Lelieur asks the national reporters to illustrate possible existing or emerging national solutions of artificial intelligence (AI) that can be used as risk assessment tools and thus can be applicable also in preventive justice. Therefore this subchapter offers an examination of two major Finnish artificial intelligence programs, which are Hyteairo program[13] and AuroraAI program[14], and in relation to them discusses about various challenges noted in respect to developing ethical artificial intelligence for identifying personal needs and risks. The evaluation about the use and impact of artificial intelligence in public services in Finland can be contrasted with the European-level development by findings of the report of Misuraca and Van Noordt (2020)[15]. Officially Hyteairo program and AuroraAI

[10] E. van Ginneken, The Use of Risk Assessment in Sentencing, in: *Predictive Sentencing. Normative and Empirical Perspectives (supra* note 3), pp. 9-32, at 26.

[11] See the report on Predictive Policing by S. Söderholm, chapters I.2-3; and R. Koulu, Digitalisaatio ja algoritmit – oikeustiede hukassa? [Digitalisation and algorithmic decision-making – jurisprudence at the crossroads?]. *Lakimies,* Vol. 116, 2018, pp. 840-867, at 858-859. Especially the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security should be mentioned (Act of 1054/2018; an informal translation into English is available from the website of the Ministry of Justice: https://www.finlex.fi/fi/laki/kaannokset/2018/en20181054.pdf). For example, Section 13 of the Act prescribes that "a decision shall not be based solely on automated processing of personal data if the decision produces adverse legal effects concerning the data subject or otherwise significantly affects him or her".

[12] See a more detailed research article: Lauri Lahti (2022). Challenges of developing personalized artificial intelligence for public services. 1 August 2022. A self-archived research article manuscript available with open access at https://aaltodoc.aalto.fi

[13] Ministry of Social Affairs and Health (no date). The Well-being and Health Sector's Artificial Intelligence and Robotics Programme (Hyteairo). [Hyvinvoinnin tekoäly ja robotiikka -ohjelma Hyteairo.] Ministry of Social Affairs and Health. https://stm.fi/en/the-well-being-and-health-sector-s-artificial-intelligence-and-robotics-programme-hyteairo- and https://stm.fi/hyteairo

[14] Ministry of Finance (no date). National Artificial Intelligence Programme AuroraAI. [Kansallinen tekoälyohjelma AuroraAI.] Ministry of Finance. https://vm.fi/en/national-artificial-intelligence-programme-auroraai and https://vm.fi/tekoalyohjelma-auroraai

[15] G. Misuraca & C. Van Noordt (2020). Overview of the use and impact of AI in public services in the EU. AI Watch : artificial intelligence in public services. Science for Policy Report. EUR 30255 EN. Publications Office of the European Union.

program have not been initiated specifically for the purposes of predictive justice (such as the assessment of dangerousness of offenders) but it appears that anyway these programs are actively advancing development of solutions that could be technically relatively easily reconfigured and converted in the future to be applicable in preventive justice as well although this could be ethically very problematic. A thorough and open public discussion about the acceptability of using artificial intelligence in preventive justice is still lacking, and also the development of regulation about various criteria and responsibilities concerning this purpose seems difficult[16]. As long as the acceptability among ordinary people and the regulation remain unclear and incomplete, it is highly recommendable not to use artificial intelligence in preventive justice.

It has been considered difficult to develop artificial intelligence solutions that can be fluently connected to the human conceptualization[17]. Especially the ethical and emotional aspects of human cognition and decision making are features that have proven to be hard to translate into computational formulations. A large amount of human knowledge is already available in a digital format (for example as texts, images and videos) and thus can be processed by computations but developing algorithmic human-like reasoning based on the knowledge entities is a complex task. If the current problem of interpretation of texts automatically could become increasingly solved it might offer a practical way to make artificial intelligence algorithms to take into consideration various legal texts and regulatory statements when carrying out diverse decision making tasks, for example assisting in planning a patient's care, crafting a cost-effective municipal budgeting and designing the recycling options for the community biowaste.

In general, it seems that artificial intelligence solutions are easier to accept and adopt by the citizens if these solutions have an emphasis on giving help that does not limit anyone's freedom but instead offers positive personalized, empowering advice[18]. However, serious ethical questions are encountered, if the artificial intelligence is expected to be used for purposes that may implement punishments, such as

https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120399/jrc120399_misuraca-ai-watch_public-services_30062020_def.pdf

[16] R. Koivisto, J. Leikas, H. Auvinen, V. Vakkuri, P. Saariluoma, J. Hakkarainen & R. Koulu (2019). Artificial intelligence in authority use - ethical and societal acceptance issues. [Tekoäly viranomaistoiminnassa - eettiset kysymykset ja yhteiskunnallinen hyväksyttävyys.] Publications of the Government's analysis, assessment and research activities 14/2019. Prime Minister's Office. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161345/14-2019-Tekoaly%20viranomaistoiminnassa.pdf

[17] L. Laranjo, A. Dunn, H. Tong, A. Kocaballi, J. Chen, R. Bashir, D. Surian, B. Gallego, F. Magrabi, A. Lau & E. Coiera (2018). Conversational agents in healthcare: a systematic review. *Journal of the American Medical Informatics Association*, 2018;25(9):1248-1258. https://doi.org/10.1093/jamia/ocy072

[18] R. Koivisto et al. (2019).

deciding whether a crime has occurred based on the available evidence, or deciding the suitable sanctions for committed crimes or predicting the emergence of criminal behavior in ordinary citizens or assessment of dangerousness of offenders. The development of artificial intelligence solutions that assist in implementing public services that are personalized to address the person's needs and identified risks is introducing various ethical challenges. Various types of socioeconomic disadvantage and risk behavior is accumulated on certain same overlapping population groups. Thus when the public authorities are developing artificial intelligence solutions that assist in screening persons that could be helped by the social workers, home care nurses or the employment office for positive empowering of the citizen, these developed screening tools can at the same time introduce possibilities for screening the same citizen in respect to identifying behavior patterns that are expected to be linked to criminal activity.

The Ministry of Social Affairs and Health coordinated and funded during years 2018-2021 the Well-being and Health Sector's Artificial Intelligence and Robotics Programme (Hyteairo program) that had an aim to support and accelerate the use of artificial intelligence and robotics in wellbeing services and processes[19]. The Hyteairo program was implemented with a diverse network of collaborating organizations representing public, private and non-governmental sectors. During the realization of the Hyteairo program its application domains and focus points were clarified so that from the year 2021 the program had three main application domains and four operational domains. Thus, as of 2021 the Hyteairo program's three main application domains were living at home, conversational artificial intelligence for social affairs and health (together with the AuroraAI program that was started in 2020) and artificial intelligence in analytics (in knowledge management and in research), and the four operational domains were network collaboration, developing know-how, evaluation of outcomes and effectiveness, and international collaboration.

The report about the artificial intelligence-based knowledge management relying on the data of the social affairs and health[20] provides an overview of the recent development and results in this field concerning among others the various aims, investigations, experiments, developed solutions and findings, identified needs for

[19] Ministry of Social Affairs and Health (2022). Hyteairo - Hyvinvoinnin tekoäly ja robotiikka -ohjelma : loppuraportti 2022. [Hyteairo - Well-being and Health Sector's Artificial Intelligence and Robotics Programme : final report 2022.] Ministry of Social Affairs and Health. https://urn.fi/URN:NBN:fi-fe2022021619558

[20] M. Perälä-Heape & V. Virta (2021). Tekoäly sote-tiedolla johtamisessa. Tilannekuvaraportti. [Artificial intelligence in directing with social affairs and health information. Situation description report.] December 2021. Centre for Health and Technology, University of Oulu. https://thl.fi/documents/10531/6281814/Tilannekuvaraportti+Teko%C3%A4ly+sote-tiedolla+johtamisessa+-+s.pdf

analytics and addressing the regulation. This report mentions that the Finnish Institute of Health and Wellbeing (THL) and the Finnish Social Insurance Institution (KELA) are organizations that have initiated experiments about artificial intelligence-based solutions to identify peoples at risks to provide personalized support services. The importance of careful and efficient decision making is highlighted in the emergency care and thus responsible development of artificial intelligence-supported services in this domain can be considered to be valuable. The public authorities maintain various knowledge resources that can be expected to be exploitable for building new artificial intelligence-supported services that can assist in decision making about the emergency care, such as the emergency care requirement guidance library that is publicly provided by DigiFinland Oy with the coordination and assignment given by the Ministry of Social Affairs and Health[21].

Relying on the Hyteairo program's broad participant network the report of J. Lähesmaa *et al.* (2021)[22] presents a collection of recommendations for advancing the development of a clear operational model to address the evaluation of health and wellbeing applications and their substitutability by public funds. These recommendations highlight various complementing aspects of different interest groups, including the technology companies, authorities, customers, organizations of the social affairs and health, professionals, researchers, ability experts and educators. The report proposes that health and wellbeing applications should have an evaluation process that is defined and agreed collaboratively on the European level and that Finland should have nationally an own specifically dedicated authority or institution for carrying out evaluations. Also, the report argues that the data generated by health and wellbeing applications has an essential value and there is a need to formulate shared agreements on the European level about its use and the transparency of its use. The report emphasizes that the evaluations, approvals and substitutability by public funds should be done based on the utility value which needs to be evidenced by an independent research evaluation.

[21] Hoidon perusteet (2022). Emergency care requirement guidance library provided by DigiFinland Oy with the coordination and assignment given by the Ministry of Social Affairs and Health. In Finnish. https://hoidonperusteet.fi/static/instructions and https://116117.fi/hoidonperusteet/

[22] J. Lähesmaa, J. Reponen, H. Anttila (eds.) (2021). Hyteairon pyöreän pöydän julkilausuman tausta ja yhteisesti kirjoitetut ratkaisuehdotukset: Terveys- ja hyvinvointiteknologioiden arviointi ja korvattavuus sosiaali- ja terveyspalveluiden asiakkaille. [Background and collectively written solution proposals of the public statement of the Hyteairo's round table: Assessment of the health and wellbeing technologies and their substitutability for the customers of the social affairs and health services.] Based on the meetings 14-17 June 2021. https://thl.fi/documents/10531/5914371/Hyteairon+py%C3%B6re%C3%A4n+p%C3%B6yd%C3%A4n+julkilausuma+14_17.6.2021-+pitk%C3%A4+versio_logo+ok.pdf

The Finnish national artificial intelligence program AuroraAI is a development project that has been launched and funded for the years 2020-2022 to address strategic goals of the Finnish government[23]. The AuroraAI program is planned to build a network of artificial intelligence-supported public sector services (AuroraAI network) that is usable by citizens and organizations by the end of the year 2022 as well as to build a new operational model which integrates the knowledge, tools and structures about how to transition well to a new era using more human-centric and artificial intelligence-supported public sector services.

The AuroraAI program initially aimed to focus addressing specifically three different life event entities (which were keeping young people involved in the society by preventing their marginalization, enabling foreign students to become attached into the Finnish working life and society, and supporting coping in working life with continuous learning)[24], but during the implementation the AuroraAI program has reduced the number of focused three life event entities to only one focused life event entity which appears to be the prevention of the marginalization of young people[25] [26]. This prevention of the marginalization of young people is aimed to be carried out by building a new recommendation tool that recommends suitable services for a person based on the information input that he/she provides to the tool without a strong identification.

The mid-term evaluation of the AuroraAI program identifies that the program has suffered from unclear aims, coordination and governance. [27] The mid-term evaluation suggests that the planning discussions for the further continuation of the AuroraAI program relies on four entities: efforts to link different service providers to the shared knowledge base, finding ways for a public sector reform that could enable implementation of the new operational model, continuing further technical development addressing also the available resources and a possible introduction of

[23] Ministry of Finance (no date).

[24] Ministry of Finance (2020). Asettamispäätös VN/1332/2020. Kansallinen tekoälyohjelma AuroraAI. [Appointment decision VN/1332/2020. National Artificial Intelligence Programme AuroraAI.] Ministry of Finance. https://vm.fi/documents/10623/16264993/aurora+asettamispaatos+korjattu.pdf/fd7831ba-d4b8-d0a8-e7f2-9cb38407c698/aurora+asettamispaatos+korjattu.pdf

[25] Ministry of Finance (2021). AuroraAI-ohjelma 2020-2022. Toimintasuunnitelma 2022. [AuroraAI program 2020-2022. Action plan 2022.] VN/1332/2020. 25.11.2021. Ministry of Finance. https://vm.fi/documents/10623/89568191/AuroraAI-ohjelman+toimintasuunnitelma+2022.pdf/e80d88db-ed11-267d-3f27-d9d0e8ca4067/AuroraAI-ohjelman+toimintasuunnitelma+2022.pdf

[26] Owal Group and 4Front (2022). AuroraAI-ohjelma. Arviointiraportti. Väliarviointi, 10.1.2022. [AuroraAI program. Evaluation report. Mid-term evaluation, 10.1.2022.] A report implemented collaboratively by Owal Group Oy and 4Front Oy by the appointment of Ministry of Finance. https://vm.fi/documents/10623/101263033/AuroraAI+v%C3%A4liarviointiraportti.pdf/c2bd5500-9588-251d-7155-b0a713ecb69b/AuroraAI+v%C3%A4liarviointiraportti.pdf

[27] *Ibid.*

a strong identification with non-anonymous identities, and advancing the discussions about the ethical use of artificial intelligence in the public sector and sharing useful notions and recommendations of this ethical use. The AuroraAI program's initial ethical code appears to have been defined in the report of Haataja et al. (no date)[28] which aims to represent the legal basis for the artificial intelligence services developed by the AuroraAI program.

The AuroraAI program has established an Ethics Board coordinated by the Digital and Population Data Services Agency (Digi- ja väestötietovirasto) to evaluate the efforts to develop the AuroraAI program's artificial intelligence-supported public sector services in a human-centric, ethical and responsible way and verifying the use of artificial intelligence non-harmfully for human wellbeing. The AuroraAI program's action plan for the year 2022 [29] mentions that the people developing the AuroraAI program have during the year 2021 investigated the AuroraAI program's activities from various ethical and juridical perspectives and created two reports evaluating the program's principles, aims, service recommendation, knowledge management, juridical questions, service ecosystems and supporting equality. The AuroraAI program's action plan for the year 2022 also mentions that the program aims to continue addressing ethical questions among others by creating operational recommendations, evaluating the need for initiating a new legislative preparation and possibly initiating it, and formulating a new visionary document describing how to advance human-centric aspects in the legislation.

Various outcomes of the work that the AuroraAI program's Ethics Board has produced by the beginning of the year 2022 are reported in the research article of Leikas et al. (2022)[30] which appears to be one of the most detailed publicly archived documents describing the ethical issues identified in the development of the AuroraAI program and discussing them in a peer-reviewed scientific format with giving contexts and references to other related research. According to Leikas et al. (2022)[31], the main issues identified by the AuroraAI program's Ethics Board include, among others, that the AuroraAI program has a positive aim to help citizens in

[28] M. Haataja, M. Latvanen and the AuroraAI's ethics network (no date). AuroraAI-esiselvityshanke : Etiikka-työkokonaisuuden suositukset. [AuroraAI pre-investigation project : Recommendations of the ethics work entity.] Meeri Haataja (Saidot), Marko Latvanen (VRK) and the AuroraAI's ethics network. https://vm.fi/documents/10623/13292513/AuroraAI+esiselvityshanke+-+Etiikka-suositukset.pdf/e1737144-14bd-8dec-e706-db8a963b6cc7/AuroraAI+esiselvityshanke+-+Etiikka-suositukset.pdf

[29] Ministry of Finance (2021).

[30] J. Leikas, A. Johri, M. Latvanen, N. Wessberg & A. Hahto (2022). Governing Ethical AI Transformation: A Case Study of AuroraAI. *Frontiers in Artificial Intelligence*, 5:836557, 2022. https://doi.org/10.3389/frai.2022.836557

[31] *Ibid.*

service findability, to create service ecosystems for specific life events, and to better identify and address the needs of different population groups, but that the AuroraAI program requires careful attention and appropriate actions to implement data policy and privacy to protect the citizens.

According to Leikas et al. (2022)[32], the AuroraAI program's Ethics Board has considered that significant data privacy issues need to be carefully addressed if the AuroraAI program aims to update its service development so that the originally planned high-level anonymization of the users could become possibly relaxed in data handling. The anonymization of the user identities has been initially seen as an important way to enforce trust and to avoid privacy and security risks of the AuroraAI program. On the other hand, it is acknowledged from a technical viewpoint, that to enable the artificial intelligence models to evolve to identify better data patterns and generate increasingly accurate and useful predictions and recommendation based on them it is valuable to maximize the tracking of the same user when he/she interacts at consecutive times with the service so that the models could learn wellbeing entities in longer chains of events than just in single events and how the earlier recommendations may have affected the user's later wellbeing progress. However, since the AuroraAI program aims to carry out very detailed and long-lasting personal data collection and aims to use it to design and implement new large complex service networks and ecosystems, the AuroraAI program's Ethics Board has expressed a strong need to further deepen addressing the data privacy aspects in the development of the AuroraAI program, as well as a need to broaden the planning by gathering a further representative involvement from various intended future user groups.

The research article of Kuziemski & Misuraca (2020)[33] has evaluated the AuroraAI program in a comparison of artificial intelligence governance in the public sector covering three national approaches implemented in Finland, Poland and Canada. This evaluation identified that among the risks for the AuroraAI program are that the program appears lacking transparency thus being hard to comprehend for both public authorities and general public, and the program's success was considered to rely on the introduction of a common legal framework, and implementing appropriate data protection for the sensitive user data of the intended artificial intelligence services.

[32] *Ibid.*

[33] M. Kuziemski & G. Misuraca (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications policy*, 44(6), 101976, July 2020. https://doi.org/10.1016/j.telpol.2020.101976

While it has shown to be difficult to develop large comprehensive semantic models for artificial intelligence, there are also other efforts to advance human-computer interaction with relatively compact and simple models that can be modularly exploited as building blocks for greater algorithm entities[34]. Among these alternative approaches, we mention some recent promising results gained when developing a human-understandable artificial intelligence methodology with self-rating data collected from diverse population groups recruited from Finnish patient and disabled people's organizations, other health-related organizations and professionals, and educational institutions. The research articles of this author[35] [36] proposed and experimentally motivated a new methodology that enabled to identify in interpretation tasks done by humans how statistically significant rating differences were linked to machine learning results thus helping to develop better human-understandable machine learning models. These machine learning models can serve as useful building blocks for advanced artificial intelligence solutions. Furthermore, that research provided empirical evidence about the applicability of machine learning to support interpretation of the need for help in the patient's expressions.

Extending on the foundation and promising results of the previous research, a subsequent research[37] proposed a new methodology, questionnaire data and its statistical patterns which enabled analyzing with self-rated expression statements the representations of decision making steps in healthcare situations and their chaining, agglomeration and branching in the large knowledge entities of personalized care paths, such as patient records, patient diaries, care plans and care guidelines. Identified differences and dependencies in personal interpretation ratings and their durations in respect to the person's background enable building new artificial intelligence solutions that can manage to interpret increasingly

[34] L. Laranjo et al. (2018).

[35] Lauri Lahti (2020). Interpretation of the patient's need for help can be supported with machine learning. In Juli Mansnérus, Raimo Lahti & Amanda Blick (eds.), *Personalized medicine: legal and ethical challenges.* Faculty of Law, University of Helsinki, Finland, Forum Iuris Series, Helsinki, Finland, 2020. ISBN 978-951-51-6940-2 (printed), ISBN 978-951-51-5021-9 (online). Open access: https://doi.org/10.31885/9789515169419

[36] Lauri Lahti (2022a). Detecting the patient's need for help with machine learning based on expressions. *BMC Medical Research Methodology,* Volume 22, article number 60, 2022. This research article is supplemented with two supplementing documents. https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/s12874-021-01502-8 and https://doi.org/10.1186/s12874-021-01502-8

[37] Lauri Lahti (2022b). Developing patient-driven artificial intelligence based on personal rankings of care decision making steps. A research article manuscript completed and self-archived on 11 May 2022 on the open-access Arxiv repository (https://arxiv.org/abs/2205.07881). This manuscript (104 pages) is supplemented with seven supplementing documents (2781 pages). Open access: https://arxiv.org/pdf/2205.07881 and https://doi.org/10.48550/arXiv.2205.07881

complex linguistic structures of decision making steps when helping to address the patient's needs and preferences concerning his/her care.

Motivated by the above-mentioned previous research, a subsequent research has been designed by proposing a new research methodology for developing artificial intelligence algorithms to support decision making in healthcare based on a multidisciplinary combination of real-life data gathered in brain research and care events of different patient groups[38]. An important motivator for the proposed new research methodology is also that the patient's rights have gained increasing protection by legislation in the European region, Finland being among the pioneers[39] [40], and the European Commission has proposed artificial intelligence regulation[41]. The European Commission's Coordinated Plan on Artificial Intelligence 2021 Review[42] recognizes the importance of developing application of artificial intelligence in various domains of health and healthcare, including also supporting humans in clinical decisions and treatment choices as well as improving analysis of health images, laboratory and histological data, diagnostic accuracy, and access to healthcare.

[38] Lauri Lahti (2022c). Developing ethical and transparent artificial intelligence algorithms to support decision making in healthcare based on brain research and personal care events of patients. Research article manuscript self-archived on 15 July 2022 at https://aaltodoc.aalto.fi/handle/123456789/115565 . Open access: http://urn.fi/URN:NBN:fi:aalto-202207154400

[39] Raimo Lahti (2012). Medical law and biolaw. In K. Nuotio, S. Melander, S., & M. Huomo-Kettunen,(eds.), *Introduction to Finnish Law and Legal Culture.* Faculty of Law, University of Helsinki, Helsinki, Finland. Forum Iuris Series, Helsinki, Finland, 2012, pp. 249-260. ISBN 978-952-10-7817-0. Reprinted in the compilation publication: Raimo Lahti (2021). Towards an Efficient, Just and Humane Criminal Justice: Nordic Essays on Criminal Law, Criminology and Criminal Policy 1972-2020. Publications of the Finnish Lawyers' Association, Series D (Ius Finlandiae), No. 8, pp. 528-541, The Finnish Lawyers' Association, Helsinki, Finland, 2021. ISBN 978-951-855-386-4 (printed), ISBN 978-951-855-387-1 (online). Open access: https://edition.fi/lakimiesyhdistys/catalog/book/121

[40] D. Townend, C. Clemens, D. Shaw, H. Brand, H. Nys, & W. Palm (2016). Patients' rights in the European Union: mapping exercise: final report. Written by PRE-MAX Consortium, March 2016. European Commission, Directorate-General for Health and Food Safety, 2018. Publications Office. Published 25 January 2018. ISBN 978-92-79-66960-6. https://data.europa.eu/doi/10.2875/751285

[41] European Commission (2021a). Proposal for a Regulation of the European Parliament and of the Council. Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM(2021) 206 final, 2021/0106(COD). European Commission, Directorate-General for Communications Networks, Content and Technology, 21 April 2021, Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[42] European Commission (2021b). Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Fostering a European approach to Artificial Intelligence. Coordinated Plan on Artificial Intelligence 2021 Review. COM(2021) 205 final, ANNEX. 21 April 2021, Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0205

The new proposed research[43] develops ethical and trustworthy artificial intelligence algorithms to address the European Commission's recommendations by carrying out extensive series of alternative microbiological and human-computer interaction measurements, data pattern modeling and experimental clustering and deep learning-based computational analyses concerning the fundamental processes of biologically naturally emerging classifications and decision making steps of the human mind in carefully designed new experimental setups. The proposed new research methodology is motivated and takes inspiration from the broad review and comparative analysis of Karim et al. (2021)[44] about unsupervised deep learning-based clustering analysis techniques for bioinformatics research (especially in the three use cases of bioimaging, cancer genomics and biomedical text clustering), the alternative approaches developed for comparisons between biological data clustering algorithms (such as the quality of clusters measured in respect to known classification schemes or some theoretical standards)[45], and the previous neurobiology research that has proposed various ways to explain how the brain learns and uses models[46] [47] [48] [49] [50].

This subchapter has described challenges that are present when aiming to develop ethical artificial intelligence for identifying personal needs and risks. These challenges affect also the development of artificial intelligence solutions for the purposes of preventive justice. It seems difficult to develop and implement trustworthy artificial solutions and especially so that their operational principles could be easily understandable, investigable and acceptable by all people who are affected by the decision making done with these solutions[51]. Therefore it is important

[43] Lauri Lahti (2022c).

[44] M. Karim, O. Beyan, A. Zappa, I. Costa, D. Rebholz-Schuhmann, M. Cochez & S. Decker (2021). Deep learning-based clustering approaches for bioinformatics. *Briefings in Bioinformatics*, Volume 22, Issue 1, January 2021, pp. 393–415. https://doi.org/10.1093/bib/bbz170

[45] Y. Lu, C. Phillips & M. Langston (2019). A robustness metric for biological data clustering algorithms. *BMC Bioinformatics* 20, 503 (2019). https://doi.org/10.1186/s12859-019-3089-6

[46] M. Botvinick (2007). Multilevel structure in behaviour and in the brain: a model of Fuster's hierarchy. *Philosophical Transactions of the Royal Society B*, 362(1485), 1615-26. https://doi.org/10.1098/rstb.2007.2056

[47] J. Wang, Z. Kurth-Nelson, D. Tirumala, H. Soyer, J. Leibo, R. Munos, C. Blundell, D. Kumaran & M. Botvinick (2016). Learning to reinforcement learn. *arXiv.* 2016; 1611.05763. https://arxiv.org/abs/1611.05763

[48] J. Wang, Z. Kurth-Nelson, D. Kumaran, D. Tirumala, H. Soyer, J. Leibo, D. Hassabis & M. Botvinick (2018). Prefrontal cortex as a meta-reinforcement learning system. *Nat. Neurosci.* 2018; 21: 860-868. https://doi.org/10.1038/s41593-018-0147-8

[49] Y. Duan, J. Schulman, X. Chen, P. Bartlett, I. Sutskever & P. Abbeel (2016). RL^2: fast reinforcement learning via slow reinforcement learning. *arXiv*. 2016: 1611.02779. https://arxiv.org/abs/1611.02779

[50] S. Ritter, J. Wang, Z. Kurth-Nelson, S. Jayakumar, C. Blundell, R. Pascanu & M. Botvinick (2018). Been there, done that: meta-learning with episodic recall. *International Conference on Machine Learning*. 2018: 4351-4360. https://proceedings.mlr.press/v80/ritter18a/ritter18a.pdf

[51] R. Koivisto et al. (2019).

that the public authorities take a clear responsibility for realization of appropriate legal regulation and sufficient control and sanctioning mechanisms to guarantee that the development and implementation of artificial intelligence solutions and their application is carried out openly and with a mutual agreement of all parties involved and ensuring that the citizens' rights and privacy are well protected from unethical use of artificial intelligence.

Part III. Evidence law

Written by Juhana Riekkinen[*]

1. Evidence-gathering through AI-based systems

1.1 Use of AI-based systems in practice

There is very little information publicly available on the use of AI-based systems for evidence-gathering purposes in Finland. Within the police organization, in particular the National Bureau of Investigation ('NBI') has significant digital forensics capabilities. The NBI Forensic Laboratory assists and supports other law enforcement units by performing forensic analyses of various kinds, including digital forensics. Further, the NBI has a unit focused on cybercrime prevention and investigations (Cybercrime Center). While the exact operational capabilities of these units are not public, it is highly likely that they have access to state-of-the-art digital forensics tools with AI-based features, including tools for technology-assisted review of documents and mobile device forensics.

In the private sector, digital forensics services are offered by several companies that operate in the cybersecurity/ICT field and major accounting firms. At least one Finnish digital forensics firm is partnered with providers of forensic software with known AI-based features, such as OpenText (EnCase Forensic) and Cellebrite (UFED).[1] It is likely that other companies are offering services featuring the use of some AI-based tools for the purposes of evidence-gathering and analysis, but there are no statistics or research that would show to what extent these services are used by law firms or any other companies in Finland. The following will therefore focus

[*] Juhana Riekkinen is University Lecturer in Legal Informatics, University of Lapland, Faculty of Law, Finland (juhana.riekkinen@ulapland.fi).

[1] Difseco Oy, OpenText and Other Services <https://difseco.com/other-services/> accessed 28 March 2022.

on the legal conditions of AI-assisted or AI-enabled digital forensics investigations under Finnish law.

1.2 Relevant normative frameworks

First, it should be noted that the European data protection framework fully applies to data processing by Finnish public organizations and private companies. Most police data processing activities are governed by the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018, 'Act on the Processing of Personal Data in Criminal Matters'), which implements the Law Enforcement Directive ((EU) 2016/680)[2]. This act grants the police and other competent criminal justice authorities the permission to process personal data when it is necessary for performing their duties related to, *inter alia*, prevention, detection, investigation, and prosecution of criminal offences.[3] Besides providing the legal basis for processing, this act regulates and sets limits on data processing activities by these authorities. The Act on the Processing of Personal Data by the Police (616/2019) complements the Act on the Processing of Personal Data in Criminal Matters, and in part, the General Data Protection Regulation ((EU) 2016/679, 'GDPR')[4], which applies as a *lex generalis* to police data processing that is beyond the scope of the Law Enforcement Directive. Other law enforcement authorities with duties relating to investigating crime are bound by their own data processing acts.[5] Public data processing activities beyond the scope of the Law Enforcement Directive and practically all private data processing activities are subject to the GDPR and the Data Protection Act (1050/2018), which complements the directly applicable EU regulation on the national level.

To be clear, the directly AI-related prohibitions on fully automated individual decision-making in the GDPR (Article 22) and the Act on the Processing of Personal

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[3] Act on the Processing of Personal Data in Criminal Matters, ss 4(1) and 1(1).

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] These acts concern the processing of personal data by the Border Guard (639/2019), by the Customs (650/2019), and in the Defence Forces (332/2019). – As a general note, Finnish parliamentary acts are officially available in Finnish and Swedish, but there is a collection of unofficial translations to other languages available at Finlex, Translations of Finnish acts and decrees < https://www.finlex.fi/en/laki/kaannokset/> accessed 28 March 2022. This report makes use of these unofficial translations when possible, but for some acts mentioned in this report, there are no English translations available.

Data in Criminal Matters (section 13) do not apply to evidence-gathering with the help of AI-based tools. Evidence-gathering activities do not produce the kind of decisions referred in these provisions, and AI-assisted evidence-gathering is typically subject to human oversight. More generally, however, AI-assisted evidence-gathering and digital forensics investigations necessarily involve processing of personal data. Therefore, data protection law needs to be fully complied with in all such activities, regardless of whether these investigations are performed by public authorities or private companies.

Beyond data protection legislation, there is currently no normative framework explicitly governing the use of AI-based systems for gathering evidence.[6] The principle of legality, enshrined in section 2(3) of the Constitution of Finland (731/1999), requires that the exercise of public powers shall be based on an Act. In the absence of a parliamentary act granting law enforcement authorities the power to use AI-based systems in evidence-gathering, it could be argued that the use of such systems is illegal. However, Finnish legislation generally adheres to the principle of *technology neutrality*, focusing more on functions and purposes than on specific technologies. Hence, the use of many AI-based systems by public authorities may be based on more general laws and provisions that do not specifically recognize AI, AI-related technologies, or individual AI-based systems.

Thus, to determine the legal limits of AI-enabled evidence-gathering by the police, the general normative framework that enables law enforcement authorities to conduct criminal investigations should be considered. The bulk of this framework consists of three parliamentary acts: the Criminal Investigation Act (805/2011), the Coercive Measures Act (806/2011), and the Police Act (872/2011).[7]

The conduct of criminal investigations is regulated in the Criminal Investigation Act. This *lex generalis* is complemented by the Coercive Measures Act, which governs the use of coercive measures that, among other things, allow the police to gather evidence of suspected criminal offences. These measures include different types of searches and seizure (chapters 7 and 8), but also a multitude of covert investigatory powers for surreptitious monitoring of telecommunications and technical devices (chapter 10). In addition to provisions on other police activities beyond criminal investigations, the Police Act contains provisions on covert measures similar to those regulated in chapter 10 of the Coercive Measures Act. These powers may be used for

[6] Of course, if approved, the EU AI Act (European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts' COM(2021) 206 final) will likewise be directly applicable in Finland.

[7] Additionally, *lex specialis* acts govern some aspects of crime prevention and criminal investigations by the Border Guard (108/2018), the Customs (623/2015), and in the Defence Forces (255/2014).

the purposes of prevention and detection of crime and for civilian intelligence, as opposed to the Coercive Measures Act powers, which enable the police to investigate criminal offences that have already been committed (or are suspected to have been committed).[8]

Powers defined in the Coercive Measures Act allow the police to gain access to, copy, or record computer data (including content data and metadata) from various sources, including devices used by suspects and third parties. In keeping with the principle of technology neutrality, the Coercive Measures Act contains very little regulation on what kind of hardware or software tools or methods may be used for executing these investigatory measures. There are no explicit mentions of AI or AI-based tools, and the addition of specific AI-related rules seems unlikely in the near future.[9] The focus is on regulating decision-making procedures and conditions of access to potential evidence, and the further analysis of data that has been lawfully confiscated (along with a physical medium) or copied to be used as evidence is largely unrestricted. The Coercive Measures Act does not explicitly prohibit any analytical methods or tools, and it should not be interpreted as precluding the use of AI-based software in general. However, institutionalized legal principles such as *proportionality*, *minimum intervention*, and *sensitivity*,[10] and provisions safeguarding legal privileges[11] may limit certain methods, tools, or means subject to case-by-case analysis. In particular, this is relevant for searches targeting devices used by certain groups of professionals, such as lawyers, medical professionals, and journalists.[12] These principles and rules may even limit the use of non-AI-related digital forensics

[8] Generally on investigatory powers in Finnish law from the viewpoint of digital investigations, see Juhana Riekkinen, 'Evidence of Cybercrime and Coercive Measures in Finland' (2016) 13 Digital Evidence and Electronic Signature Law Review 49, 50, 55–66.

[9] A working group set by the Ministry of Justice recently published a report concerning the needs to amend the Coercive Measures Act. This report only mentions AI in relation to real-time biometric identification in connection with certain covert coercive measures, and the working group opted not to prepare any draft provisions on this (largely due to uncertainty regarding the impact of the upcoming EU AI Act). Lauri Rautio et al., *Pakkokeinolain muutostarpeiden tarkastelu: Työryhmämietintö* (Ministry of Justice 2022) 65–66.

[10] Coercive Measures Act, c 1 ss 2–4. Criminal Investigation Act, c 4 ss 4–6 and Police Act, c 1 s 2 define similar principles.

[11] Coercive Measures Acts, c 7 s 3 contains prohibitions on confiscation and copying of privileged material, with references to provisions on right or duty not to testify in Code of Judicial Procedure, c 17. Provisions on "special" searches which are likely to involve privileged material are located in Coercive Measures Act, c 8, and may apply to searches of data contained in a device (through a reference in c 8 s 28).

[12] These "special" searches are subject to specific conditions and procedural rules, including the appointment of an independent representative, who is tasked with supervising the search procedure and making sure that no privileged material is searched or copied.

practices, such as the creation of forensic duplicates (bit-for-bit copies) of the entire contents of storage media.[13]

Private companies are not bound by the constitutional principle of legality. However, to be able to conduct (or to authorize a third party to conduct) forensic investigations, they must have lawful access to the potential evidence to be analyzed. Generally, private parties may not conduct investigations with methods comparable to investigatory powers defined in the Coercive Measures Act or the Police Act, regardless of whether AI-based tools are used or not. Private investigations targeting devices and computer data that are not under the lawful control of the investigating party may trigger criminal liability. Potentially applicable provisions of the Criminal Code (39/1889) include computer break-in[14] and message interception[15].[16]

If the private party conducting the investigation has access to a device on which potentially relevant data are stored, they need to consider data protection obligations. For private entities, the law imposes no general duty to investigate crime, and therefore they do not have a similar general legal basis for processing crime-related personal data as the police do. However, Article 6(1)(f) of the GDPR recognizes the legitimate interests of the controller or a third party as a legal ground for processing, and Article 9(2)(f) allows the processing of even sensitive "special categories of personal data" for the establishment, exercise, or defense of legal claims. While these provisions provide a legal basis for data processing in most scenarios where digital forensics investigations are performed, the investigating party needs to adhere to all of the data processing principles defined in Article 5 (including *purpose limitation* and *data minimization*) and other duties and obligations specified in data protection law. This may limit the use of data-intensive AI-based tools.

If the potential evidence contains personal data of employees, the employer's evidence-gathering activities may be further restricted by the Act on the Protection

[13] Alternatively, it can be argued that forensic imaging is permissible regardless of the contents, and that the provisions that prohibit copying of privileged material should in these cases be interpreted as exclusionary rules that forbid further analysis and evidentiary use of any such material that is included in the forensic duplicate. Black-letter law and law drafting materials do not provide clear answers, and although there is some recent case law concerning the practicalities of "special" searches targeting devices with privileged data, the legal situation remains unclear. See Juhana Riekkinen, *Sähköiset todisteet rikosprosessissa* (Alma Talent 2019) 240–247.

[14] Criminal Code, c 38 ss 8–8a.

[15] Criminal Code, c 38 ss 3–4.

[16] As elaborated later, criminal acts by private parties may trigger exclusion of evidence obtained by such means in a subsequent trial. However, compared to unlawful or outright criminal evidence-gathering by public authorities, criminal acts by private parties are less likely to trigger the exclusionary rule under Code of Judicial Procedure, c 17 s 25(3).

of Privacy in Working Life (759/2004). Processing of e-mails and other data related to electronic communications is also subject to the Act on Electronic Communications Services (917/2014), which contains provisions implementing the EU ePrivacy Directive (2002/58/EC)[17]. In general, parties to electronic communications are entitled to process their own messages and traffic data, and may also give consent to other parties to engage in such processing (the consent of one party is sufficient).[18] The aforementioned act also regulates the conditions under which communications service providers and "corporate or association subscribers"[19] may process traffic data for the purposes of investigating suspected misconduct and criminal offences.[20] As a result of these rules, the permissibility of large-scale AI-based document review targeting the contents of employee e-mail accounts is highly questionable at best, and usually clearly illegal. AI-based review and analyses limited to communications metadata may be permissible.

Questions relating to evidence-gathering through AI-based systems have not been addressed in published case law, and there is practically no legal commentary.

1.3 Informational rights of the defendant

While there are no specific procedural rules concerning AI-based systems and information relating to the use of such systems, Finnish law grants the defendant informational rights allowing them wide access to information relevant to their case. These rights could be interpreted to cover some information relating to methods and tools of evidence-gathering, including if and how AI-based systems have been used in the investigation and how these systems operate. The informational rights of the defendant are governed by the European Convention on Human Rights ('ECHR'), the Constitution of Finland, the Criminal Investigation Act, and the Act on the Openness of Government Activities (621/1999, 'Openness Act').[21]

The principles of *audiatur et altera pars* and *equality of arms* are acknowledged in Finnish law. While these two principles are closely linked and sometimes even

[17] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[18] Act on Electronic Communications Services, s 136.

[19] This is defined as "an undertaking or organization which subscribes to a communications service or an added value service and which processes users' messages, traffic data or location data in its communications network" (Act on Electronic Communication Services, s 3(41)).

[20] Act on Electronic Communications Services, ss 143, 145a and 146–156.

[21] Data protection law (GDPR, Article 15 and Act on the Processing of Personal Data in Criminal Matters, s 23) contains further informational rights that may, under specific circumstances, enable the data subject to receive information that may be relevant in the context of criminal proceedings and thus complement the informational rights discussed here.

considered to be one and the same, they can be distinguished from each other.[22] *Audiatur et altera pars* is a foundational principle of procedural law: each party should have a chance to be heard. This includes a chance to present evidence, as well as to challenge and comment on evidence presented by other parties, which necessitates access to such evidence. The principle is incorporated in numerous provisions in different parliamentary acts, and it applies in virtually all court proceedings and in administrative decision-making.

Instead, *equality of arms* is more specifically a principle applicable in criminal proceedings, largely concretized by the case law of the European Court of Human Rights ('ECtHR') concerning Article 6(3) of the ECHR. From the point of view of informational rights and evidence, Finnish commentators have emphasized that this principle requires that the defendant is granted access not only to prosecution evidence but also to material which has not been named as evidence by the prosecution, but has surfaced during the investigation and may help the defense case. It should be possible for the defendant to gather evidence from the same "pool" of potential evidence that the criminal justice authorities have access to, including sources that have been left out from the official police protocol.[23] Mere technical possibility of access is not sufficient to guarantee true participation in the proceedings, and the defendant should also be provided with adequate time and facilities as required by Article 6(3)(b) of the ECHR.[24]

More specifically, the informational rights of parties, including defendants, are governed by chapter 4, section 15 of the Criminal Investigation Act. As a main rule, parties have the right to information on matters that have led to or become apparent in the criminal investigation and any documentation of the criminal investigation that may affect or could have affected the consideration of their matter. This right exceeds the general right of access to public documents,[25] applying also to documents and information that are to be kept secret under the Openness Act. However, there are some exceptions. Notably, the right may be denied if this is necessary to secure a very important public or private interest.[26] This exception may be applicable to some information regarding technical and tactical capabilities of law enforcement authorities, possibly including some information concerning the

[22] See Laura Ervo, *Oikeudenkäynnin oikeudenmukaisuusvaatimus: Käsikirja lainkäyttäjälle* (WSOYPro 2008) 133–136.

[23] Markku Fredman, *Rikosasianajajan käsikirja* (2nd edn, Alma Talent 2021) 476.

[24] Generally on equality of arms in Finnish legal literature, see, e.g., Laura Ervo, *Oikeudenkäynnin oikeudenmukaisuusvaatimus: Käsikirja lainkäyttäjälle* (WSOYPro 2008) 155–157, 262–264, 291 and Matti Pellonpää, Monica Gullans, Pasi Pölönen and Antti Tapanila, *Euroopan ihmisoikeussopimus* (6th edn, Alma Talent 2018) 616–621.

[25] Openness Act, s 9. Access to documents in the possession of public authorities is also guaranteed as a constitutional right (Constitution of Finland, s 12(2)).

[26] Criminal Investigation Act, c 4 s 15(3).

features of AI-based digital forensics tools or other AI-based systems used in criminal investigations. However, when considering such restrictions, "consideration shall be taken in the assessment of the right of the party to a proper defense or otherwise to appropriately secure their right in the court proceedings".[27] In practice, any restrictions must be evaluated in accordance with the requirements of ECtHR case law concerning Article 6(3) of the ECHR.[28] Of course, even law enforcement authorities may not have full access to all information regarding proprietary AI-based tools that they use, in which case such information may practically remain unavailable to the defendant, as well.

There are no published cases relating to the interpretation of informational rights of the defendant or equality of arms in relation to the use of AI-based systems. Furthermore, there is practically no legal commentary that would specifically address these AI-related issues in Finland.

2. Evidence produced by AI-based systems

2.1 Use of automated facial recognition and other AI-based systems for production of evidence

Data processing acts applicable to Finnish law enforcement authorities permit the use facial recognition technology for the purposes of preventing, detecting, and investigating criminal offences. Authorities may compare faces extracted from, e.g., surveillance camera recordings to photographs in various police databases.[29] A specific automated facial recognition system (KASTU) has been developed for police use. The use of this system began in May 2020, and details about its features are not public.[30] The system is mainly intended to be used to as a tool for directing investigations and finding likely matches to be confirmed by further analysis. The

[27] Criminal Investigation Act, c 4 s 15(4).

[28] Further, there are limitations to the right of access relating to covert investigations and the ways in which access to audio and video recordings may be granted (Coercive Measures Act, c 10 ss 60 and 62, Police Act, c 5 ss 58 and 60 and Criminal Investigation Act, c 9 s 7(2). A detailed account on the defendant's right to information can be found in Markku Fredman, *Rikosasianajajan käsikirja* (2nd edn, Alma Talent 2021) 466–515.

[29] Act on the Processing of Personal Data by the Customs, s 14(2) specifically mandates such comparison through automated facial recognition. The Act on the Processing of Personal Data in Criminal Matters and the Act on the Processing of Personal Data by the Police do not specifically mention automated facial recognition, but regulate the use of special categories of data in police registries for various purposes, including prevention, detection, and investigation of crime. The use of biometric data is generally permitted only when it is necessary (ss 11 and 15 of these Acts, respectively).

[30] Simo Ortamo, 'Poliisi on saanut rikollisia kiinni kasvoja tunnistavan tekoälyn avulla ja haluaisi laajentaa valtuuksiaan – testasimme, miten kone toimii' *Yle Uutiset* (1 August 2020) <https://yle.fi/uutiset/3-11448002> accessed 28 March 2022.

system is not intended to be used (or particularly suitable) for producing evidence directly.[31]

> As already discussed above, data protection law sets limits to evidence-gathering and investigations with the help of AI-based systems, and may prohibit or limit the use of certain kinds of facial recognition systems. For instance, current law arguably does not permit the use of real-time automated facial recognition systems in connection with live video streams and the coercive measures of technical observation and extended surveillance.[32] Furthermore, the use of the controversial *Clearview AI* facial recognition application has been deemed unlawful by the Finnish data protection authority. The application was trialed without a specific legal basis by the CAM/CSE unit of the NBI in early 2020; approximately 120 queries were made during the trial.[33] In September 2021, the Finnish Data Protection Ombudsman issued a reprimand to the NBI for unlawful processing of personal data in violation of the Act on the Processing of Personal Data in Criminal Matters.[34] Apparently, the queries did not lead to any information generated by the Clearview AI application being used as evidence in Finnish courts.

Although the police have shown considerable interest in automated facial recognition and other AI-based technologies in recent years, as far as the rapporteur is aware, the criminal justice authorities do not regularly employ any notable AI-

[31] However, as elaborated below, there are no evidence law rules that would specifically bar such evidence, or any other type of AI-produced evidence.

[32] Lauri Rautio et al., *Pakkokeinolain muutostarpeiden tarkastelu: Työryhmämietintö* (Ministry of Justice 2022) 65.

[33] 'Testing of facial recognition software by NBI reported to Data Protection Ombudsman' (9 April 2021) <https://poliisi.fi/en/-/testing-of-facial-recognition-software-by-nbi-reported-to-data-protection-ombudsman> accessed 28 March 2022.

[34] Data Protection Ombudsman, Decision, 20 September 2021, 3394/171/21. Further, the NBI were ordered to request the service provider to delete any personal data relayed to it by the NBI through the use of the Clearview AI software. See 'Police reprimand from Deputy Data Protection Ombudsman – police have initiated measures ordered' (28 September 2021) <https://poliisi.fi/en/-/police-reprimand-from-deputy-data-protection-ombudsman-police-have-initiated-measures-ordered> accessed 28 March 2022.

based systems to produce evidence for the purposes of criminal trials. Some evidence produced with the help of AI-based systems may be proffered in individual court cases, but AI-produced evidence remains a largely unrecognized phenomenon in Finnish courts.

2.2 Applicability of general evidence law norms

In short, there are no specific rules concerning evidence gathered or produced by AI-based systems in Finnish law. AI-based evidence is not considered a separate class or category of evidence, and there are no specific conditions on its admissibility in a trial, nor specific rules on how it should be assessed by triers of fact.

Traditionally, Finnish law of evidence has strongly embraced the *free theory of evidence*, setting very few formal standards, conditions, and requirements for the admissibility, presentation, and evaluation of evidence. Most aspects of evidence in civil and criminal proceedings are regulated in chapter 17 of the Code of Judicial Procedure (4/1734). The latest complete renewal of this chapter, which largely upheld the foundational status of the free theory of evidence despite introducing some new statutory exceptions, came into effect on 1 January 2016 (amendment 732/2015). Questions relating to *electronic evidence* or *digital evidence* were not emphasized in the drafting process, and Finnish law of evidence remains largely technology neutral. As a consequence of these general characteristics, the admissibility of computer data as evidence has never presented any particular legal problems in Finland,[35] but many norms on ICT-related aspects of evidence remain unclear.

Free introduction of evidence is an essential part of the free theory of evidence. Chapter 17, section 1(1) of the Code of Judicial Procedure guarantees each party the right to present evidence to the court investigating the case, as well as the right to comment on each piece of evidence presented in court. While there is no list of allowed or disallowed types of evidence, Finnish evidence law recognizes and regulates five basic categories (or means) of evidence. The court may hear 1) parties, 2) witnesses, and 3) expert witnesses, and 4) documents and 5) objects of judicial view may be presented to the court as evidence.

[35] Notably, Finland is a party to the Council of Europe Convention on Cybercrime (ETS No 185, 2001), which it ratified in 2007. According to the Explanatory Report to the Convention on Cybercrime, para 141 (concerning Article 14, on the scope of procedural provisions), this "Convention makes it explicit that Parties should incorporate into their laws the possibility that information contained in digital or other electronic form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted." This obligation did not necessitate any particular legislative amendments in connection with the ratification of the Convention.

All five categories of evidence may be used to relay AI-produced information to the court. For instance, parties and witnesses may tell the court how they conducted digital forensics investigations or otherwise produced evidence with the help of AI-based tools, and what results they obtained. Generally, parties and witnesses are heard orally in the courtroom, and written testimonies are not permitted.[36] However, if the person who conducted an AI-assisted investigation is not a party and has certain qualifications, they can be classified as an expert witness,[37] in which case they give their evidence initially in the form of a written statement. Expert witnesses may be further heard and cross-examined orally in the courtroom.[38]

The category of documents includes any representations of textual or comparable content, regardless of technology, format, or medium used for storing this information. Raw data, notes, and documentation generated during AI-assisted investigations may sometimes be considered as documents that can be presented as evidence as such. Especially in the context of digital forensics reporting, however, there may be some unclarity as to the difference between a written statement by an expert witness (in which case there should be the possibility of cross-examination in court) and a document presentable as evidence (in which case the opposing party has a right to comment on the document, but there may not be a person to cross-examine). However, if the court opts for the latter interpretation and the identity of the author (or a person who contributed to the creation of the document) is known, it may be possible to hear them as a (normal) witness.

Furthermore, there may be differing interpretations on whether a particular piece of evidence should be considered a document or an object of judicial view. The basic difference is that the probative value of a document lies in the textual message or content fixed on some medium, whereas the probative value of an object of judicial view is tied to its external (physical) properties, which can be observed directly with the human senses (typically sight, hearing, or touch).

[36] Code of Judicial Procedure, c 17 s 24, which also defines some exceptions. For instance, the court may allow a written statement "for a special reason".

[37] While normal witnesses tell the court of their experiences, expert witnesses are heard regarding empirical rules requiring special knowledge as well as regarding their application to the circumstances that arise in the case (Code of Judicial Procedure, c 17 s 34). Expert witnesses are to be known to be honest and competent in their field, and they may not be connected with the case or a party in a manner that endangers their impartiality (s 35).

[38] Code of Judicial Procedure, c 17 s 36(2): "An expert witness shall be heard in court in person if: 1) this is necessary in order to remove ambiguities, deficiencies or inconsistencies in their expert statement; 2) the court deems it necessary for another reason; or 3) a party requests this and the hearing would apparently not be meaningless."

> As has been traditionally noted, the very same sheet of paper can be both a document and an object of judicial view, depending on what a party intends to prove by presenting it. If the relevant fact can be proven by the informational content of the words written on a sheet of paper, the sheet should be considered a document. If the *factum probandum* can be deduced from the ink stains on the paper, the sheet should be considered an object of judicial view.[39] Similarly, an audio recording (digital or analogue) might be considered a document if the *factum probandum* relates to what has been said, whereas the recording could be considered an object if the *factum probandum* relates to the identity or the emotional state of the speaker, or the noises in the background. In law drafting materials and literature, visual representations of information, such as photographs, maps, and video recordings, are typically considered objects of judicial view (regardless of whether they are printed on paper or stored electronically in digital or analogue form).[40] Nevertheless, in court practice they might occasionally be included in the list of documents that have been presented as evidence.[41]

The traditional distinction between documents and objects is badly suited for many modern types of electronic evidence, as computer data that corresponds to textual content or other comparable "static" information with evidentiary value may be (re)presented in various alternative ways. Computer systems excel in the dynamic and often seamless combination of textual information with other types of media, and the correct interpretation of a message may depend on visual and structural

[39] This example is also mentioned in the Government Proposal on the 2016 evidence law renewal (Hallituksen esitys 46/2014 vp 100; law drafting documents are only available in Finnish and Swedish).

[40] Hallituksen esitys 46/2014 vp 100 and Pasi Pölönen and Antti Tapanila, *Todistelu oikeudenkäynnissä* (Tietosanoma 2015) 443–444, 449–450. Instead, for the purposes of the Openness Act and other laws concerning access to public documents, any photographs, maps, video recordings, and audio recordings clearly fall under the concept of document.

[41] In Sweden, differing views have been expressed concerning the classification of sound and video recordings (which is noteworthy, as Finnish and Swedish law of evidence traditionally share many similarities). See Jonas Ekfeldt, *Om informationstekniskt bevis* (Juridiska institutionen, Stockholms universitet 2016) 406–409.

aspects of its representation. Luckily, the legal significance of this distinction is also limited, as documents and objects of judicial view are mostly subject to the same norms.[42]

Judicial view may be directed at a physical object that is brought to the courtroom, or a virtual or digital object that is presented with the help of computer hardware and software.[43] An example of something that clearly falls into the category of judicial view in the digital context would be an interactive live demonstration of how a computer system or its user interface operates.[44] The technologies underlying the computer system are largely irrelevant for this classification, and attempts to interactively demonstrate the functioning of an AI-based system may thus also fall into the category of judicial view.

Chapter 17 of the Code of Judicial Procedure contains a relatively comprehensive set of procedural rules concerning hearings of parties and witnesses. In contrast, the presentation of documents and objects of judicial view is subject to minimal regulation: according to section 54, they shall be presented to the extent necessary in the main hearing; the same applies to written statements by expert witnesses. Details are left to the discretion of the presiding judge, and the exact manner of presentation may also depend on the availability of technological equipment, such as presentation screens, in the courtroom. As stated in section 39, copies of documents may be presented in the courtroom, unless the court orders a document to be presented in the original, typically in order to ensure or assess its authenticity and integrity.[45]

In practice, different types of evidence and means of presentation may be combined. This may even be necessary to guarantee that the evidence is vetted thoroughly and its meaning and probative value can be correctly understood and appropriately assessed. For example, raw input and output data processed by an AI-based system can be presented as documentary evidence, and an expert witness may clarify the functional principles of the AI-based system in question, interpret the meaning of

[42] For further discussion of this distinction and electronic evidence (including the classification of metadata relating to digital audiovisual recordings presented as evidence), see Juhana Riekkinen, *Sähköiset todisteet rikosprosessissa* (Alma Talent 2019) 378–383.

[43] Judicial view may also take place as a session outside of the courtroom, to allow judges to make direct sensory observations about a specific place, location, or environment.

[44] An example mentioned in the law drafting materials (Hallituksen esitys 46/2014 vp 100) is “an electronic registry, the operation of its administration software and ways of storing information into the registry”. The example refers to an earlier case in the Supreme Administrative Court (KHO 2009:39), which concerned problems with an electronic voting system.

[45] For digital documents, *originality* can be understood as integrity in the sense that the content and the format of the data have remained unchanged and unaltered. The concept of copies includes digitized copies of physical documents as well as paper printouts of digital documents or computer data that were originally produced with the help of computer systems.

the output, point out any potential weaknesses or sources of error, and give their expert assessment on the reliability of the information produced by the system in a written statement. Both the original documents and the written statement may be presented in the courtroom with the help of laptops and presentations screens, with parties highlighting and reading out loud relevant excerpts. After this, the expert may be heard and cross-examined in the courtroom. If there are several expert witnesses, it is possible to hear them concurrently.[46]

Chapter 17 of the Code of Judicial Procedure contains some general rules on admissibility. According to section 8, the court shall reject evidence that, *inter alia*, concerns a circumstance that is not relevant in the case, is otherwise unnecessary, or can be replaced by evidence that is essentially more credible[47].[48] Sections 10–23 contain provisions on various evidentiary privileges, such as doctor-patient and lawyer-client confidentiality and the privilege against self-incrimination. These provisions give parties and witnesses either the right or the duty not to answer certain questions, or to refuse to testify entirely. If a person has a right or duty not to answer a question, they are not obliged to present documents or objects regarding the same issues, either.[49] For the most part, these privileges do not bear any particular relevance for AI-produced evidence, but some AI-produced data may, of course, fall under some of these privileges in specific circumstances (e.g., data produced by an AI-based medical device used to treat a patient).

Further limitations on admissibility are set in section 25, which concerns exclusionary rules. First, evidence obtained through torture (subsection 1) or contrary to the privilege against self-incrimination (subsection 2)[50] may not be used. Subsection 3 concerns unlawfully obtained evidence in general, and states that "[i]n other cases the court may use also evidence that has been obtained unlawfully,

[46] Code of Judicial Procedure, c 17 s 50(1). Concurrent expert evidence or "hot-tubbing" in Finnish law has been discussed by Timo Saranpää, 'Asiantuntijat ammeeseen? Ajatuksia asiantuntijoiden vastakkainkuulustelusta ja sen toteuttamisesta' (2018) 99 Defensor Legis 1, 11–18.

[47] This can be understood as a form of the *best evidence rule* (although it is more like a principle than a strict rule). However, because the alternative evidence needs to be *essentially* more credible in order to warrant rejection of the proffered evidence, this provision is unlikely to lead to the rejection of any AI-related evidence in favor of evidence produced by a more reliable AI-based system, or in favor of unprocessed data that is not subject to possible sources of error introduced by AI-enabled processing. Exceptions to the right to present evidence should be construed narrowly, and a claim regarding more credible evidence is likely to lead to both of the competing pieces of evidence being presented and compared to each other.

[48] Furthermore, the court shall also reject evidence that can be replaced by evidence that is available with essentially less cost or difficulty, and evidence that despite appropriate measures could not be obtained.

[49] Code of Judicial Procedure, c 17 s 9(2).

[50] Beyond this one privilege specifically mentioned in s 25(2), the law is not perfectly clear on whether violations of other evidential privileges should automatically lead to exclusion of evidence, or if evidence erroneously presented in violation of these privileges should be subjected to the test set in s 25(3). Law drafting material suggests the first interpretation (Hallituksen esitys 46/2014 vp 92–93).

unless such use would endanger the conduct of a fair trial, taking into consideration the nature of the case, the seriousness of the violation of law involved in the obtaining of the evidence, the significance of the method in which the evidence was obtained in relation to its credibility, the significance of the evidence in respect of the decision in the case, and the other circumstances."[51] Even unlawfully obtained evidence may thus be used in criminal cases, unless this would lead to a violation of the defendant's right to a fair trial.

Consequently, the threshold for excluding AI-produced evidence, like any other evidence, is high. It is important to notice, however, that the applicability of subsection 3 does not require that the evidence in question has been obtained through a criminal offence – any unlawfulness will do.[52] The possible unfairness of the trial may need be considered in situations where the input data has been gathered illegally or without a legal basis, or where the use of the AI-based system can be otherwise considered illegal or unlawful. For instance, a minor violation of a data protection principle (e.g., data minimization or storage limitation), which might lead to administrative sanctions under the GDPR, would still be very unlikely to lead to exclusion, provided that such unlawful data processing ended up producing relevant evidence that can be considered reliable and credible.[53]

Some of the assessment criteria mentioned in subsection 3 do not bear any particular relevance in relation to AI-based systems, as AI-produced evidence can be proffered in all kinds of cases and have any level of significance in respect to the decision. Although credibility is a factor in the assessment, it should be noted that subsection 3 *only* concerns situations where evidence is unlawfully obtained—If no laws have been violated, any issues that give reason to question the credibility of the AI-produced evidence (whether they relate to the input data, the algorithm, or anything else) are to be considered when assessing the probative value of the evidence, but will not result in inadmissibility. On the other hand, as taking appropriate measures to ensure the integrity of personal data is a legal obligation of the controller and the processor under data protection law,[54] negligent data security practices that allow

[51] It should be noted that sub-ss 1 and 3 apply to all cases in the general courts, whereas sub-s 2 applies only to criminal cases.

[52] Hallituksen esitys 46/2014 vp 92–93.

[53] Cf. Oskari Paasikivi, 'Tietosuojasta vapaa todistelu? Todistelu siviiliprosessissa henkilötietojen suojan näkökulmasta' (Master's thesis, Helsinki University 2019) 30–31. The author, who discusses the relationship between data protection and evidence in civil proceedings, concludes that s 25(3) does not prevent the presentation of evidence that has been obtained in violation of data protection law, despite the broad meaning of "unlawfulness" and the fact that the provision is formally applicable in civil proceedings.

[54] GDPR, Articles 5(1)(f) and 32 and Act on the Processing of Personal Data in Criminal Matters, ss 9, 31 and 32.

tampering with or corruption of input data or data processing operations might (theoretically) be enough to make subsection 3 applicable.

Finally, it should be noted that the exclusionary rule in subsection 3 is particularly aimed at deterring misconduct by public officials. Law drafting documents suggest that the exclusion of credible evidence is not a desirable result in case of private misconduct, even when this private action amounts to a criminal offence.[55] However, this position has not been fully endorsed in legal commentary,[56] and criminal actions by private individuals have led to exclusion of evidence in earlier case law.[57] None of these sources of law address situations in which the illegal activity relates to the production of evidence with the help of AI-based systems, however. In the rapporteur's view, exclusion of evidence that has been produced by private entities using AI-systems in an illegal or unlawful manner is very unlikely, but cannot be ruled out categorically.

2.3 Evaluation of AI-produced evidence

Concerning evaluation of evidence, the Finnish system grants broad discretion to judges. There are no formal or categorical rules concerning the reliability, weight, or probative value of certain types or means of evidence. According to chapter 17, section 2(2) of the Code of Judicial Procedure, "[t]he court[58], having considered the evidence presented and the other circumstances that have been shown in the proceedings, determines what has been proven and what has not been proven in the case. The court shall consider the probative value of the evidence and the other circumstances thoroughly and objectively on the basis of free consideration of the evidence, unless provided otherwise in law." Notably, free consideration does not mean freedom to make arbitrary decisions or freedom from the general principles of

[55] Hallituksen esitys 46/2014 vp 94. Taking a more restrictive view, the Legal Affairs Committee stated that exclusion due to a criminal act by a private third party should only occur in "extremely exceptional cases" (Lakivaliokunnan mietintö 19/2014 vp 21).

[56] See, e.g., Mikko Vuorenpää, 'Muutama huomio laittomalla tavalla hankitun todistusaineiston hyödyntämisestä' (2018) 99 Defensor Legis 306, 312–313. Antti Jokela, *Pääkäsittely, todistelu ja tuomio. Oikeudenkäynti III* (Talentum 2015) 341 argues that legal practitioners should be held to the same standards as public officials. See also Pasi Pölönen and Antti Tapanila, *Todistelu oikeudenkäynnissä* (Tietosanoma 2015) 336–337 and Juhana Riekkinen, *Sähköiset todisteet rikosprosessissa* (Alma Talent 2019) 352–356.

[57] Court of Appeal of Eastern Finland, Judgment of 12 May 2010 (R 09/506, I-SHO 2010:5).

[58] In a criminal case, the court may consist of a single legally trained judge, a legally trained judge and (usually two) lay judges, or a panel of legally trained judges. In the Finnish system, lay judges are not restricted to merely deciding on the innocence or guilt of the defendant. They have independent decision-making power and right to vote equal to the legally trained judge. See the Judiciary website, Lay judges <https://oikeus.fi/tuomioistuimet/en/index/tuomioistuinlaitos/tuomioistuimet/yleisettuomioistuimet/karajaoikeudet/layjudges.html> accessed 28 March 2022.

scientific knowledge, logic, and reasoning. The court is also obligated to explain its reasoning on matters of evidence in the written judgment.[59]

Finnish legal commentary offers little insight into how AI-produced evidence should be evaluated in criminal cases, and indeed, there is little that can be said on a general level. The specific circumstances of the case, of the type of AI-produced evidence, and of each individual piece of evidence need to carefully considered. However, the rapporteur has argued for a general 'auxiliary questions' framework to assist triers of fact in assessing electronic evidence. This model places the emphasis on the origins of the data as well as the informational process that leads to the evidence being presented in a court of law. The aim is to identify or rule out different kinds of sources of error that relate to different aspects of digital data and to the processing of the data in question. The non-exhaustive list of auxiliary questions additionally serves as a checklist that may help parties in supporting their own evidence and challenging evidence presented by other parties.[60]

Applying this model, and in accordance with the general principles on the burden of proof and equality of arms,[61] a party wishing to introduce AI-produced evidence would need to support their evidence by presenting information about the functioning of the AI-based system in general and in the particular case, as well as information on subsequent processing of the data and measures taken to guarantee its integrity.[62] Unless the opposing party and the court are supplied with information that makes it possible to properly test the reliability of the system and of the data, such evidence should not be given significant weight by the court, especially when the AI-produced evidence is proffered by the prosecution in criminal cases. AI-produced evidence may not simply be presumed reliable and trustworthy, and the presumption of innocence must be guaranteed. If AI-produced evidence is presented in support of the innocence of the defendant, however, the requirements of providing supporting information should not be interpreted to be as stringent. Nevertheless, any information that enables the court to rule out sources of error that could diminish the credibility of potentially exonerating evidence will certainly help the defense case in practice.

[59] Criminal Procedure Act (689/1997), c 11 s 4(1): "The reasons for the judgment shall be stated. The statement of reasons shall indicate the factors and the legal reasoning on which the decision is based. The statement shall also indicate the basis on which a contentious issue has been proven or not proven." Code of Judicial Procedure, c 24 s 4 contains a similar obligation applicable to civil cases.

[60] See Juhana Riekkinen, 'Auxiliary Questions for Evaluating Electronic Evidence' (2019) Jusletter IT and Juhana Riekkinen, *Sähköiset todisteet rikosprosessissa* (Alma Talent 2019) 527–530.

[61] In criminal cases, the burden of proof is on the plaintiff regarding all circumstances on which their request for punishment is based, and the applicable standard of proof is "no reasonable doubt" regarding the guilt of the defendant (Code of Judicial Procedure, c 17 s 3).

[62] This can also be described as meta-level evidence relating to the reliability of the primary evidence.

3. Evidence assessed through AI-based systems

In Finland, judges are not known to use any AI-based systems to assess criminal evidence or its probative value. There is no legal basis for the use of such systems. The recently introduced case and document management system of the general courts, *AIPA*, contains no such functionality, nor does any other official information system currently or previously used by the courts. Consequently, there is no case law regarding decisions or judgements where such systems would have been (openly) used to assess evidence.

Under current Finnish law, it is clear that a person's guilt may not be determined by an AI-based system, and the introduction of any AI-based decision-making in criminal cases, especially in questions relating to evidence or culpability, seems highly unlikely even in the long term. Introduction of such a system would most likely require a constitutional amendment, as AI-based decision-making in such matters could be seen to contradict the provisions of the Constitution of Finland on procedural rights and protection under law (section 21) and the independence of courts (section 3(3)).[63] In general, Finnish discussion on automated decision-making in the public sector has predominantly focused on administrative decision-making in fields such as taxation,[64] and the automation of complex judicial decision-making is yet to be seriously discussed.[65]

From a legal point of view, the use of automated tools to support human decision-making is not as problematic as fully automated decision-making.[66] In the context of sentencing, a simple rule-based software tool, which can be used to analyze the criminal records of defendants, is reportedly already in use in several Finnish

[63] Further, Courts Acts (673/2016), c 9 s 1(1) states that "[a] judge is independent in the administration of justice and in this activity is subject only to the law".

[64] See, e.g., Jorma Kuopus, *Hallinnon lainalaisuus ja automatisoitu verohallinto* (Lakimiesliiton Kustannus 1988), and more recently, Hanne Hirvonen, 'Automatisoitu päätöksenteko julkisella sektorilla' (2018) 48 Oikeus 302 and Tuomas Pöysti, 'Kohti digitaalisen ajan hallinto-oikeutta' (2018) 116 Lakimies 868, 892–895.

[65] Notably, already Kaarle Makkonen discussed computational modelling of legal (and judicial) decision-making in his dissertation *Zur Problematik der juridischen Entscheidung: eine strukturanalytische Studie* (University of Turku 1965). More recently, use of AI in the courts has been discussed by Riikka Koulu, Risto Koulu and Sanna Koulu, *Tuomarin roolit tuomioistuimissa* (Alma Talent 2019) 178–188, 191 and Sanna Luoma, 'Artificial Intelligence Improving the Delivery of Justice and How Courts Operate' in Riikka Koulu and Laura Kontiainen (eds), *How Will AI Shape the Future of Law* (Legal Tech Lab, University of Helsinki 2019).

[66] Nevertheless, even simpler forms of automation and digitalization in the courts may bring about issues of legal significance, some of which have been point out by Riikka Koulu, 'Digitalisaatio ja algoritmit – oikeustiede hukassa?' (2018) 116 Lakimies 840, 847.

courts.[67] In the context of evidence, it could be argued that the use of AI-based support systems might help judges to map out the relations between different pieces of evidence, to structure their reasoning on matters of evidence, and consequently, to write better and more logically sound judgments. Further, as judges already have broad discretion in evaluating evidence, it could be argued that as long as the judgment openly elaborates on how AI-based systems have been used to help in assessing the evidence, or at least describes the logic utilized by the AI-based system as understood by the human decision-maker, this would be permissible.[68] For the moment, however, the availability of easy-to-use and proven-to-be-reliable AI-based evidence management or decision support tools seems scarce, and therefore their adoption by Finnish judges—especially in the absence of parliamentary or other high-level institutional approval—seems unlikely in the near future.[69]

A further argument against the likelihood of adoption of software tools for evaluation of evidence is the fact that Bayesian and other mathematical theories of evidence (the logic of which can easily be expressed in code)[70] seem to have gained very limited acceptance among Finnish judges and other legal professionals, although they have been discussed in domestic literature for decades.[71] As mathematical models are not generally relied on, judges would probably be somewhat reluctant to accept probabilities, likelihood ratios, probative values, or any other numerical values calculated by a software tool. Moreover, as the case law of the Supreme Court of Finland does not approach the definition of the standard of proof in criminal cases in terms of mathematical probabilities, but instead by

[67] Juha Terho, 'Automaattinen päätöksenteko ratkaisuna konkurrenssin katkeamiseen liittyviin ongelmiin' (2022) 103 Defensor Legis 106. According to Criminal Code, c 7 s 6, the court may need to consider earlier sentences of imprisonment in sentencing. The interpretation of this provision has been clarified by the Supreme Court (KKO 1972 II 5 and KKO 2004:130), and the tool seeks to model and automatize this 'algorithm' determined in case law. The tool itself, *Konkurrenssikone*, is available at GitHub <https://github.com/konkurrenssikone> accessed 28 March 2022.

[68] Machine learning approaches typically suffer from limitations related to explainability (as well as various biases) that would be unacceptable in criminal proceedings. Adoption of support tools based on machine leaning is effectively prevented by the legal obligation to provide reasoning concerning the basis on which a contentious issue has been proven or not proven (Criminal Procedure Act, c 11 s 4(1)).

[69] If the approval for such a system is not derived from a parliamentary act, this could be seen as problematic in regard to Courts Acts, c 9 s 1(1) and the principle of legality. In any case, simple visualization tools that do not provide any conclusions or numerical values but allow for easier structuring of relationships between individual pieces of evidence and *facta probanda* could be the most realistically adoptable type of support software.

[70] Of course, this is not to say that software tools would necessarily need to be limited to mathematical models.

[71] See, e.g., Hannu Tapani Klami, Minna Gräns and Johanna Sorvettula, *Law and Truth: A Theory of Evidence* (Finnish Society of Sciences and Letters 2000).

focusing on alternative hypotheses or explanations,[72] such numerical values would be, ultimately, of limited use without a wider reform of law of evidence.

References

Cases

The Court of Justice of European Union

Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministres* [2022]

The Supreme Court of Finland

KKO 2013:96, KKO 1972 II 5, KKO 2004:130

Court of Appeal of Eastern Finland

Judgment of 12 May 2010 (R 09/506, I-SHO 2010:5)

Supreme Administrative Court

KHO 2009:39

[72] See, e.g., KKO 2013:96, para 6. The approach of the Finnish courts is largely characterized by non-mathematical theories of evidence, such as the hypothesis model proposed by Christian Diesen, *Bevisprövning i brottmål* (Juristförlaget 1994) 120–151.

National non-discrimination and equality tribunal of Finland 216/2017, date of issue 21 March 2018 <https://www.yvtltk.fi/en/index/opinionsanddecisions/decisions.html> accessed 29 December 2021

Decision of the Deputy-Ombudsman of the Parliament (EOA 1634/4/01) 18 December 2003 <https://www.oikeusasiamies.fi/r/fi/ratkaisut/-/eoar/1634/2001> accessed 29 December 2021

Data Protection Ombudsman, Decision, 20 September 2021, 3394/171/21

Legislation

Act on Crime Prevention by the Border Guard (108/2018)

Act on Crime Prevention by the Customs (623/2015)

Act on Electronic Communications Services (917/2014)

Act on Information Management in Public Administration (906/2019)

Act on Military Discipline and Combating Crime in the Defence Forces (255/2014)

Act on the Openness of Government Activities (621/1999)

Act on the Processing of Personal Data by the Border Guard (639/2019)

Act on the Processing of Personal Data by the Customs (650/2019)

Act on the Processing of Personal Data by the Defence Forces (332/2019)

Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018). An informal translation into English is available from the website of the Ministry of Justice: https://www.finlex.fi/fi/laki/kaannokset/2018/en20181054.pdf

Code of Judicial Procedure (4/1734)

Coercive Measures Act (806/2011)

Constitution of Finland (731/1999)

Council of Europe Convention on Cybercrime (ETS No 185, 2001)

Courts Acts (673/2016)

Criminal Code of Finland (39/1889)

Criminal Investigation Act (805/2011)

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

European Convention on Human Rights

Police Act (872/2011)

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Bibliography

Annual report of the Financial Intelligence Unit (2020) <https://poliisi.fi/documents/25235045/67733116/2020-Rahanpesun-selvittelykeskus-vuosikertomus-2020.pdf/e340331f-f04c-7eec-2756-111628ae368a/2020-Rahanpesun-selvittelykeskus-vuosikertomus-2020.pdf?t=1617010848853> accessed 29 December 2021

Annual report of the Border Guard (2020) <https://raja.fi/documents/44957406/64377821/Tilinp%C3%A4%C3%A4t%C3%B6s_2020.pdf/d7f4c8ec-92ce-fe60-0825-

b45e209fd4c1/Tilinp%C3%A4%C3%A4t%C3%B6s_2020.pdf?t=1615290408994> accessed 29 December 2021

Andrew Ashworth and Lucia Zedner, Preventive Justice, Oxford University Press, Oxford 2014; Jan W. de Keijser, Julian V. Roberts and Jesper Ryberg (eds.), Predictive Sentencing. Normative and Empirical Perspectives, Hart Publishing, Oxford 2019.

M. Botvinick (2007). Multilevel structure in behaviour and in the brain: a model of Fuster's hierarchy. Philosophical Transactions of the Royal Society B, 362(1485), 1615-26. https://doi.org/10.1098/rstb.2007.2056

Diesen Christian, Bevisprövning i brottmål (Juristförlaget 1994)

Y. Duan, J. Schulman, X. Chen, P. Bartlett, I. Sutskever & P. Abbeel (2016). RL2: fast reinforcement learning via slow reinforcement learning. arXiv. 2016: 1611.02779. https://arxiv.org/abs/1611.02779

Ekfeldt Jonas, Om informationstekniskt bevis (Juridiska institutionen, Stockholms universitet 2016)

Ervo Laura, Oikeudenkäynnin oikeudenmukaisuusvaatimus: Käsikirja lainkäyttäjille [The requirement of fairness of the proceedings: Handbook for judicial decision-makers] (WSOYPro 2008)

European Commission (2021b). Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Fostering a European approach to Artificial Intelligence. Coordinated Plan on Artificial Intelligence 2021 Review. COM(2021) 205 final, ANNEX. 21 April 2021, Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0205

European Commission (2021a). Proposal for a Regulation of the European Parliament and of the Council. Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM(2021) 206 final, 2021/0106(COD). European Commission, Directorate-General for Communications Networks, Content and Technology, 21 April 2021, Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European data protection supervisor, Request for an Opinion by the European Parliament, draft EU-Canada PNR agreement (Opinion 1/15) Hearing of 5 April 2016 Pleading notes of the European Data Protection Supervisor (EDPS)

<https://edps.europa.eu/sites/default/files/publication/16-04-05_pleading_canada_pnr_en.pdf> accessed 27 December 2021

Fredman Markku, Rikosasianajajan käsikirja [Criminal attorney's handbook] (2nd edn, Alma Talent 2021)

E. van Ginneken, The Use of Risk Assessment in Sentencing, in: Predictive Sentencing. Normative and Empirical Perspectives (supra note 3), pp. 9-32, at 26.

Government Proposal on amending the Coercive Measures Act and the Criminal Investigation Act (HE 217/2022 vp)

Government Proposal on the evidence law renewal (HE 46/2014 vp)

Government Proposal on the PNR legislation (HE 55/2018 vp)

Government Proposal on the Police Act (HE 224/2010 vp)

M. Haataja, M. Latvanen and the AuroraAI's ethics network (no date). AuroraAI-esiselvityshanke : Etiikka-työkokonaisuuden suositukset. [AuroraAI pre-investigation project : Recommendations of the ethics work entity.] Meeri Haataja (Saidot), Marko Latvanen (VRK) and the AuroraAI's ethics network. https://vm.fi/documents/10623/13292513/AuroraAI+esiselvityshanke+-+Etiikka-suositukset.pdf/e1737144-14bd-8dec-e706-db8a963b6cc7/AuroraAI+esiselvityshanke+-+Etiikka-suositukset.pdf

Hakkarainen Jenni, Koulu Riikka and Markkanen Kalle, 'Läpinäkyvät algoritmit? lähdekoodin julkisuus ja laillisuuskontrolli hallinnon digitalisaatiossa' [Transparent algorithms? Openness of the source code and the control of legality in the digitalisation of administration] Edilex 2020/18 <https://www.edilex.fi/artikkelit/21042.pdf> accessed 29 December 2021

Hirvonen Hanne, 'Automatisoitu päätöksenteko julkisella sektorilla' [Automated decision-making in the public sector] (2018) Oikeus 47(3) 302

Hoidon perusteet (2022). Emergency care requirement guidance library provided by DigiFinland Oy with the coordination and assignment given by the Ministry of Social Affairs and Health. In Finnish. https://hoidonperusteet.fi/static/instructions and https://116117.fi/hoidonperusteet/

Joh Elizabeth E., 'Feeding the Machine: Policing, Crime Data, & Algorithms' (2017) 26 Wm. & Mary Bill Rts. J. 287

Jokela Antti, Pääkäsittely, todistelu ja tuomio. Oikeudenkäynti III [Main hearing, evidence and judgment. Trial III] (Talentum 2015)

M. Karim, O. Beyan, A. Zappa, I. Costa, D. Rebholz-Schuhmann, M. Cochez & S. Decker (2021). Deep learning-based clustering approaches for bioinformatics. Briefings in Bioinformatics, Volume 22, Issue 1, January 2021, pp. 393–415. https://doi.org/10.1093/bib/bbz170

J. De Keijser et al., Introduction, in: Predictive Sentencing. Normative and Empirical Perspectives (supra note 3), pp. 1-8, at 2.

Klami Hannu Tapani, Gräns Minna and Sorvettula Johanna, Law and Truth: A Theory of Evidence (Finnish Society of Sciences and Letters 2000)

R. Koivisto, J. Leikas, H. Auvinen, V. Vakkuri, P. Saariluoma, J. Hakkarainen & R. Koulu (2019). Artificial intelligence in authority use - ethical and societal acceptance issues. [Tekoäly viranomaistoiminnassa - eettiset kysymykset ja yhteiskunnallinen hyväksyttävyys.] Publications of the Government's analysis, assessment and research activities 14/2019. Prime Minister’s Office. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161345/14-2019-Tekoaly%20viranomaistoiminnassa.pdf

Korff Douwe and Georges Marie, Passenger Name Records, data mining & data protection: the need for strong safeguards. Executive summary. Council of Europe. The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-Pd) Strasbourg, 15 June 2015. <https://rm.coe.int/16806b1761> accessed 27 December 2021

Koulu Riikka, ‘Digitalisaatio ja algoritmit – oikeustiede hukassa?’ [Digitalisation and algorithmic decision making – jurisprudence at a crossroads?] (2018) 116 Lakimies 840, pp. 840-867.

Koulu Riikka, Koulu Risto and Koulu Sanna, Tuomarin roolit tuomioistuimissa [The roles of the judge in courts] (Alma Talent 2019)

Koulu Riikka, Mäihäniemi Beata, Kyyrönen Vesa, Hakkarainen Jenni and Markkanen Kalle, Algoritmi päätöksentekijänä?: Tekoälyn hyödyntämisen mahdollisuudet ja haasteet kansallisessa sääntely-ympäristössä [An algorithm as a decision-maker ?: Opportunities and challenges of utilizing artificial intelligence in the national regulatory environment] (Government’s publication series 2019:44) 122–123 <https://julkaisut.valtioneuvosto.fi/handle/10024/161700> accessed 29 December 2021

Kritsos Anita, ‘Algoritmisten päätöksentekojärjestelmien soveltaminen rikoksentekijän vaarallisuutta koskevassa tuomarin päätöksenteossa’ [The application of algorithmic decision-making systems in judicial decision-making concerning dangerousness of the offender] (Master's thesis, Helsinki University 2019)

Kroll Joshua A, Huey Joanna, Barocas Solon, Felten Edward W, Reidenberg Joel R, Robinson David G and Yu Harlan, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review 633 <https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3> accessed 29 December 2021

Kuopus Jorma, Hallinnon lainalaisuus ja automatisoitu verohallinto [The Rule of Law and Computerized Administration of Taxation] (Lakimiesliiton Kustannus 1988)

M. Kuziemski & G. Misuraca (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. Telecommunications policy, 44(6), 101976, July 2020. https://doi.org/10.1016/j.telpol.2020.101976

Lauri Lahti (2022). Challenges of developing personalized artificial intelligence for public services. 1 August 2022. A self-archived research article manuscript available with open access at https://aaltodoc.aalto.fi

Lauri Lahti (2022a). Detecting the patient's need for help with machine learning based on expressions. BMC Medical Research Methodology, Volume 22, article number 60, 2022. This research article is supplemented with two supplementing documents. https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/s12874-021-01502-8 and https://doi.org/10.1186/s12874-021-01502-8

Lauri Lahti (2022c). Developing ethical and transparent artificial intelligence algorithms to support decision making in healthcare based on brain research and personal care events of patients. Research article manuscript self-archived on 15 July 2022 at https://aaltodoc.aalto.fi/handle/123456789/115565 . Open access: http://urn.fi/URN:NBN:fi:aalto-202207154400

Lauri Lahti (2022b). Developing patient-driven artificial intelligence based on personal rankings of care decision making steps. A research article manuscript completed and self-archived on 11 May 2022 on the open-access Arxiv repository (https://arxiv.org/abs/2205.07881). This manuscript (104 pages) is supplemented with seven supplementing documents (2781 pages). Open access: https://arxiv.org/pdf/2205.07881 and https://doi.org/10.48550/arXiv.2205.07881

Lauri Lahti (2020). Interpretation of the patient's need for help can be supported with machine learning. In Juli Mansnérus, Raimo Lahti & Amanda Blick (eds.), Personalized medicine: legal and ethical challenges. Faculty of Law, University of Helsinki, Finland, Forum Iuris Series, Helsinki, Finland, 2020. ISBN 978-951-51-6940-2 (printed), ISBN 978-951-51-5021-9 (online). Open access: https://doi.org/10.31885/9789515169419

Raimo Lahti, Life Imprisonment and Other Long-Term Sentences in the Finnish Criminal Justice System: Fluctuations in Penal Poliy, in Khalid Ghanayim and Yuval Shany (eds.), The Quest for Core Values in the Application of Legal Norms. Essays in Honor of Mordechai Kremnitzer, Springer, Cham 2021, pp. 201-217, at 204-205.

Raimo Lahti (2012). Medical law and biolaw. In K. Nuotio, S. Melander, S., & M. Huomo-Kettunen,(eds.), Introduction to Finnish Law and Legal Culture. Faculty of Law, University of Helsinki, Helsinki, Finland. Forum Iuris Series, Helsinki, Finland, 2012, pp. 249-260. ISBN 978-952-10-7817-0. Reprinted in the compilation publication: Raimo Lahti (2021). Towards an Efficient, Just and Humane Criminal Justice: Nordic Essays on Criminal Law, Criminology and Criminal Policy 1972-2020. Publications of the Finnish Lawyers' Association, Series D (Ius Finlandiae), No. 8, pp. 528-541, The Finnish Lawyers' Association, Helsinki, Finland, 2021. ISBN 978-951-855-386-4 (printed), ISBN 978-951-855-387-1 (online). Open access: https://edition.fi/lakimiesyhdistys/catalog/book/121

T. Lappi-Seppälä, Life Imprisonment and Related Institutions in the Nordic Countries, in D. van Zyl Smit & C. Appleton (Eds.), Life Imprisonment and Human Rights (Hart Publishing, Oxford 2016), pp. 461-505, at 500.

L. Laranjo, A. Dunn, H. Tong, A. Kocaballi, J. Chen, R. Bashir, D. Surian, B. Gallego, F. Magrabi, A. Lau & E. Coiera (2018). Conversational agents in healthcare: a systematic review. Journal of the American Medical Informatics Association, 2018;25(9):1248-1258. https://doi.org/10.1093/jamia/ocy072

J. Leikas, A. Johri, M. Latvanen, N. Wessberg & A. Hahto (2022). Governing Ethical AI Transformation: A Case Study of AuroraAI. Frontiers in Artificial Intelligence, 5:836557, 2022. https://doi.org/10.3389/frai.2022.836557

Letter to the author on 17 November 2021 (POL-2021-127171)

Y. Lu, C. Phillips & M. Langston (2019). A robustness metric for biological data clustering algorithms. BMC Bioinformatics 20, 503 (2019). https://doi.org/10.1186/s12859-019-3089-6

Luoma Sanna, 'Artificial Intelligence Improving the Delivery of Justice and How Courts Operate' in Riikka Koulu and Laura Kontiainen (eds), How Will AI Shape the Future of Law (Legal Tech Lab, University of Helsinki 2019)

J. Lähesmaa, J. Reponen, H. Anttila (eds.) (2021). Hyteairon pyöreän pöydän julkilausuman tausta ja yhteisesti kirjoitetut ratkaisuehdotukset: Terveys- ja hyvinvointiteknologioiden arviointi ja korvattavuus sosiaali- ja terveyspalveluiden asiakkaille. [Background and collectively written solution proposals of the public statement of the Hyteairo's round table: Assessment of the health and wellbeing technologies and their substitutability for the customers of the social affairs and health services.] Based on the meetings 14-17 June 2021. https://thl.fi/documents/10531/5914371/Hyteairon+py%C3%B6re%C3%A4n+p%C3%B6yd%C3%A4n+julkilausuma+14_17.6.2021-+pitk%C3%A4+versio_logo+ok.pdf

Makkonen Kaarle, Zur Problematik der juridischen Entscheidung: eine strukturanalytische Studie (University of Turku 1965)

Ministry of Finance (2020). Asettamispäätös VN/1332/2020. Kansallinen tekoälyohjelma AuroraAI. [Appointment decision VN/1332/2020. National Artificial Intelligence Programme AuroraAI.] Ministry of Finance. https://vm.fi/documents/10623/16264993/aurora+asettamispaatos+korjattu.pdf/fd7831ba-d4b8-d0a8-e7f2-9cb38407c698/aurora+asettamispaatos+korjattu.pdf

Ministry of Finance (2021). AuroraAI-ohjelma 2020-2022. Toimintasuunnitelma 2022. [AuroraAI program 2020-2022. Action plan 2022.] VN/1332/2020. 25.11.2021. Ministry of Finance. https://vm.fi/documents/10623/89568191/AuroraAI-ohjelman+toimintasuunnitelma+2022.pdf/e80d88db-ed11-267d-3f27-d9d0e8ca4067/AuroraAI-ohjelman+toimintasuunnitelma+2022.pdf

Ministry of Finance (no date). National Artificial Intelligence Programme AuroraAI. [Kansallinen tekoälyohjelma AuroraAI.] Ministry of Finance. https://vm.fi/en/national-artificial-intelligence-programme-auroraai and https://vm.fi/tekoalyohjelma-auroraai

Ministry of Social Affairs and Health (2022). Hyteairo - Hyvinvoinnin tekoäly ja robotiikka -ohjelma : loppuraportti 2022. [Hyteairo - Well-being and Health Sector's Artificial Intelligence and Robotics Programme : final report 2022.] Ministry of Social Affairs and Health. https://urn.fi/URN:NBN:fi-fe2022021619558

Ministry of Social Affairs and Health (no date). The Well-being and Health Sector's Artificial Intelligence and Robotics Programme (Hyteairo). [Hyvinvoinnin tekoäly ja robotiikka -ohjelma Hyteairo.] Ministry of Social Affairs and Health. https://stm.fi/en/the-well-being-and-health-sector-s-artificial-intelligence-and-robotics-programme-hyteairo- and https://stm.fi/hyteairo

Ministry of the Interior, Finland's Strategy on Preventive Police Work 2019–2023 (Publications of the Ministry of the Interior 2019:11) <https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161343/SM_11_19_Strat

egy%20on%20preventive%20police%20work.pdf?sequence=1&isAllowed=y> accessed 27 December 2021

G. Misuraca & C. Van Noordt (2020). Overview of the use and impact of AI in public services in the EU. AI Watch : artificial intelligence in public services. Science for Policy Report. EUR 30255 EN. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120399/jrc120399_misuraca-ai-watch_public-services_30062020_def.pdf

Opinion of the Data Protection Ombudsman for the Constitutional Law Committee on 10 September 2018 <https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-203144.pdf> (accessed 29 December 2021).

Opinion of the National Bureau of Investigation on data processing in the police on 10 January 2019 <https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2019-AK-236903.pdf> accessed 29 December 2021

Opinion of a senior officer for the Administrative Committee on 7 January 2019 <https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2019-AK-235519.pdf> (accessed 29 December 2021)

Ortamo Simo, 'Poliisi on saanut rikollisia kiinni kasvoja tunnistavan tekoälyn avulla ja haluaisi laajentaa valtuuksiaan – testasimme, miten kone toimii' [The police have apprehended criminals using a facial recognition artificial intelligence and would like to expand their powers – we tested how the machine works] Yle Uutiset (1 August 2020) <https://yle.fi/uutiset/3-11448002> accessed 28 March 2022

Owal Group and 4Front (2022). AuroraAI-ohjelma. Arviointiraportti. Väliarviointi, 10.1.2022. [AuroraAI program. Evaluation report. Mid-term evaluation, 10.1.2022.] A report implemented collaboratively by Owal Group Oy and 4Front Oy by the appointment of Ministry of Finance. https://vm.fi/documents/10623/101263033/AuroraAI+v%C3%A4liarviointiraportti.pdf/c2bd5500-9588-251d-7155-b0a713ecb69b/AuroraAI+v%C3%A4liarviointiraportti.pdf

Paasikivi Oskari, 'Tietosuojasta vapaa todistelu? Todistelu siviiliprosessissa henkilötietojen suojan näkökulmasta' Evidence free from data protection? Evidence in civil proceedings from the perspective of data protection] (Master's thesis, Helsinki University 2019)

Pellonpää Matti, Gullans Monica, Pölönen Pasi and Tapanila Antti, Euroopan ihmisoikeussopimus [European Convention on Human Rights] (6th edn, Alma Talent 2018)

Perry Walter L, McInnis Brian, Price Carter C, Smith Susan C and Hollywood John S, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations (1st edn, RAND Corporation 2013)

M. Perälä-Heape & V. Virta (2021). Tekoäly sote-tiedolla johtamisessa. Tilannekuvaraportti. [Artificial intelligence in directing with social affairs and health information. Situation description report.] December 2021. Centre for Health and Technology, University of Oulu. https://thl.fi/documents/10531/6281814/Tilannekuvaraportti+Teko%C3%A4ly+sote-tiedolla+johtamisessa+-+s.pdf

Pietiläinen Tuomo, 'Supo haluaa lisää oikeuksia tiedustella salaa – laillisuusvalvojat täsmentäisivät nykyisiä tiedustelulakeja' [The Finnish Security and Intelligence Service wishes to widen its intelligence powers – The supreme overseers of legality in Finland would clarify the current legislation] Helsingin Sanomat (23 November 2021) <https://www.hs.fi/politiikka/art-2000008422934.html> accessed 29 December 2021

Pietiläinen Tuomo, 'Poliisi haluaa puhelinkuuntelun ja muita salaisia keinoja käyttöön ilman rikosepäilyä – sisäministeriö aloittaa esiselvityksen' [The police wishes to use phone tapping and other secret methods of gathering intelligence without suspicion of crime – The Ministry of the Interior initiates preparatory study] Helsingin Sanomat (18 November 2021) <https://www.hs.fi/politiikka/art-2000008414156.html> accessed 29 December 2021

Pohjola Annakaisa, Vaarallinen rikoksentekijä? Tutkimus rikoksentekijän vaarallisuuden arvioinnista rikosoikeudellisessa seuraamusjärjestelmässä [Dangerous offender? A Study on offender risk assessment within the Finnish penal system] (Suomalainen Lakimiesyhdistys, Helsinki, 2017)

Police reprimand from Deputy Data Protection Ombudsman – police have initiated measures ordered' (28 September 2021) <https://poliisi.fi/en/-/police-reprimand-from-deputy-data-protection-ombudsman-police-have-initiated-measures-ordered> accessed 28 March 2022

Poliisi panostaa rikosten ehkäisemiseen ja paljastamiseen [The police invest in crime prevention and detection] <https://poliisi.fi/-/poliisi-panostaa-rikosten-ehkaisemiseen-ja-paljastamiseen> accessed 27 December 2021

Poliisiylijohtaja Seppo Kolehmainen muistutti poliisien valatilaisuudessa: Poliisin pysyttävä mukana muutoksessa [The National Police Commissioner Seppo Kolehmainen reminded at the police swearing-in: The police have to stay on top of the change] <https://poliisi.fi/-/poliisiylijohtaja-seppo-kolehmainen-muistutti-poliisien-valatilaisuudessa-poliisin-pysyttava-mukana-muutoksessa> accessed 29 December 2021

Pölönen Pasi and Tapanila Antti, Todistelu oikeudenkäynnissä [Evidence in the trial] (Tietosanoma 2015)

Pöysti Tuomas, 'Kohti digitaalisen ajan hallinto-oikeutta' [Towards administrative law in the digital era] (2018) 116 Lakimies 868

Rautio Lauri et al., Pakkokeinolain muutostarpeiden tarkastelu: Työryhmämietintö [Examination of the needs for amending the Coercive Measures Act: Report of the Working Group] (Ministry of Justice 2022)

Report of the Administrative Committee (HaVM 42/2018 vp)

Report of the Legal Affairs Committee (LaVM 19/2014 vp)

Report by Rikostorjunnan tila -selvityshanke and Tero Kurenmaa, Rikostorjunnan tila -selvityshankkeen loppuraportti [The final report of the study project on the Status of Crime-prevention in Finland] (The publication series of the National Police Board of Finland 1/2018) 45 <https://poliisi.fi/julkaisut/-/asset_publisher/Ga8MkKWl5ss3/content/rikostorjunnan-tila-selvityshankkeen-loppuraportti?_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_Ga8MkKWl5ss3_assetEntryId=43809202> accessed 29 December 2021

Report by Valvonta- ja hälytystoiminnan selvityshanke and Arto Karnaranta, Valvonta- ja hälytystoiminnan tila -selvityshankkeen loppuraportti (The publication series of the National Police Board of Finland 3/2019)

Riekkinen Juhana, Sähköiset todisteet rikosprosessissa [Electronic Evidence in Criminal Procedure] (Alma Talent 2019)

Riekkinen Juhana, 'Auxiliary Questions for Evaluating Electronic Evidence' (2019) Jusletter IT

Riekkinen Juhana, 'Evidence of Cybercrime and Coercive Measures in Finland' (2016) 13 Digital Evidence and Electronic Signature Law Review 49

S. Ritter, J. Wang, Z. Kurth-Nelson, S. Jayakumar, C. Blundell, R. Pascanu & M. Botvinick (2018). Been there, done that: meta-learning with episodic recall.

International Conference on Machine Learning. 2018: 4351-4360. https://proceedings.mlr.press/v80/ritter18a/ritter18a.pdf

Strategy and Action Plan for Tackling the Grey Economy and Economic Crime <https://www.vero.fi/en/grey-economy-crime/prevention/torjuntaohjelma/> accessed 29 December 2021

Sutela Mika, 'Tiedon, analyysin ja analytiikan hyödyntämisen tarve poliisissa – ilmeinen ja suuri?' [The need for the police to use information, analysis and analytics – obvious and great?] (Official blog of the police, 15 September 2019) <https://poliisi.fi/blogi/-/blogs/tiedon-analyysin-ja-analytiikan-hyodyntamisen-tarve-poliisissa-ilmeinen-ja-suuri-> accessed 29 December 2021

Syngelmä Vesa, 'Ennustamisteknologioiden hyödyntämismahdollisuudet osana ennakoivaa poliisitoimintaa' [The opportunities for using predictive technologies as a part of predictive policing] (Master's thesis, Tampere University 2021) <https://trepo.tuni.fi/handle/10024/130523> accessed 27 December 2021

Söderholm Sofia, Potentiaalisen rikoksentekijän asema ja oikeus syyttömyysolettamaan ennakoivassa poliisitoiminnassa [The Legal Status of a Potential Offender and her Right to the Presumption of Innocence in the Context of Predictive Policing] (Legal Tech Lab 2020) <https://helda.helsinki.fi/handle/10138/331782> accessed 29 December 2021

Terho Juha, 'Automaattinen päätöksenteko ratkaisuna konkurrenssin katkeamiseen liittyviin ongelmiin' [Automated decision-making as a solution to problems relating to how earlier sentences are taken into account] (2022) 103 Defensor Legis 106

Testing of facial recognition software by NBI reported to Data Protection Ombudsman' (9 April 2021) <https://poliisi.fi/en/-/testing-of-facial-recognition-software-by-nbi-reported-to-data-protection-ombudsman> accessed 28 March 2022

Matti Tolvanen et al., Vaarallisuuden ja väkivaltariskin arvioiminen [Assessment of the Risk of Danger and Violence]- Publications of the Government's analysis, assessment and research activities 2021:70, Helsinki 2021 (Abstract).

M. Tonry, Sentencing and Prediction. Old Wine in Old Bottles, in Predictive Sentencing. Normative and Empirical Perspectives (supra note 3), pp. 269–298, at 290–291.

D. Townend, C. Clemens, D. Shaw, H. Brand, H. Nys, & W. Palm (2016). Patients' rights in the European Union: mapping exercise: final report. Written by PRE-MAX Consortium, March 2016. European Commission, Directorate-General for Health and Food Safety, 2018. Publications Office. Published 25 January 2018. ISBN 978-92-79-66960-6. https://data.europa.eu/doi/10.2875/751285

Ulosottolaitoksen hankkeet RATKE ja Harmaa hyödyntävät uutta teknologiaa [The projects RATKE and Harmaa of the National Enforcement Authority Finland make use of new technologies] (21 December 2021) <https://ulosottolaitos.fi/fi/index/ulosottolaitos/ajankohtaista/verkkouutisetjatiedotteet/uutiset2021/ulosottolaitoksenhankkeetratkejaharmaahyodyntavatuuttateknologiaa.html> accessed 29 December 2021

Vainio Niklas, Tarkka Valpuri and Jaatinen Tanja, Arviomuistio hallinnon automaattiseen päätöksentekoon liittyvistä yleislainsäädännön sääntelytarpeista [Memorandum on the reform the administrative legislation for automated decision-making] (Publications of the Ministry of Justice 2020:14) 44 <https://api.hankeikkuna.fi/asiakirjat/ff3444f4-24c9-4ee8-8c9d-7bc581c0021a/e034bf5c-e2bd-4245-a626-9b679b2144ff/LAUSUNTOPYYNTO_20210609083824.PDF> accessed 29 December 2021.

Valtioneuvoston periaatepäätös kansalliseksi harmaan talouden ja talousrikollisuuden torjunnan strategiaksi ja toimenpideohjelmaksi 2020–2023 [The Decision in Principle on the National Strategy and Action Plan for Tackling the Grey Economy and Economic Crime taken by the Finnish Government]

Voutilainen Tomi, ICT-oikeus sähköisessä hallinnossa [ICT law in e-government] (Edita 2009)

Vuorenpää Mikko, 'Muutama huomio laittomalla tavalla hankitun todistusaineiston hyödyntämisestä' [A few observations on the admissibility of unlawfully obtained evidence] (2018) 99 Defensor Legis 306

J. Wang, Z. Kurth-Nelson, D. Kumaran, D. Tirumala, H. Soyer, J. Leibo, D. Hassabis & M. Botvinick (2018). Prefrontal cortex as a meta-reinforcement learning system. Nat. Neurosci. 2018; 21: 860-868. https://doi.org/10.1038/s41593-018-0147-8

J. Wang, Z. Kurth-Nelson, D. Tirumala, H. Soyer, J. Leibo, R. Munos, C. Blundell, D. Kumaran & M. Botvinick (2016). Learning to reinforcement learn. arXiv. 2016; 1611.05763. https://arxiv.org/abs/1611.05763