http://dx.doi.org/10.12775/CLR.2024.001

Ammar Alqatawna*

UTILIZING ARTIFICIAL INTELLIGENCE (AI) IN CRIMINAL JUSTICE AND POLICING

Abstract

The use of AI in criminal justice and policing has significantly increased in EU countries. AI tools are being used in various phases of a criminal case, from police tasks to those of judges. While the use of AI in criminal justice is impressive in certain areas, it poses serious challenges and concerns, including potential violations of fundamental rights. This paper examines the risks of using AI in criminal justice, addresses the current use of some AI systems, and explores how the legal framework within the EU regulates its use, including EU directive 2016/680 and the projected AI Act.

Keywords

AI; criminal justice; risks of AI; AI and human rights; AI and policing

Introduction

Day after day, AI proves to be the next most powerful technology. The power of AI makes a stupendous variation in effectiveness, timesaving, and effort regarding many aspects of our lives, such as the criminal justice system. The AI tool mechanism is suitable for criminal justice use by judges, enforcement authorities, and police departments. The abilities of data analysis, experience learning, and powerful algorithms

* PhD student, University of Miskolc, ORCID 0009-0000-5874-6065, ammar.qataw-neh@yahoo.com.

could make a huge variation in criminal justice, such as predictive policing, investigative analysis, evidence analysis, risk assessment, and sentencing.

However, the use of AI did not realize the height of its ambitions owing to some practical reasons. Some of these reasons are related to existing problems in the mechanism of AI tools, such as bias of data and a lack of transparency and ability to explain its outcomes. All of these concerns affect the nature and principles of criminal justice, and are directly or indirectly related to violations of fundamental rights, such as the right to protection of personal data, the right to non-discrimination, and the right to a fair trial. AI usage is increasing in Europe, but regulations are still being developed. It is crucial to address this before AI becomes more deeply integrated into the criminal justice system, in order to ensure its proper use.

This paper provides an overview of using artificial intelligence in criminal justice and policing in Europe. The first part offers a simplified explanation of AI, while the second portion delves into the potential risks associated with its use. The third part investigates how AI is currently used in criminal justice and policing in some European countries. The final section tackles the legal framework for implementing AI in criminal justice within the European Union, including EU Directive 2016/680 and the projected AI Act.

I. Overview of artificial intelligence

Artificial intelligence is not magic.[1] It is a field of computer science that the European Commission defined as "systems that display intelligent behaviour by analysing their environment and taking action with some degree of autonomy to achieve specific goals".[2] AI is not a single system or technology, but a collection of combined technologies that work

---

[1] A. Amarendar Reddy, *Legal Implications in Artificial Intelligence*, "International Journal of Law Management & Humanities", Issue 4, 2022, p. 1776.

[2] European Commission (2018). 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 - Coordinated Plan on Artificial Intelligence (COM(2018) 795 final). Brussels: European Commission, available at: https://eur-

together to achieve a goal. One of the main benefits of AI is its ability to rapidly store, analyse, and retrieve vast amounts of data, making it a valuable tool for various applications.[3] In general, there are two types of artificial intelligence: narrow or "weak AI" and general or "strong AI". Narrow AI is designed to perform specific tasks and is commonly used in current AI applications. On the other hand, strong AI refers to an AI system that can perform a wide range of tasks and has the ability to do most activities that humans can do. This type of AI is very ambitious and has not yet achieved its ambitions.[4]

Narrow AI systems can be classified into two main stages based on their age and mechanisms:

1. The rules-based stage

The rules-based approach or symbolic AI, which Ray Worthy Campbell has described as it "involves the creation of complex logic trees, involving 'if A, then B'" kind of commands. Once an event or fact has been characterized, the software will apply the prescribed rule".[5] A rule-based system consists of two main components: a set of facts about a situation and a set of rules that apply to those facts. Human experts are required to specify all the necessary steps that the machine needs to take to make a decision to build such a system.[6] Symbolic AI, which was the primary approach to the field of AI between the 1950s and the 1990s, is now considered an old version of AI. However, it is still used in several contexts, from thermostats to advanced robotics, even though other ap-

---

lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0795&rid=3 [last accessed 10.1.2024].

[3] L. Foit, *Your Artificial Mediator Is Ready for You Now: The Role of Artificial Intelligence in Conflict Resolution*, "American Journal of Mediation" Issue 15, 2022, p. 47.

[4] B. Philip, *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, 2020, p. 13, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf. [last accessed 27.11.2023].

[5] R. W. Campbell, *Artificial Intelligence in the Courtroom: The Delivery of Justice in the Age of Machine Learning*, "Colorado Technology Law Journal", Issue 18(2), 2020, p. 326.

[6] G. H. Kasap, *Can Artificial Intelligence ("AI") Replace Human Arbitrators? Technological Concerns and Legal Implications*, Journal of Dispute Resolution, Issue 2, 2021, p. 212.

proaches dominate the field today.[7] It works within specific problems consistent with a sequence of logical rules and is a step-by-step deduction. Therefore, this kind can be helpful in similar cases consistent with the principle of operation of this kind. Moreover, this type of system heavily relies on expert human knowledge presented in a readable format. As a result, humans can always monitor the system's performance and comprehend the outcomes in a manner that strengthens transparency for both users and programmers.[8] However, this system suffers from a significant limitation. On one hand, it works only for problems that follow a specific logical sequence. On the other hand, this system requires a substantial and persistent effort from human experts to gather, maintain, and update knowledge and rules.[9] Moreover, adding new knowledge or rules to the system also requires the involvement of human experts.[10]

2. Machine learning stage

The shortage of rule-based systems stimulated computer experts to promote another new version of AI. The latest trend of AI relies on Machine Learning (ML) algorithms that learn and adapt through experience. This trend is based upon data analysis and involves a kind of machine learning; it reaches relationships and correlations by looking for patterns in large amounts of data, where results can be achieved and specific services can be provided.[11] New AI tools can process data and access training "data" and "big data", which can lead to practical breakthroughs. When combined with complex algorithms, this can result in beneficial outcomes for a wide range of fields, such as medical diagnoses and self-driving vehicles, among many other AI applications. Machine learning is a process that involves setting a goal, such as identifying a cat in a picture and collecting data, like pictures of cats, to learn from. The machine then uses trial and error to invent rules to help

---

[7] B. Philip, *supra note* 4, p. 3.

[8] G. H. Kasap, *supra note* 6, p. 212.

[9] *Ibid*.

[10] *Ibid*.

[11] R. W. Campbell, *supra note* 5, p. 326.

it achieve its desired goal in any given situation.[12] Unlike rule-based programs, where the programmer manually codes the algorithms into the machine, machine learning allows the machine to detect and extract necessary algorithms from the data to achieve the goal defined by the programmer, such as accurately identifying a cat in a picture. As a result, the programmer does not need to write code that defines what a cat is. This makes machine learning algorithms similar to a baby that learns through examples, while rule-based algorithms are more like a human being born with fixed knowledge.[13] However, ML algorithms are not without disadvantages. The ML process can introduce bias, and the algorithms' complexity can make decision-making logic hard to understand and explain.[14] It is also important to mention that ML operates through two main methods: supervised learning and unsupervised learning. In supervised learning, the algorithms are trained using labelled data. The algorithms then develop their own techniques to predict outcomes based on the patterns in the labelled data. On the other hand, unsupervised learning is used when high-quality labelled data are not readily available. These approaches excel at identifying new clusters and connections within data that humans may not have identified or labelled.[15]

I. Caveats of the utilization of AI in Criminal Justice and Policing

Stephen Hawking once said, "Artificial intelligence is either the best or the worst thing to happen to humanity".[16] Legal experts are concerned about using AI in criminal justice. Policymakers, AI developers, users, and judges must consider the possible limitations. This section will

---

[12] G. H. Kasap, *supra note* 6, p. 213.

[13] *Ibid*., p. 213.

[14] B. Philip, *supra note* 4, p. 3.

[15] B. Philip, *supra note* 4, p. 5.

[16] A. Hern, *AI will be 'either best or worst thing' for humanity*, "The Guardian" 2016, available at: https://www.theguardian.com/science/2016/oct/19/stephen-hawking-ai-best-or-worst-thing-for-humanity-cambridge, [last accessed 7.1.2024].

address the major concerns of implementing AI in the criminal justice system.

Using artificial intelligence (AI) in the criminal justice system, especially in court processes, raises concerns about fairness. The impact of AI on fairness, compared to human judicial decision-making, is a significant concern. This issue, known as the human-AI fairness gap, questions whether AI tools in legal proceedings violate the constitutional right to a fair trial.[17] According to a recent study, human judges tend to demonstrate fairer judgment than projected AI judges, possibly owing to ineffective communication and mutual understanding between humans and AI tools. This communication gap may lead individuals to feel unheard and misunderstood when their cases are deliberated on by AI tools.[18]

On the other hand, some may argue that AI as an assistant tool in litigation procedures is not related to fairness because, in the end, it is not the final decision for the case. However, this argument undervalues procedural justice. Procedural fairness is not less important than the fairness of the outcomes, especially in the legal domain.[19] It is crucial to ensure that a human judge always supervises AI as an assistant tool in the courtroom, and it should not work alone or as an independent decision-maker.

Another critical issue to consider regarding the use of AI in criminal justice is its impact on the nature of justice. Specifically, there is a concern that AI may shift the focus of justice from equitable justice to codified justice. By introducing AI into the litigation process, standardization may become more important than discretion. Richard M. Re and Alicia Solow-Niederman have pointed out that AI introduces a new form of adjudication, where machines produce correlations across vast amounts of data without constructing an explanatory or causal model.[20]

---

[17] B. M. Chen, A. Stremitzer, K. Tobia, *Having your day in robot court*, "Harvard Journal of Law & Technology", Issue 36(1), 2022, p. 129.

[18] *Ibid*., p. 169.

[19] D. Baryse, *People's Attitudes towards Technologies in Courts*, "Laws Journal", Issue 11(5), 2022, p. 6, available at: https://doi.org/10.3390/laws11050071 [last accessed 15.12.2023].

[20] R. M. Re, A. Solow-Niederman, *Developing Artificially Intelligent Justice,* "Stanford Technology Law Review" Issue 242, 2019, p. 246, available at: https://law.stanford.edu/wp-content/uploads/2019/08/Re-Solow-Niederman_20190808.pdf [last accessed 10.12.2023].

While automated adjudicators may be unbiased and not corrupt, they lack the human faculty of conscience, making them less effective at delivering justice than human judges.[21] This is because human judges possess qualities that AI lacks, such as values, morals, knowledge of human life, and the ability to understand the intentions and motivations underlying human behaviour.[22] AI in the criminal justice system may lead to "codified justice", where machines predict case outcomes based on existing data without considering unique circumstances.[23] This approach may not be suitable for criminal cases where social factors and conditions should be considered.

Addressing the risk of relying too heavily on AI in the justice system is essential. Zichun Xu warns that increasing the use of robotic enforcement and adjudication and reducing human interaction and communication may have the unintended consequence of turning citizens into "tame bodies".[24] Therefore, equitable justice must be maintained in cases where social factors, conditions, and circumstances need to be considered to ensure that human judges continue to play an essential role in the justice system.

There is significant concern about potential AI bias in police and criminal justice. The question of whether AI violates fundamental human rights and leads to discrimination arises. Is AI truly objective? This question arises from two key factors. Firstly, "unintentional bias" can occur when AI relies on the available data while making decisions. In such cases, if the data are biased, the AI's decisions will inevitably reflect that. Secondly, "intentional bias" may arise if the creators of algorithms inject their value judgments and priorities into the algorithms themselves.[25] As a result, AI systems have the potential to perpetuate

---

[21] A. Morrison, *Artificial Intelligence in the Courtroom: Increasing or Decreasing Access to Justice?*, "International Journal of Online Dispute Resolution", Issue 1, 2020, p. 82.

[22] *Ibid*.

[23] *Ibid*.

[24] Z. Xu, *Human Judges in the Era of Artificial Intelligence: Challenges and Opportunities*, "Applied Artificial Intelligence Journal", Issue 36:1, 2022, p. 1040, available at: https://doi.org/10.1080/08839514.2021.2013652 [last accessed 10.12.2023].

[25] C. Rocha, J. Carvalho, *Artificial Intelligence in the Judiciary: Uses and Threats*, "Algoritmi Centre University of Minho", 2023, available at: https://ceur-ws.org/Vol-3399/paper17.pdf [last accessed 5.1.2024].

and amplify bias linked to race, ethnicity, nationality, socio-economic status, and other factors, thereby contributing to discrimination.

One of the most important concerns about using AI in criminal justice and policing is profiling people, and taking action before a crime has been committed. This goes against the right to be presumed innocent until found guilty in criminal proceedings. These decisions are often based on factors beyond an individual's control, including their behaviour, the actions of people they contact, or even demographic information such as data about the neighbourhood they live in.[26]

The cost of using AI in the criminal justice system could also be an essential challenge. AI is very expensive to develop from scratch.[27] Developing AI technology is a high-cost investment, and companies in such sectors invest a lot of money in building and operating AI systems. Thus, the government or private sector needs sufficient financial solvency to apply AI in the criminal system. In contrast, some opinions say that using AI in the criminal system will save more money for the state budget and the individuals involved because the number of judges and judicial staff might decrease.[28] Indeed, using AI in the criminal system is a subsequent stage to automating many other services in the country. Therefore, it is unreasonable to introduce AI into the criminal system of any country that does not have high technological capabilities in the state or supporting institutions, which means that non-developed countries do not have substantial opportunities to use AI in the early stages.

Applying artificial intelligence to assist judges may also raise risks related to judges' overconfidence and overreliance on artificial judicial intelligence decisions.[29] The risk is that judges could use AI systems to evade the decision-making process and not increase the quality of their decisions. In fact, this risk is related to the values of litigation principles.

---

[26] Fair Trials, *Artificial intelligence (AI), data and criminal justice*, available at: https://www.fairtrials.org/campaigns/ai-algorithms-data/ [last accessed 5.6.2024].

[27] J. Snyder, *Robo Court: How Artificial Intelligence Can Help Pro Se Litigants and Create a "Fairer" Judiciary*, "Indiana Journal of Law and Social Equality", Issue 1, 2022, p. 218.

[28] N. Chronowski, Kinga Kálmán, B. Szentgáli-Toth, *Artificial Intelligence, Justice, and Certain Aspects of Right to a Fair Trial*, "Acta Universitatis Sapientiae Legal Studies", Issue 2, 2021, p. 170.

[29] Z. Xu, *supra note* 25, p. 1040.

Therefore, there is an urgent need to ensure the optimal use of AI tools by judges.

There are concerns about the use of AI, particularly related to the difficulty of understanding the results it produces. The complex and opaque nature of algorithms can lead to a "black box problem", where even AI creators may not understand, or be able to explain, how the results were achieved. To ensure that the use of AI in criminal justice does not undermine fundamental rights, transparency and the ability to explain are crucial. If AI-powered tools are not transparent and explainable, it can be challenging to comprehend how they arrived at a particular decision. This lack of transparency can make it difficult for legal professionals to assess the accuracy and reliability of AI-powered tools. It can also make it challenging for citizens to understand how decisions are made, undermining trust in the legal system. Moreover, AI-powered tools must be able to explain how they arrived at a particular decision.[30]

II. How Did AI Enter Criminal Justice and Policing?

The criminal justice system comprises three main components: the police, the courts, and corrections.[31] The police play a crucial role in upholding the law, safeguarding the public, apprehending suspected law violators, and preventing criminal activities. They also engage in proactive measures by predicting potential crimes and investigating those that have already occurred.[32] Additionally, the police are responsible for gathering and preserving evidence relevant to criminal cases.[33] The

---

[30] For more about transparency and explaining ability of AI, see: ETHICS GUIDELINES FOR TRUSTWORTHY AI, 2019, available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, {last accessed 15/3/2024}.

[31] K. J. Peak, T. D. Madensen-Herold, *Introduction to Criminal Justice: Practice and Process*, "SAGE Publications", 2020, p. 4, available at: https://www.sagepub.com/sites/default/files/upm-binaries/90113_Chapter_1_Introduction_to_Criminal_Justice.pdf [last accessed 5.6.2024].

[32] G. Mesko, M. Pagon, B. Dobovsek, *Some Dilemmas of Contemporary Criminal Justice*, "National Institute of Justice (NIJ) Publication", 2004, p. 6, available at: https://nij.ojp.gov/library/publications/some-dilemmas-contemporary-criminal-justice-policing-central-and-eastern [last accessed 5.6.2024].

[33] *Ibid*.

courts' primary responsibility is to ensure that individuals accused of crimes receive fair trials. They play a pivotal role in determining the guilt or innocence of the accused while upholding the principles of justice and due process. The correctional subsystem is focused on rehabilitating offenders, aiming to modify their behaviour to promote law-abiding conduct and contribute to their successful reintegration into society. The ultimate goal of all three subsystems is to collectively reduce crime within the community and foster a safer, law-abiding environment for all individuals.

Over the years, the criminal justice system has increasingly leveraged technology to enhance its operations. Both law enforcement and the judicial system have adopted various technological tools to streamline and improve efficiency. However, the emergence of artificial intelligence (AI) represents a significant departure from conventional technology usage. Unlike previous technologies, which relied on human intervention, AI can autonomously process immense volumes of data, identify patterns, and execute specific tasks with remarkable speed and accuracy. This transformative technological shift marks a new era in the criminal justice field. In particular, AI is making notable contributions to European criminal justice by playing a crucial role in crime prediction and detection, and in the analysis of crime evidence – essential functions within policing. Additionally, AI is increasingly being employed in developing risk assessment tools utilized by courts. This chapter delves into some current applications of AI in these aspects of the European criminal justice system, shedding light on the impact of AI technology in the realm of law enforcement and judicial decision-making.

1. Crime Prediction Tools

Crime prediction essentially involves analysing historical crime data to anticipate when and where criminal activities are more likely to occur. Artificial intelligence has emerged as a promising tool for crime prediction, as it relies on data analysis and identifying patterns. In fact, algorithms are already used to predict various outcomes, such as health, stock market activity, driving behaviour, and the likelihood of reoffend-

ing for convicted criminals.[34] There are two key steps to implementing AI in predictive policing: data collection and data modelling. The first step involves gathering a vast amount of data related to historical crime data (time and location), social data, and economic data from various sources.[35] During the data modelling process, AI algorithms are utilized to analyse the collected data and identify patterns within the available historical data.[36]

This enables the AI to connect indicators to the likelihood of a crime occurring and subsequently present these probabilities as a risk score.[37] Through this processing, it is possible to predict the time when and location where crimes are more likely to occur, the type of crime that is more likely to happen, and the individual who is most likely to commit a criminal act.[38] This feature helps authorities focus their activity and resources more effectively in such places or times, which can be important in ensuring public safety.[39] Predictive policing is used in several European countries, such as the Netherlands, Germany, Austria, France, Estonia, and Romania.[40] Currently, the police in the Netherlands use AI in various applications. For example, the Crime Anticipation System (CAS) predicts crimes using statistical data from multiple channels.[41] The Dutch police have used an automated risk assessment tool called ProKid since 2011 to assess the risk of future criminality of children and young people. The tool has undergone several iterations, with the

---

[34] R. Jenkins, D. Purves, *Artificial Intelligence and Predictive Policing: A Roadmap for Research*, Report funded by US National Science Foundation, 2020, p. 1, available at: http://www.aipolicing.org/year-1-report.pdf [last accessed 10.12.2023].

[35] Majsa Storbeck, Intern, EUCPN Secretariat "Artificial intelligence and predictive policing: risks and challenges", EUCPN, 2022, p. 6, Available at: https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf. {last accessed 9.11.2023}.

[36] *Ibid*.

[37] *Ibid*.

[38] *Ibid*.

[39] *Ibid*.

[40] *Ibid*., p. 8.

[41] F. Dechesne, V. Dignum, L. Zardiashvili, J. Bieger, *AI & Ethics at the Police: Towards Responsible Use of Artificial Intelligence in the Dutch Police*, "Leiden University Scholarly Publications", 2019, p. 5, available at: https://scholarlypublications.universiteitleiden.nl/access/item%3A2983928/view [last accessed 3.6.2024].

latest version, ProKid 23, focusing on under 23-year-olds.[42] In Portugal, a study shows that official police data from Porto, Portugal, between 2016 and 2018, were analysed using spatial analysis and machine learning methods to identify spatial patterns, hotspots, and crime variables.[43] Tweets related to insecurity were also analysed. These methods assist in interpreting patterns, prediction, and the performance of police and planning professionals.[44] In Germany, crime prediction software is utilised in six federal states. This includes PRECOBS in Bavaria, PreMap in Lower Saxony, SKALA in North Rhine-Westphalia, and KrimPro in Berlin, which predict the location and timing of future crimes.[45] However, many civil rights groups, academics, and media outlets have criticized using AI as a predictive tool because AI has the potential to replicate or amplify racially biased patterns of policing. Additionally, it could unfairly burden marginalized communities and infringe upon the liberty of targeted communities.[46]

2. Crime Detection Tools

Crime detection involves determining if a crime has occurred or is in progress. It is focused on the past and present.[47] In this context, AI-powered sensors can detect and record signs of criminal activity, aiding law

---

[42] See Fair Trials, *Automating Injustice: The Use Of Artificial Intelligence & Automated Decision-Making Systems In Criminal Justice In Europe*, p. 8, available at: https://policehumanrightsresources.org/content/uploads/2021/09/Automating_Injustice.pdf?x19059 [last accessed 22.5.2024].

[43] M. Saraiva, I. Matijošaitiene, S. Mishra, A. Amante, *Crime Prediction and Monitoring in Porto, Portugal, Using Machine Learning, Spatial and Text Analytics*, "ISPRS Int. J. Geo-Inf", Issue 11(7), 2022, p. 1, available at: https:// doi.org/10.3390/ijgi11070400 [last accessed 23.5.2024].

[44] *Ibid*.

[45] L. H. Vepřek, L. Sibert, L. Sehn, L. Köpp, D. Friedrich, *Beyond Effectiveness: Legitimising Predictive Policing in Germany*, "Criminology - the online journal", Issue 3, 2020, p. 428, available at: https://www.kriminologie.de/index.php/krimoj/article/download/67/65/255 [last accessed 23.5.2024].

[46] R. Jenkins, D. Purves, *supra note* 34, p. 1-2.

[47] B. Dupont, Y. Stevens, H. Westermann, M. Joyce, *Artificial Intelligence in the Context of Crime and Criminal Justice*, "International Centre for Comparative Criminology – Université de Montréal", 2018, p. 65, available at: https://www.cicc-iccc.org/public/media/

enforcement investigations; for example, gunshot detection technology can help the police respond quickly to shooting events. AI-powered sensors can be installed in the public infrastructure and connected to a cloud-based computer to identify and pinpoint gunshots accurately. These sensors record the timing of the shots, allowing law enforcement to quickly and efficiently respond to the situation. Gunshot detection technology can be considered a part of AI since it utilizes machine learning to train its system to recognize the audio characteristics of gunfire.[48] Using this technology makes it possible to isolate the sound of gunfire from other common sounds that occur in urban areas.[49] In this regard, ShotSpotter technology is utilized by UK police to detect gunfire. Sensors listen to shots and pinpoint the location within an 82-foot (25-meter) radius.[50] While this technology may not yet be able to prevent massacres at the hands of gunmen, it can listen to gunfire and inform the police about the location from which the shots were fired. Another example of AI-powered sensors is traffic accident detection tools that use video to maintain safe and efficient traffic in various conditions.[51] Furthermore, AI algorithms are necessary for criminal justice because they can detect fraud, financial, and tax crimes by analysing volumes of data and recognizing anomalous patterns.[52] In the Netherlands, the Online Fraud Report Intake System employs advanced NLP (Natural Language Processing) techniques, computational argumentation, and reinforcement learning to aid citizens in reporting instances of crime.[53]

---

files/prod/publication_files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf [last accessed 15.11.2023].

[48] *Ibid*., p. 83.

[49] *Ibid*.

[50] S. Griffiths, *Fighting a losing battle? AI ShotSpotter computer used to track gunfire reveals far more shots are fired than are ever reported*, Mail online, 2016, available at: https://www.dailymail.co.uk/sciencetech/article-3547719/Fighting-losing-battle-AI-ShotSpotter-computer-used-track-gunfire-reveals-far-shots-fired-reported.html [last accessed 29.5.2024].

[51] C. Rigano, *Using Artificial Intelligence to Address Criminal Justice Needs*, "NIJ Journal 280", 2019, p. 2, available at: https://www.nij.gov/journals/280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.aspx [last accessed 20.11.2023]. For details and examples of using these tools in Germany, see https://www.yunextraffic.com/newsroom/ai-revolutionizing-road-safety/ [last accessed 28.5.2024].

[52] *Ibid*.

[53] F. Dechesne, V. Dignum, L. Zardiashvili, J. Bieger, *supra note* 41, p. 5.

3. Evidence Analysis Tools

Criminal justice has a unique evidence nature that requires close attention to all relevant details. Without a doubt, humans can analyse criminal evidence. However, they consume a lot of time in detecting every sign, and humans are always prone to making mistakes. On the contrary, the use of technology in evidence analysis is not a new trend. In fact, it has been utilized for decades. Therefore, using AI in this context is a continuation of past usage. However, the mechanism of AI tools gives AI an advantage over other used technologies because AI algorithms can be used to analyse various sets of evidence: photos, voices, fingerprints, and DNA samples. In detail, AI algorithms can learn complex tasks and develop independent complex facial recognition features that allow them to identify faces, weapons, and other objects. These features make huge improvements regarding quality and speed.[54] In this regard, AI algorithms can be used to improve the work of forensic medicine by addressing any related evidence or medical images to determine the time and cause of death.[55]An important example is researchers at the University of Texas in Dallas, who, with funding from the National Institute of Justice (NIJ), evaluate facial recognition by humans and AI algorithms in partnership with the FBI and the National Institute of Standards and Technology (NIST).[56] Initial results show that AI algorithms developed in 2017 perform comparably to humans when recognition time is limited to 30 seconds. The study suggests that AI-powered algorithms can increase the accuracy and productivity of human facial examiners.[57]

---

[54] *Ibid*.

[55] C. Rigano, *supra note* 51, p. 2. For more details about using AI in forensic medicine see: A.-I. Piraianu, A. Fulga, C. Liana Musat, O.-R. Ciobotaru, D. G. Poalelungi, E. Stamate, O. Ciobotaru, I. Fulga, *Enhancing the Evidence with Algorithms: How Artificial Intelligence Is Transforming Forensic Medicine*, "Diagnostics", 13:2992, 2023, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10529115/ [last accessed 28.5.2024].

[56] C. Rigano, *supra note* 51, p. 3.

[57] *Ibid*.

4. Risk Assessment Tools

4.1. Overview of risk assessment tools

AI algorithms are used to analyse various factors to assess the risk of recidivism. This helps judges in making well-informed decisions regarding sentencing and parole. In Europe, several applications are used to assess the risks and needs of offenders. For instance, in the United Kingdom, the National Probation Service and the prison system use OASys (Offender Assessment System) to evaluate the likelihood of reoffending and determine appropriate interventions.[58] In Germany, SAPROF (Structured Assessment of Protective Factors) is used along with other risk assessment tools to evaluate risk factors and protective factors that may reduce the likelihood of reoffending.[59] Similarly, in the Netherlands, probation services use RISc (*Recidive Inschattingsschalen*), a structured tool to assess the risk of recidivism and plan interventions.[60]

Despite these European applications, the researcher has focused on the US AI application COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) for detailed exploration. This is because European applications do not mainly rely on AI, but on professional judgement and statistical data.[61] COMPAS has also been widely used in the US and has undergone judicial and critical review. It shares similar goals with European applications by improving the objectivity and consistency of risk assessments in the criminal justice system. COMPAS is an AI assistant used by US judges. It can calculate the risk and dangerousness of the accused by evaluating several personal fac-

---

[58] E. Tiarks, *Report on Artificial Intelligence and the Administration of Justice in the United Kingdom Predictive Justice*, a part of an international research project on AI and criminal justice run by the International Association of Penal Law. This project, which took place from February 2022 to March 2023, p. 1, available at: https://penal.org/sites/default/files/files/A-14-2023.pdf [last accessed 3.6.2024].

[59] D. Yoon, A. Spehr, P. Briken, *Structured assessment of protective factors: a German pilot study in sex offenders*, "The Journal of Forensic Psychiatry & Psychology" 22(6), 2011, p. 834, available at: https://doi.org/10.1080/14789949.2011.617831 [last accessed 5.6.2024].

[60] L. M. van der Knaap, L. E. W. Leenarts, M. P. Born, P. Oosterveld, *Reevaluating inter-rater reliability in offender risk assessment*, "Crime and Delinquency", 58(1), 2012, p. 147.

[61] E. Tiarks, *supra note* 58, p. 1.

tors, such as criminal history.[62] This section will provide a more detailed explanation of the COMPAS algorithm used in several US courts to address the benefits and concerns of risk assessment tools.

In 1960, US courts began using risk assessment tools, one of the oldest being the "Salient Factor Score."[63] This tool evaluated offenders based on seven factors, such as education, employment, and family background. Age was initially included as a factor, but it was later removed.[64] Later, the private company "Equivant" (known as Northpointe) designed The COMPAS risk assessment software in 2000.[65] The COMPAS assessment consists of a total of 137 questions.[66] The accused person answers some of the questions, while others are answered based on information obtained from the accused person's criminal record.[67] The questions cover various topics, including general information about the defendant. Some factors considered are not directly influenced by the defendant, such as their age, any criminal history in their family, socioeconomic background, or any criminal activity in the neighbourhood.[68] After the person answers a set of questions, COMPAS compares their answers to the scores of a "norm group".[69] It then uses logistic regression, survival analysis, and bootstrap classification methods to generate a report which consists of two sections. The first section, "Overall Risk Potential", evaluates a person's recidivism risk based on three factors: A) the risk of being charged with the same crime within two years of assessment, B) the likelihood of failure to appear before the court, and C) the probability of committing a violent

---

[62] S. M. Sacoto, *Artificial Intelligence (AI): Beyond Legal Limits,* "Revista de la Facultad de Jurisprudencia (RFJ)", Issue 10, 2021, p. 376.

[63] K. Schwerzmann, *Abolish! Against the Use of Risk Assessment Algorithms at Sentencing in the US Criminal Justice System*, "Philosophy & Technology", Issue 34, 2021, available at: https://doi.org/10.1007/s13347-021-00491-2 [last accessed 23.11.2023].

[64] *Ibid*.

[65] M. A. Vaccaro, *Algorithms in Human Decision Making: A Case Study with the COMPAS Risk Assessment Software*, "Bachelor's thesis, Harvard College", 2019, p. 3, available at: https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37364659 [last accessed 22.11.2023].

[66] K. Schwerzmann, *supra note* 63.

[67] *Ibid*.

[68] *Ibid*.

[69] *Ibid*.

crime. The evaluation is on a scale of 1 to 10.[70] Scores ranging from one to four are classified as low risk, while those ranging from five to seven are classified as medium risk, and those ranging from eight to ten are classified as high risk.[71] The company "Equivant" did not disclose the detailed process by which COMPAS makes predictions, resulting in COMPAS being characterized by opacity.[72] The use of COMPAS is prevalent in several US states, including Arizona, Colorado, Delaware, Kentucky, Louisiana, Oklahoma, Virginia, Washington, and Wisconsin, for bail, parole, and sentencing decisions.[73]

4.2. The *State v. Loomis* case

In a case involving the use of COMPAS in sentencing decisions, Eric Loomis was charged with five counts, all as a repeat offender: (1) First-degree recklessly endangering safety, (2) Attempting to flee or elude a traffic officer, (3) Operating a motor vehicle without the owner's consent, (4) Possession of a firearm by a felon, and (5) Possession of a short-barrelled shotgun or rifle.[74] Loomis denied any involvement in the shooting, claiming that he only drove the car after the shooting occurred.[75] As part of a plea deal, he entered a plea of guilty for two minor offences – trying to evade a traffic officer and driving a vehicle without the owner's permission.[76] The court accepted the plea, and a presentence investigation was ordered, which included a COMPAS risk assessment.[77] Loomis was categorised as having a high risk of recidivism in categories (pre-trial release risk, general recidivism, and violent recidivism) by the COMPAS assessment.[78] The State argued that a risk assessment should

---

[70] *Ibid*.

[71] M. A. Vaccaro, *supra note* 65, p. 3.

[72] B. Dupont, Y. Stevens, H. Westermann, M. Joyce, *supra note* 47, p. 130.

[73] M. A. Vaccaro, *supra note* 65, p. 3.

[74] The State v. Loomis case, SUPREME COURT OF WISCONSIN, 2015, AP157-CR, 2016, para 11, available at: https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690 [last accessed 4.6.2024].

[75] *Ibid*., para 12.

[76] *Ibid*.

[77] *Ibid*.

[78] *Ibid*., para 16.

be considered when determining an appropriate sentence for Loomis.[79] The risk assessment was then used as a basis to deny Loomis probation. The circuit court judge explained that probation was ruled out owing to the severity of the crime, Loomis's history, and the results of the risk assessment, which indicated that he was at an extremely high risk of re-offending.[80] Loomis raised three objections to the use of COMPAS. Firstly, he argued that the algorithm violated his right to a fair sentence, as it failed to provide accurate information, partly owing to its proprietary nature, which prevented him from assessing its accuracy.[81] Secondly, he claimed that the algorithm violated his right to a personalized sentence.[82] Lastly, he contended that the algorithm inappropriately considered gender while generating its scores.[83]

The Wisconsin Supreme Court considered Loomis's challenges and rejected them. In response to the gender argument, the court stated that Loomis failed to prove that the circuit court actually relied on gender as a factor in imposing its sentence.[84] The court said that including gender as an input for the algorithm actually improved the tool's accuracy and furthered the goal of non-discrimination.[85] As for the second argument, the court clarified that judges still retain the discretion to disagree with the algorithm's decisions, and thus, the defendant still received an appropriately individualized sentence.[86] It is worth noting that the court cautioned judges against relying too heavily on algorithmic recidivism predictions and required written advisement to accompany the risk assessment scores in the presentencing advisement report.[87] However, according to the Harvard Law Review, this written advice may not be effective.[88] Stricter measures may be more appropriate, such as excluding

---

[79] *Ibid*., para 18.
[80] *Ibid*., para 19.
[81] *Ibid*., para 34.
[82] *Ibid*.
[83] *Ibid*.
[84] *Ibid*., para 85.
[85] *Ibid*., para 83.
[86] *Ibid*., para 9.
[87] *Ibid*., para 100.
[88] *Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*, "Harvard Law Review" 130, no. 8, 2017, pp. 1530-1538, available at: https://harvardlawreview.org/print/vol-130/state-v-loomis/ [last accessed 5.6.2024].

risk assessments with secret methodologies or limiting their use until more studies are available.[89]

4.3. Does COMPAS have a bias against black persons?

In 2016, ProPublica, an online nonprofit investigative journalism organization, published an article titled Machine Bias.[90] This piece demonstrates that the COMPAS algorithm incorrectly classifies black defendants as high risk nearly two times more frequently than white defendants.[91] Moreover, the algorithm incorrectly classifies white defendants as low risk nearly two times more frequently than black defendants.[92] Based on these findings, the authors claimed that the COMPAS software demonstrated biases against blacks.[93] ProPublica's allegations sparked heated debates within the computer science community about algorithmic fairness and transparency.[94]

III. The EU Legal Framework for Using AI in Criminal Justice and Policing

1. Law Enforcement Directive (LED) 2016/680

The increased integration of AI in criminal justice and law enforcement throughout Europe underscores the importance of thoroughly evaluating the existing legal framework within EU regulations about using personal data in criminal justice. This is especially crucial owing to the substantial reliance of AI systems on personal data for tasks such as crime detection and prediction, analysis of criminal evidence, and risk

---

[89] *Ibid*.

[90] J. Angwin, J. Larson, S. Mattu, L. Kirchner, ProPublica May 23, 2016, available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [last accessed 10.1.2024].

[91] *Ibid*.

[92] *Ibid*.

[93] *Ibid*.

[94] *Ibid*.

assessment. Within this context, EU Directive 2016/680, also called the Law Enforcement Directive, sets regulations aimed at safeguarding individuals when their personal data are processed by law enforcement authorities to prevent, investigate, detect, or prosecute criminal offences and enforce criminal penalties.[95] The directive covers how authorities handle personal data.[96]

Under LED, there is an essential difference between the nature of the two personal data. Under Article 8 of LED, Member States must only allow data processing if necessary for a task which is carried out by a competent authority for the purposes set out in Article 1(1) and is based on Union or Member State law. This general rule applies to all types of data, whether these data are sensitive or not. On the contrary, article 10 of LED described that the processing of personal data that includes information about a person's race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data to identify a person, data concerning health, or data concerning a person's sex life or sexual orientation, will only be allowed when it is absolutely necessary.[97] As a result, if the data are sensitive, as described in Article 10, there should be a strict necessity to allow the processing of these data. In the criminal justice context, and as has been mentioned before, some AI tools, such as risk assessment tools, use sensitive personal data to give outcomes. Therefore, using these tools should be compatible with what Article 10 requires. Besides the existence of strict necessity, the data can only be processed if it is allowed by the law of the European Union or a member state to protect the important interests of the person the data are about or another person or if the data have been intentionally made public by the person they are about.[98]

The European Court of Justice (ECJ), in the case "Criminal proceedings against VS, Case C-205/21, Judgment of 26 January 2023", has clarified the difference between ordinary and sensitive data under LED and connected that with the fundamental rights and freedoms guaranteed

---

[95] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April, Official Journal of the European Union, L 119, Article 1, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680 [last accessed 4.6.2023].

[96] *Ibid*., Article 2(1).

[97] *Ibid*., Article 10.

[98] *Ibid*., Article 10.

by Articles 7 and 8 of The Charter of Fundamental Rights of the European Union by stating that:

> Article 10 of Directive 2016/680 constitutes a specific provision governing the processing of the special categories of personal data, including biometric and genetic data. As is clear from the case law, the purpose of that article is to ensure enhanced protection about that processing, which, because of the particular sensitivity of the data at issue and the context in which they are processed, is liable, as is apparent from recital 37 of the directive, to create significant risks to fundamental rights and freedoms, such as the right to respect for private life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter.[99]

The ECJ interpretation of "strictly necessary" in Article 10 focused on the difference between this specific requirement and the general necessity in the directive. The court noted that in the French-language version of the LED, the term used in Article 10 was "*nécessité absolue*", indicating strengthened conditions for lawful processing of sensitive data.[100] The court emphasized that using the adverb 'only' before the words 'where strictly necessary' underlines that processing special categories of data is limited.[101] Additionally, the court highlighted that the processing of such data requires particularly strict checking to ensure compliance with the requirement of data minimization under the LED.[102] The ECJ noted that data processing should be connected to preventing criminal offences or threats to public security, displaying a certain degree of seriousness, punishing such offences, or protecting against such threats.[103] The court emphasized the need to consider the objective's nature and ensure the processing is warranted.[104]

---

[99] ECJ, Criminal proceedings against VS, Case C-205/21, Judgment of 26 January 2023, para 116, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0205&qid=1717867485607 [last accessed 1.6.2024].

[100] *Ibid*., para 117.

[101] M. Naarttijärvi, *AI and Sensitive Personal Data Under the Law Enforcement Directive: Between Operational Efficiency and Legal Necessity*, "Springer, Cham", 2023, p. 341, available at: https://doi.org/10.1007/16495_2023_57 [last accessed 8.6.2024].

[102] *Ibid*.

[103] *Ibid*.

[104] *Ibid*.

The most related article in LED on using AI in the criminal justice system is article 11, which states that decisions that significantly affect someone and are made by automated processing, like profiling, should be prohibited unless authorized by the law of the European Union or a Member State.[105] This authorization should also provide ways to protect the rights and freedoms of the person involved, including the right to ask for human intervention.[106] However, this article does not solely address or ensure that the use of AI in the criminal justice system upholds individuals' rights and liberties. This is because the primary challenges to human rights of AI systems stem from their design, training, and the technology they employ, such as machine learning.[107] While existing laws govern the impact of decisions made through automated processing, they do not specifically regulate AI systems themselves.[108] Therefore, the regulations must extend to decisions regarding designing and implementing AI systems. Furthermore, The LED does not provide rules for situations where automated processing is not the only basis of a decision, but plays a significant role.[109] It is often unclear whether a decision is fully automated or involves some human input. Because of this, AI systems can have major legal effects without the necessary safeguards.[110] This means that stronger legal standards are needed to ensure that semi-automated decision-making processes do not effectively become fully automated. Moreover, the LED generally prohibits automated decision-making unless it is allowed by the law of a European Union member country and provides appropriate protections for people's rights. This gives member countries a lot of leeway to override the general ban.[111] Also, as has been analysed before, using AI systems in the criminal justice system raises significant concerns regarding the lack of transparency and causing discrimination. While the

---

[105] Directive (EU) 2016/680, *supra note* 95, Article 11.

[106] *Ibid*.

[107] Fair Trials, *Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU*, "Policy Paper", 2022, p. 6, available at: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf [last accessed 7.6.2024].

[108] *Ibid*.

[109] *Ibid*.

[110] *Ibid*.

[111] *Ibid*.

LED mainly concentrates on safeguarding personal data used for law enforcement, it does not specifically tackle the potential risks related to transparency and non-discrimination in AI systems.

2. Projected Artificial Intelligence ACT (AIA)*

The European Union is on the verge of adopting the AIA, the first extensive legislation regulating the use of AI systems in the region. The AIA is currently awaiting final proofreading and formal endorsement by the European Council. The primary aim of this Act is to establish a legal framework for trustworthy AI based on EU values and fundamental rights.[112] In the context of criminal justice, the AIA encompasses various regulations for using AI. Firstly, the use by law enforcement of AI systems is subject to certain regulations, particularly regarding high-risk AI systems, such as those which Article 6(2) outlines. These high-risk AI systems include those used for assessing risk, conducting polygraph tests, evaluating evidence, predicting the likelihood of offending, and profiling during criminal investigations.[113] These systems must comply with the requirements outlined in section two of the Act, which cover aspects such as risk management, data governance, technical documentation, provision of information to users, and human oversight.[114] Secondly, the use of AI for real-time identification in public spaces for law enforcement should be restricted, except for specific purposes: targeted search for victims, preventing imminent threats, and locating criminal suspects for investigation or prosecution.[115]

The recently approved AIA text by the EU parliament has received significant criticism, especially from civil society organizations. One of

---

* The AIA is a regulation, not a directive like LED. It will have binding legal force across the EU.

[112] European Parliament, (2024), Legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), Official Journal of the European Union, Article 1.

[113] *Ibid*., Annex III, Section [6].

[114] *Ibid*, section two, articles (8,9,10,11,12,13,14,15).

[115] *Ibid*., article 5(1)(h).

the major concerns is the exemption granted to law enforcement authorities from transparency and oversight safeguards. While the Act mandates public authorities to register high-risk AI systems onto a publicly accessible database, law enforcement is exempt from this requirement, leading to secrecy around potentially harmful AI uses.[116] This lack of transparency makes it difficult for affected individuals, civil society, and journalists to track the deployment of AI systems.[117] Additionally, the exemption for national security allows member states to bypass the rules for any activity they consider relevant for "national security", essentially providing a blanket exemption for matters related to migration, policing, and security.[118] In addition to that, The AI Act should include a complete ban on the use of emotional recognition technologies and real-time remote biometric identification in publicly accessible spaces, according to civil society organizations.[119] They argue that these technologies are fundamentally incompatible with human rights and should be banned completely from the design phase to deployment, with narrower exemptions and stronger safeguards for law enforcement use.[120]

Conclusions

The use of AI is expected to significantly impact various aspects of our lives, especially in the criminal justice system. AI can potentially improve the effectiveness, quality, and cost-efficiency of policing and criminal justice. It is changing how police operate by enhancing crime

---

[116] Access Now, *Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move*, "Access Now", 2022, available at: https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/ [last accessed 10.6.2024].

[117] *Ibid*.

[118] *Ibid*.

[119] Algorithm Watch, *EU Parliament votes on AI Act; member states will have to plug surveillance loopholes*, 2023, available at: https://algorithmwatch.org/en/eu-parliament-votes-on-ai-act/ [last accessed 8.6.2024], see also: EU: AI Act passed in Parliament fails to ban harmful biometric technologies. Article 19, 2023, available at: https://www.article19.org/resources/eu-ai-act-passed-in-parliament-fails-to-ban-harmful-biometric-technologies/ [last accessed 7.6.2024].

[120] *Ibid*.

prediction, detection, and evidence collection and analysis. However, it is crucial to be cautious when integrating AI, particularly concerning fundamental rights. In Europe, AI is growing in criminal justice and policing, with several AI applications being used to support court and police tasks. While this usage improves efficiency and saves time, it raises concerns about transparency, explainability, and non-discrimination. Although current EU regulation (LED) governs the processing of personal data in criminal justice, it does not specifically address considerations related to AI systems, such as ensuring transparency and non-discrimination. The upcoming AI Act is a comprehensive legal framework project that addresses many issues not covered in LED. However, in some aspects, it does not strike the proper balance between fundamental rights considerations and the features of AI systems used by law enforcement in criminal justice, especially in guaranteeing the transparency of AI systems. Regulating artificial intelligence (AI) systems in the criminal justice system is a complex task. Creating strict regulations when integrating this new technology to protect fundamental rights is important. This will allow for the development of suitable applications and the accumulation of experience before widespread adoption.