

Artificial Intelligence in Criminal Procedure: Instigating Imbalances in Traditional Tendencies

ABSTRACT: *The evolution of criminal procedural law has historically been characterised by a clash between two fundamental tendencies, present since the inception of the field. First, there is the pursuit of an effective criminal procedure, aimed at safeguarding society and individuals by identifying and punishing offenders. This goal is contrasted with the aim of ensuring a robust defence for every citizen subject to criminal proceedings, thereby preventing the wrongful conviction of the innocent and restricting any arbitrary or abusive exercise of state authority. Historically, the imbalance between these tendencies often stemmed from differing legal, philosophical, and political perspectives. In the 21st century, criminal procedural law faces a new challenge in balancing these traditionally conflicting aspirations due to the advent and integration of new technologies, particularly artificial intelligence (AI). This technological disruption, favouring the effectiveness of criminal prosecution, presents a dilemma for the conventionally and historically slower-evolving criminal procedural law, which struggles to respond at a pace in line with the rapid development and application of AI in criminal proceedings. The first segment of this research delves into the historical analysis of criminal procedural law, examining the interplay and shifting dominance of traditional tendencies through time. It aims to identify the challenges that influenced their interplay and, based on historical insights, presume future developments. The second part focuses on a systematic examination of individual AI systems, using specific examples of their implementation in criminal procedure. This analysis aims to determine whether these technologies genuinely represent a shift towards prioritising the efficiency of criminal proceedings over strong defence rights. Finally, the study explores current legislative responses to these emerging challenges, primarily the AI Act of the European Union and the draft AI Treaty of the Council of Europe. These legislations lay the groundwork for national responses to the utilisation of AI in criminal procedure, and their impact on the balance of traditional legal tendencies is critically assessed.*

* Master of Laws, Teaching Assistant, Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek, Chair of Criminal Law Sciences, ORCID: <https://orcid.org/0000-0002-7003-632X>, e-mail: ivan.vidakovic@pravos.hr.



KEYWORDS: *Artificial Intelligence, Artificial Intelligence Treaty, Criminal Procedure, European Union Artificial Intelligence Act, Traditional Tendencies of Criminal Procedure*

1.

Introductory Remarks

The development of criminal procedural law is marked by a constant conflict between two traditional tendencies. To achieve the objectives and social purpose of criminal procedural law, it is necessary to regulate criminal procedure normatively, with numerous factors influencing the process.¹ Among these, the dominance of one traditional aspiration over another, depending on differing goals and social purposes, has significantly shaped the normative structure of criminal procedure. One of these tendencies emphasises the effectiveness or functionality of punishment, aiming to protect individuals and the community by identifying and punishing each guilty offender. The other focuses on safeguarding citizens' rights by normatively limiting the state's repressive power, ensuring that every individual has the opportunity for a complete defence to avoid wrongful convictions and prevent arbitrary or abusive state actions.² Achieving a balance between these opposing goals is the ideal, though it remains uncertain whether it has been or will be fully achieved in the future.

Various disruptive factors have impacted the regulatory design of criminal procedure, including influences from the state system, social values, and political and economic factors. These influences have, at certain times, tilted the scales towards greater criminal prosecution effectiveness and, at others, towards upholding the full rights of citizen defence. Thus, the first chapter of this work examines the historical development of criminal procedural law, emphasising the dominance of aspirations, causes behind these shifts, and disruptive factors that subsequently spurred entirely new procedural developments. The analysis primarily explores accusatory, inquisitorial, and mixed criminal proceedings, highlighting the foundational features through which the balance of these traditional aspirations can be observed. The hallmark of the 21st century is rapid technological progress, epitomised by artificial intelligence (AI), which has irreversibly impacted all areas of society, including criminal procedural law. Consequently, the study further examines AI as a disruptive factor in modern criminal procedural law, focusing on systems that affected it the most. The influence of these technologies on contemporary criminal proceedings is discussed

1 Krapac, 2020, p. 11.

2 Ibid.

through a brief analysis of mass communication interception and surveillance, facial recognition technologies, and risk assessment systems. Finally, the study assesses the impact of new regulations on the effort to balance these traditional tendencies.

The central hypothesis of this research posits that AI has had a significant impact on modern criminal procedure. A secondary hypothesis suggests that AI influences the balance between traditional criminal procedural tendencies, potentially altering the equilibrium between procedural efficiency and the right to a full defence. The third hypothesis proposes that AI contributes more significantly to the procedural efficiency of criminal justice than to ensuring a comprehensive right to defence.

The analysis employs a range of qualitative research methods to examine AI's impact on criminal procedural law. A doctrinal approach is used to explore traditional criminal law doctrines alongside modern AI regulations, such as the European Union (EU) Artificial Intelligence Act (AIA). Comparative analysis highlights differences across legal systems, specifically accusatorial, inquisitorial, and mixed procedures, demonstrating how AI may influence each aspect uniquely. Through empirical case analysis of real-life examples such as ANOM, EncroChat, and Sky ECC, the study provides concrete illustrations of AI's effects on procedural fairness and defence rights. The historical method adds depth by tracing the evolution of criminal procedural tendencies, showing how AI disrupts long-standing legal principles. Additionally, normative analysis addresses the ethical implications of AI, particularly the challenge of balancing procedural efficiency with the right to a full defence. Finally, legal policy analysis evaluates current regulatory frameworks, assessing how well they adapt to AI's unique challenges in criminal law. Together, these qualitative methods create a comprehensive framework for understanding the role of AI in reshaping criminal procedure.

2.

Traditional Tendencies Through the Historical Development of Criminal Procedure

Throughout the historical development of criminal procedure, various social goals have been pursued, each influencing the norms that govern legal processes. In ancient Rome, criminal procedure aimed to ensure equal standing for both parties. However, owing to a misinterpretation and incorrect reception of these rules and norms, the late imperial period saw the emergence of inquisitorial proceedings. This shift marked the rise of a system focused heavily on the efficiency of criminal prosecution. The advantages and disadvantages of these different approaches highlighted the need for an optimal model that could incorporate the best elements of both systems, ultimately giving rise to the mixed criminal procedure. By examining

the evolution of these tendencies, key aspects emerge that can be applied to modern challenges, such as the disruptive impact of AI on criminal proceedings. The following section of the study explores this historical development in greater detail.

2.1. Accusatorial Criminal Procedure

The earliest form of criminal procedure developed in the ancient communities of Greece and Rome. It represented a legal dispute between two parties – the plaintiff and the accused – brought before an independent and impartial court for resolution.³ The position of the accused is crucial for understanding the relationship between traditional tendencies. First and foremost, the burden of proof rested on the prosecutor, meaning that the accuser had the obligation to prove their case, as reflected in the maxim *actore non probante, reus absolvitur*. The defendant presented evidence only insofar as they believed the prosecutor had succeeded in proving their case.⁴ However, it is important to note that the regulations prohibited the defendant from being used as a source of information. Specifically, the prosecutor was not allowed to interrogate the defendant or use them or their statement as evidence to support their claims. When we examine the types of evidence used in Roman accusatorial proceedings, they are nearly identical to those used today, primarily witnesses, experts, and their statements and documents. The favourable position of the accused was further supported by the fact that decisions were made through public, oral, and adversarial hearings, where the court's role was passive and limited to ensuring the proper presentation of evidence.⁵ Additionally, unlike the prosecutor, the defendant had the option to hire a defence attorney, although only as a procedural assistant, meaning the defendant still had to be present during proceedings. This was significant because the prosecutor did not have the same option.⁶ This is especially relevant because we are discussing a type of criminal procedure that lacked an authorised body to initiate and conduct prosecutions, relying entirely on citizens, initially only the injured party, but later any citizen, in what was known as the popular criminal lawsuit system or *actio popularis*. This system had its drawbacks, particularly vis-à-vis the initiation of criminal proceedings, as the responsibility for pursuing cases rested solely with private individuals, with no formal prosecuting authority. Given the importance of the rights and freedoms protected in criminal proceedings, both for individuals and the community, this lack of systematic prosecution represents a significant weakness

3 Krapac, 1995, pp. VII–VIII.

4 Bayer, 1995, p. 6.

5 Roodt, 2004, p. 139.

6 Bayer, 1995, p. 9.

in terms of the efficiency of the criminal justice process.⁷ This is even more notable given the existence of *juramentum calumnie* (an oath against false accusations) and the prosecutor's criminal liability in cases of defamatory lawsuits. Additionally, the prosecutor was required to provide a property guarantee to ensure they would see the proceedings through to the end.⁸ The prosecutor was also held criminally liable if, without the court's consent, they reached an agreement with the accused and dropped the charges. Another significant disadvantage of this system was the absence of any legal remedy, which somewhat weakened the defendant's position. However, through this procedure and under the principle of legality, the elements of a criminal offense were defined, creating *crimina legitima* and establishing legal punishments (*poenae legitima*), which significantly contributed to legal certainty and protection against arbitrariness.⁹ Moreover, the free evaluation of evidence, based on the judge's free conviction, further strengthened the defendant's position.

When examining the pure Roman accusatorial procedure, it is evident that the position of the defendant was more than equal to that of the prosecutors. The fact that criminal prosecution depended solely on the will of private individuals highlights the reality that criminal proceedings were not always guaranteed to be initiated, the motives for which could vary. Additionally, the threat of criminal liability in cases of defamatory lawsuits or abandoning the prosecution could serve as a further demotivator for the plaintiff.¹⁰ Therefore, the mere initiation of criminal proceedings did not contribute to efficiency, as there was no systematic approach, and the decision to prosecute could be influenced by various personal motives, potentially leading to the non-initiation of proceedings. Additionally, owing to the rule on the burden of proof, the defendant was not required to actively defend themselves, and the outcome of the case depended solely on the prosecutor, a layperson without the right to a procedural assistant, such as a lawyer. Furthermore, the defendant could not be interrogated or questioned, either by the prosecutor or the court, and the court itself played a passive role, merely overseeing the regularity of the proceedings. While the lack of legal remedies weakened the defendant's position, other guarantees significantly improved it compared with that of the prosecutor, who faced limitations. This leads to the undeniable conclusion that the tendency to fully enable the right to defence in Roman accusatorial procedure was far more dominant.

Nevertheless, such a procedure was sufficient during the Roman Republic – a time when there was a strong sense of responsibility towards the community, and citizens regularly took the initiative to commence criminal proceedings. However, the collapse of the Republic and the rise of the Empire introduced disruptive factors

7 Mousourakis, 2021, pp. 172–173.

8 Ibid., p. 171.

9 Levy, 1938, p. 297.

10 Bayer, 1995, p. 6.

that reshaped the criminal procedure, placing greater emphasis on the effectiveness of criminal prosecution. This shift continued into the Middle Ages following the fall of the Roman Empire.

2.2. Inquisitorial Criminal Procedure

Inquisitorial criminal proceedings can be defined as the unilateral exercise of state power when a commission of a criminal offense is suspected, with the aim of identifying and punishing the perpetrator. This system developed during the Roman Empire period and later, through the Roman canon law of the Catholic Church, entered the practice of secular courts in the Italian city-states of the 13th century. It was further refined by the legal schools of glossators and post-glossators, adopted by the legislative acts of the Habsburg emperors in the German lands during the 16th century, and later by the ordinances of the French monarchy in the 17th century.¹¹ According to Bayer, part of the reception of the inquisitorial criminal procedure in the medieval Italian city-states was flawed, leading to the development of strict and formal rules that significantly influenced the future evolution of criminal procedure.¹² However, it is important to note that the inquisitorial criminal procedure is not inherently negative, as it is often perceived. In fact, some of its principles were later adopted and have endured in modern criminal procedures. The main proponent of a more objective view of the inquisitorial procedure, *Damaška*, highlights that one of its key features is the initiation of criminal proceedings *ex officio* by the judge, which remains a fundamental aspect.¹³ This shift was a response to the disruptive factors following the collapse of the Roman state, such as state particularism and changing values and culture, which made it difficult to find private citizens willing to initiate criminal prosecutions. Regarding the position of the defendant, it was no longer equal to that of the criminal prosecution authorities. The defendant was now required to answer questions and, under certain conditions, could be subjected to torture. However, *Damaška* urges caution, emphasising that torture was not easily imposed, as there were legal standards that had to be met, including a specific amount of evidence or indications. Furthermore, any evidence obtained through the illegal use of torture, including the defendant's statements, was deemed inadmissible.¹⁴ Torture was a consequence of the misapplication of criminal procedure rules at the end of the Roman imperial era, which introduced rigid rules for evaluating evidence. These legal standards dictated how certain crimes were to be proven, both in terms

11 Krapac, 2020, pp. 16–17.

12 Bayer, 1995, p. 12.

13 Damaška, 2001a, p. 479.

14 Damaška, 2013, pp. 181–182.

of the quality and quantity of evidence. For example, more serious crimes, especially those involving bloodshed, could only be proven through the defendant's confession or the testimony of two impeccable witnesses, an occurrence that is rare today and was even rarer at the time. However, there were also extra-legal factors, justified by prevailing worldviews, religious influence, and the values inherent in that mindset, which played a role in shaping these procedural practices.¹⁵ The defendant's position was further complicated by the fact that proceedings were conducted in secret, with judges making decisions indirectly, relying solely on the case files.¹⁶ Although the process was initiated *ex officio* and there was no division of procedural functions, the maxim *actore non probante, reus absolvitor* did not apply for another reason. Specifically, *absolutio ab instantia* referred to a decision to temporarily suspend criminal proceedings without finality, used in cases where guilt could not be proven but suspicion remained. This left the defendant in a precarious position, as the case could be reopened later.

The position of the defendant in inquisitorial criminal proceedings was significantly worse than that in accusatorial criminal proceedings. The cumulation of functions, where the court conducted both the investigation and trial, severely undermined the effectiveness of the defence.¹⁷ This was especially true since the trial was based primarily on the case file compiled by the investigator, who was also the judge, leaving little room for direct assessment of evidence and facts. The entire process was closed to the public, and the defendant's right to a defence attorney was rarely granted, typically only at the end of the proceedings. One of the most significant challenges was that the defendant's statement, considered highly valuable evidence at the time, could be obtained by torture. Torture often led even innocent defendants to confess, which contradicts earlier principles such as those reflected in *Emperor Trajan's maxim*.¹⁸ Despite these harsh conditions, the development of the right to appeal marked a step forward in the realisation of effective defence rights. However, this shift was far from sufficient to establish a balance between the traditional tendencies in criminal procedure. Although the defendant remained the subject of the proceedings, despite some authors' claims that they were treated as an object, their defence rights were often illusory and difficult to fully exercise due to numerous obstacles.¹⁹ It is evident that much greater emphasis was placed on making criminal proceedings as efficient as possible, often at the expense of the defendant's position.

15 For further information, see Damaška, 2021, pp. 45–57.

16 Beccaria, 1990, pp. 98–101.

17 Krapac, 2020, pp. 16–17.

18 Iustinianus, 1963, p. 846, D. 48.19.5.

19 Damaška, 2013, pp. 175–188.

The overemphasis on the effectiveness of criminal procedure, and the extreme measures it entailed, significantly increased the risk of wrongful decisions, often to the detriment of the defendant. The secrecy of the process, use of torture, reliance on indirect evidence, lack of public scrutiny during procedural actions, and limited access and rights of defence attorneys all raised serious doubts about the fairness of the procedure, and consequently, the outcomes.²⁰ Under the influence of emerging ideas about human rights and fundamental freedoms, which took shape more concretely during the Age of Enlightenment and the French Revolution, criminal procedure underwent significant reform. This reform aimed to establish a more balanced approach by integrating elements from both inquisitorial and accusatorial systems, creating a more just and equitable legal process.²¹

2.3. Mixed Criminal Procedure

Considering Krapac's definition

'Modern mixed criminal procedure represents a synthesis of the elements of accusatory (accusatory) and investigative (inquisitorial) type of criminal procedure in the legal system of actions and measures of state bodies in the case of the probability of a criminal offense, undertaken with the aim of properly distinguishing the guilty from the innocent and realizing the principle of public punishment of them'.²²

The reform of inquisitorial criminal procedure in the second half of the 19th century brought about transformative changes.²³ Influenced by Enlightenment ideas and civil liberalism, French legislation sought to align criminal procedure with the emerging concepts of fundamental human rights and freedoms. This reform included the search for acceptable procedural models, with the English criminal procedure serving as an example. From the English system, several core principles were adopted, including the principle of public trials, immediate evaluation of evidence, adversariality, and the participation of lay citizens in trials.²⁴ According to Ljubanović, Novokmet, and Tomičić,

20 Damaška, 2001b, pp. 6–7.

21 Damaška, 1995, pp. 42–44.

22 Krapac, 2020, p. 18.

23 Krapac, 1994, p. 518.

24 Krapac, 1995, p. VII.

'Modern mixed criminal procedure originates from the French Code of Criminal Investigation (Code d'instruction criminelle), which was adopted in 1808 during the reign of Napoleon Bonaparte. Under this Code, first-degree criminal proceedings were divided into two stages: the preparatory procedure and the main hearing. The main hearing was conducted before the court based on an indictment filed by an authorized prosecutor'.²⁵

Contemporary criminal procedure in the Republic of Croatia remains a mixed system, a legacy from the period of Bach's absolutism and the country's subsequent independence. Although it has undergone significant reforms and changes over time, with the most recent major revisions made in 2013, the procedure still fundamentally represents a synthesis of accusatorial and inquisitorial elements. Akin to most European continental systems, Croatia's criminal procedure, while distinct in certain aspects, shares similar elements, principles, and structural characteristics with other systems across the continent.²⁶ Accusatorial elements present in nearly all modern mixed criminal proceedings include the organisational division of the criminal court into professional judges and lay judges, and the clear separation of functions between state attorneys responsible for prosecution and judges who lead the proceedings. The position of the accused is safeguarded with procedural rights, such as the right to defence counsel from the earliest stages; the right to be informed of the charges; the ability to propose evidence and certain evidentiary actions; the right to be present during their conduct; and the public's participation in the hearing, which is conducted orally and directly. Despite the oft-negative connotations associated with inquisitorial proceedings, some of their features persist in modern mixed criminal procedures. These include the division of the criminal process into stages; the principle of officiality, where the state attorneys have a duty to initiate proceedings; the possibility of questioning the accused without the obligation to testify; and placing certain burdens of proof on the accused. These inquisitorial elements continue to shape the structure and functioning of contemporary criminal justice systems.

Such a mixed criminal procedure aims to strike a balance between traditional tendencies, granting criminal prosecution authorities the tools for effective prosecution while providing the defendant with the opportunity for a full and effective defence. Over time, various influences have weighed on the scales of these aspirations, and the most recent disruptive factor to significantly impact this balance is the introduction of AI, which has increasingly found application in criminal proceedings.

25 Ljubanović, Novokmet and Tomičić, 2020, pp. 209–210.

26 Derenčinović and Dragičević Prtenjača, 2022, pp. 91–95.

3.

AI: A New Disruptive Factor in Criminal Proceedings?

New technologies, particularly AI, have made an irreversible impact on citizens' daily lives. Owing to their advantages and potential applications, they were quickly adapted for use in criminal proceedings.²⁷ Nevertheless, for relatively traditional fields such as criminal law and criminal procedure, this new factor represents a disruptive element of the 21st century. The introduction of AI in criminal proceedings challenges fundamental principles and concepts, demanding significant adaptation and reconsideration.²⁸ Considering the wording of current regulatory initiatives, court decisions, the frequency of system use, and the profile of system users, it is evident that AI systems are significantly more advantageous for prosecuting bodies and law enforcement authorities than for defendants. This analysis examines distinct types of systems and their applications, aiming to provide an overview of how AI has been used in criminal proceedings and the disruptive impact it has had on traditional legal practices.

3.1. Bulk Communication Interception

The new concepts of big data and data mining as collection and processing techniques have enabled unprecedented access to and analysis of vast amounts of data.²⁹ Law enforcement has leveraged these technologies, particularly through the decryption of encrypted communications, to gather extensive evidence, including messages, photos, and media content, to investigate criminal activities. This is evident in the ENCROCHAT, ANOM, and Sky ECC cases, where the interception of communications, particularly in crime-heavy areas, significantly aided investigations into organised crime.³⁰

3.1.1. EncroChat

EncroChat, an encrypted communication platform, was heavily utilised by criminal organisations. In 2020, French and Dutch authorities successfully infiltrated the service, intercepting communications from over 60,000 users, resulting in

27 Kaspar et al., 2023, pp. 3–5.

28 Quattrocchio, 2020, pp. 3–4.

29 Završnik, 2018, pp. 3–7.

30 Simović and Šikman, 2023, pp. 228–230.

the capture of approximately 115 million messages. These interceptions led to the identification of 6,558 suspects, significant seizures of assets totalling hundreds of millions of euros, and the confiscation of tons of drugs and weapons, making it one of the most impactful law enforcement operations against organised crime in Europe.³¹ Legal challenges primarily focused on procedural fairness under Art. 6 of the European Convention on Human Rights (ECHR). In Dutch case law, such as the Dutch Supreme Court 2024, the admissibility of *EncroChat* data was upheld despite defence arguments concerning the legality of the interception and lack of transparency regarding the methods used. The Dutch Supreme Court upheld the use of *EncroChat* evidence, addressing key fair trial concerns raised by the defence. The court balanced operational secrecy with the need for judicial oversight, ensuring that the interception of encrypted data by French authorities did not violate Art. 6 of the ECHR. Although the defence argued for more access to the technical methods used in interception, the court ruled that transparency in the case file and mutual trust between EU states were sufficient to maintain the fairness of the trial.³² A critical development related to these issues is the ruling by the Court of Justice of the European Union (CJEU) in Case C-670/22 (*M.N. - EncroChat*), which addresses key aspects of the European Investigation Order (EIO) under Directive 2014/41/EU. Art. 6(1) of Directive 2014/41 allows a public prosecutor to issue an EIO to transmit evidence already held by the executing State's authorities if it meets the issuing State's domestic legal conditions, even when the evidence involves intercepted, encrypted telecommunications obtained in the issuing State.³³ It clarifies that an EIO for transmitting already obtained evidence does not need to be issued by a judge if national law allows a public prosecutor to do so. Furthermore, it affirms that telecommunications interception must be notified to the concerned Member State to protect the rights of affected individuals. Evidence must be excluded if the accused cannot comment effectively on it.³⁴ Therefore, it is possible to use evidence obtained legally under the laws of an EU member state, such as through mass interception, and subsequently request this evidence through the EIO framework. This allows the evidence to be introduced and used in court proceedings of the state that initially requested it, even if the method of evidence acquisition differs from its legal standards. This practice raises a significant concern regarding forum shopping in evidence collection, where authorities may seek out jurisdictions with more permissive evidence-gathering laws to bypass stricter national standards.³⁵ This tactic can undermine the fairness of proceedings, as it may limit the defence's ability to challenge the legality and admissibility of evidence collected

31 Burić et al., 2023, pp. 244–245.

32 Hoge Raad der Nederlanden, ECLI:NL:HR:2024:192, 2024, paras. 2.2.–2.4.

33 CJEU, Criminal proceedings against M.N. (*EncroChat*), 2024, para. 106.

34 Ibid., paras. 77, 119, 131.

35 Burić et al., 2023, p. 266.

through processes not typically allowed in the jurisdiction where the trial takes place. Such practices highlight the need for harmonised EU regulations on evidence admissibility to prevent imbalances in rights protections across different legal systems.

3.1.2. ANOM

ANOM, covertly operated by the Federal Bureau of Investigation (FBI) and Australian Federal Police, intercepted over 27 million messages from approximately 12,000 users in more than 90 countries.³⁶ Defence teams, particularly in Finland, questioned the legality of this evidence, arguing that it breached privacy protections under national and EU law. In KKO case 2023:14, the Finnish Supreme Court admitted ANOM messages into evidence despite privacy violations under Art. 8 of the ECHR, which protects the right to privacy in communication. The court reasoned that the relevance of the messages to organised crime outweighed the privacy breach, especially as the defence could challenge the evidence and its credibility.³⁷ The court emphasised that even when there are privacy violations, as long as trial fairness is preserved under Art. 6, such evidence may still be admitted.³⁸ The court further acknowledged that while privacy concerns were significant, the ANOM evidence had high probative value, especially given its role in revealing organised criminal networks. The Finnish Supreme Court underscored that given the scale of the operation and serious nature of the offenses under investigation, the need to protect public safety and combat organised crime justified a degree of privacy infringement. It emphasised that as long as defendants had access to legal representation and could challenge the reliability and relevance of the evidence, the principles of fair trial rights remained intact. This decision reflects a careful balancing act between upholding individual rights and addressing the broader interests of justice in cases involving sophisticated, transnational criminal activities.

3.1.3. SKYECC

Sky ECC, another encrypted communication platform used by over 170,000 people globally, including many involved in organised crime, became the subject of a joint operation by Belgian, Dutch, and French authorities. The interception of over tens of millions of encrypted messages led to significant arrests and prosecutions.³⁹

³⁶ Europol, 2021.

³⁷ Finnish Supreme Court, KKO:2023:14, 2023, paras. 9–18.

³⁸ Ibid., paras. 52–53.

³⁹ Burić et al., 2023, pp. 243–249.

In Croatia, the use of Sky ECC data in criminal law cases raised serious legal questions. Key defence challenges focus on the privacy violations stemming from mass surveillance that intercepted communications of all users, not just suspected criminals, raising concerns under Art. 8 of the ECHR. Additionally, the lack of transparency in the investigatory methods limited the defence's ability to challenge the reliability and authenticity of evidence, impacting the right to a fair trial under Art. 6 of the ECHR.⁴⁰ Issues of cross-border evidence transfer further complicated procedural fairness. A significant legal issue arises from the fact that not all legal systems recognise bulk communication interception as a valid investigatory tool. For example, the Croatian legal framework lacks specific provisions for such broad surveillance. This creates complications when such evidence is transferred from foreign jurisdictions where it is lawful. The defence argues that bulk interceptions should be subsumed under special evidentiary actions, requiring strict procedural safeguards to protect individual rights and ensure fairness in cross-border evidence use.⁴¹ In this context, individually establishing grounds for suspicion for each person whose communications are intercepted, and ensuring each is covered by a specific warrant, would align better with the rights of the defence. Such a requirement would mandate a tailored, individualised rationale for each interception decision, enabling the defence to challenge the admissibility of evidence based on this specificity. This approach would help ensure that interception is justified on a case-by-case basis, reinforcing procedural safeguards and the rights of the individuals involved. Currently, however, the broader approach simplifies evidence gathering for law enforcement, often allowing more generalised warrants or less specific grounds for interception. While this facilitates the investigative process, it can undermine the defence's ability to scrutinise the legality and proportionality of evidence collection, potentially impacting the fairness of proceedings.

3.2. Facial Recognition Technologies

The use of biometric and facial recognition technologies has clearly expanded across various applications, from seemingly harmless smartphone unlocking to critical functions in border control, emotion recognition, and beyond.⁴² In the context of criminal prosecution, these technologies serve two primary purposes: first, to establish the identity of individuals suspected of criminal offenses, known as verification; and second, to identify persons whose identity is otherwise unknown,

40 Oerlemans and Royer, 2023, pp. 445–457.

41 Burić et al., 2023, pp. 260–265; Republic of Croatia, 2008, Criminal Procedure Code, Arts. 332–339.

42 Novokmet, Tomičić and Vidaković, 2023, pp. 526–527.

known as identification. The significant advantages of these technologies, enabled by advanced AI systems and extensive biometric databases of photos and videos, facilitate both real-time and post-event recognition. This capability is invaluable for criminal proceedings, as it enhances the accuracy and efficiency of identity verification processes.⁴³

3.2.1. Real-Time Facial Recognition

Given the inherent characteristics of facial recognition systems, it is essential to distinguish between real-time and post-event recognition. Real-time facial recognition involves the immediate identification of biometric facial features, comparing them with a predefined watchlist in just seconds to determine an individual's identity.⁴⁴ This process, however, raises significant concerns regarding accuracy; the discretionary powers involved in creating comparison lists; and the potential consequences, such as arrests and the initiation of criminal proceedings. Real-time recognition, therefore, presents a high level of intrusion into fundamental human rights and freedoms, which has led to a restrictive approach in regulatory frameworks – a topic explored further in the final chapter. The issues are well illustrated by the Court of Appeal's findings in *Edward Bridges v South Wales Police*.

In *Edward Bridges v. South Wales Police*, the Court of Appeal addressed the lawfulness of the use of automated facial recognition (AFR) technology by South Wales Police under Arts. 6 and 8 of the ECHR. The court acknowledged the intrusion into privacy caused by the use of AFR technology due to its large-scale collection of biometric data in public spaces, affecting individuals not suspected of crimes.⁴⁵ However, it deemed the surveillance proportionate to its purpose in crime prevention and provided safeguards such as prompt deletion of non-matching data and clear guidelines on watchlist criteria. This ruling reflects a balance between operational efficiency and individual rights, especially given concerns about the potential for error and the discretionary power in creating watchlists, which could affect personal freedoms. The court highlighted that such surveillance needs stringent regulation to prevent arbitrary application.⁴⁶

43 Faraldo Cabana, 2023, pp. 35–38.

44 European Union, 2024, Regulation (EU) 2024/1689, recital 17 and Art. 1(43).

45 Court of Appeal, *Bridges*, 2020, paras. 57–59.

46 Court of Appeal, *Bridges*, 2020, paras. 84, 93–108.

3.2.2. Post-Event Remote Biometric Identification System

Although post-event recognition represents a slightly lower degree of intrusion into fundamental human rights and freedoms due to the time lag in analysis, certain risks remain. This is evident in administrative decisions concerning the use of the Videmo360 system in Hamburg, and the conclusions drawn by the Data Protection Authority (DPA). Similarly, in *Glukhin v. Russia*, the European Court of Human Rights (ECtHR) highlighted issues related to the use of such systems under Art. 8 of the ECHR, underscoring the privacy risks associated with delayed biometric analysis.

In the Videmo360 DPA Hamburg case, the Hamburg DPA critically assessed the deployment of the Videmo360 facial recognition system, identifying substantive privacy concerns under Art. 8 of the ECHR. The DPA determined that while Videmo360 may enhance public security, its capacity for real-time surveillance and extensive data processing poses significant risks to individual privacy. The DPA concluded that stringent limitations on data retention and clear, narrowly defined criteria for selecting individuals for surveillance are necessary to safeguard against arbitrary monitoring and ensure that the use of such technology aligns with privacy rights.⁴⁷ The decision reflects the DPA's insistence on balancing security imperatives with robust privacy protections, especially in contexts where individuals may be surveilled without suspicion.

The ECtHR case *Glukhin v. Russia* addressed similar concerns about surveillance technologies within the framework of Art. 8 of the ECHR. The court reaffirmed that surveillance systems with the potential for broad, indiscriminate data collection must incorporate rigorous safeguards to protect individuals' privacy rights. The ECtHR stressed that such surveillance must be "in accordance with the law" and demonstrably necessary within a democratic society, particularly when affecting non-suspect individuals.⁴⁸ The ruling in *Glukhin* underscores the ECtHR's requirement that even post-event biometric technologies adhere to high standards of legality, necessity, and proportionality to prevent disproportionate intrusions into private life.

3.3. Risk Assessment Tools

Assessing the risk of recidivism is a traditional activity of both courts and law enforcement authorities. The development of technology has undoubtedly contributed to the wider use of AI tools for such assessment in criminal proceedings. In this way, and through the infiltration of technology, the transformation of criminal procedure has

47 Hamburg Data Protection Authority, 2023, pp. 9–11, 14–15, 18–19.

48 ECtHR, *Glukhin v. Russia*, 2023, paras. 49–57, 78–91.

shifted from a traditional, retrospective, and individualised model that emphasises a deliberate and personalised approach to pursuing justice and truth, to a prospective, aggregated model that includes a more efficient but impersonal and distant approach, aligning with the concept of actuarial justice.⁴⁹ According to Novokmet, Tomićić and Vinković:

'So-called actuarial risk assessment instruments (RAIs) are the most used tools that, based on pre-entered data, calculate the probability that the mentioned risk will be realized as a precondition for determining pre-trial detention. The purpose of their use is to identify, based on pre-known historical data, the patterns by which a risk assessment is performed for each individual in order to make an objective and transparent decision as to whether a person should be remanded in custody or released before the trial'.⁵⁰

The transformation to a new model under the influence of AI and new technologies aimed to achieve greater consistency, transparency, and accuracy compared with human judgement.⁵¹ Although research suggests that algorithms can make better decisions than judges and other officials, there are specific objections and challenges associated with the usage of such systems.⁵² Some of these issues were highlighted in the case *Loomis v. Wisconsin*, where the Wisconsin Supreme Court ruled that using the COMPAS risk assessment tool in sentencing did not violate due process, despite the tool's proprietary, undisclosed methodology. The court required judges to be informed of COMPAS's limitations, including its non-transparent nature and potential biases, particularly concerning minority offenders.⁵³ It also stipulated that COMPAS scores should not serve as the sole basis for sentencing but rather be part of a broader evaluative process. The defence argued that reliance on an algorithm with undisclosed methods compromised the defendant's right to an individualised sentence and accurate information, pointing to potential gender and racial biases as a violation of fair trial rights.⁵⁴ While the court acknowledged these concerns, it ultimately found that procedural safeguards were sufficient to mitigate the risks of unfairness in sentencing.

The objections highlighted above underscore criticisms of AI in criminal proceedings, underscoring issues with new, aggregated, and non-personalised models.

49 Karsai, 2021, pp. 15–16.

50 Novokmet, Tomićić and Vinković, 2022, pp. 4–6.

51 Goel et al., 2021, pp. 9–10.

52 Ibid., p. 13.

53 *Harvard Law Review*, 2017, pp. 1531–1532.

54 Ibid., pp. 1533–1535.

This concern is particularly relevant given that sentencing must be individualised, considering the unique context and circumstances of each defendant.⁵⁵ Similarly, assessments for determining or extending pre-trial detention are conducted individually, adhering to standards set by the ECtHR.⁵⁶ Such an approach, alongside the shortcomings highlighted by the defence in the analysed case, demonstrates that despite the intent to unify procedures, transparency and accuracy remain challenging aspects. These limitations directly impact the right to defence and hinder the ability to effectively challenge the outcomes produced by such systems.

4.

European Approach of AI Regulation – Balancing the Scale or Shooting in the Dark?

While technology and AI offer numerous advantages, they also introduce substantial risks, particularly for defendants. To apply these tools responsibly and minimise associated risks, effective regulation is essential. One challenge lies in the fragmented regulatory landscape, involving multiple unconnected actors attempting to govern AI use.⁵⁷ However, recent progress has been made with the adoption of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 27 April 2022, laying down harmonised rules on AI (AIA) and amending certain Union legislative acts. These regulatory frameworks will play a crucial role in shaping the application of AI in criminal proceedings in European continental law systems. The following analysis examines these regulatory approaches, focusing on balancing traditional legal principles with new technological capabilities.

4.1. EU AIA

The regulatory framework under the AIA follows a risk-based approach, initiated by the European Commission's White Paper on Artificial Intelligence, which laid the foundation for future regulations.⁵⁸ This approach aims to balance innovation with the protection of fundamental rights, as evidenced by the provisions of the AIA and its sector-specific requirements. To establish proportionate and effective binding rules for AI systems, a clearly defined risk-based framework is necessary.⁵⁹ The type and

55 Novoselec and Bojanić, 2013, p. 428.

56 ECtHR, *Šoš v. Croatia*, 2015, paras. 95–100.

57 Cihon, Maas and Kemp, 2020, pp. 546–547; Nikolinakos, 2023, pp. 353–369.

58 European Commission, 2020, White Paper on Artificial Intelligence.

59 Novokmet, Tomičić and Vinković, 2022, pp. 4–6.

content of the rules should be aligned with the intensity and scope of risks posed by AI systems. Thus, the AIA prohibits certain unacceptable AI practices, sets requirements for high-risk AI systems, and establishes transparency obligations for specific AI applications. This proportionate approach aims to balance risk reduction from AI use with the innovations and benefits AI systems bring.⁶⁰

While *Ebers* supports a risk-based approach as ideal for AI regulation, he argues that the EU's approach does not fully align with the original concept of risk-based regulation. His critique focuses on the EU's reliance on predefined, fixed risk categories for regulating AI, which lack empirical grounding and may struggle to keep pace with rapid AI advancements.⁶¹ Additionally, the European Commission's authority to update the list of high-risk systems could be influenced by political rather than empirical factors. *Ebers* advocates for a more dynamic approach, allowing risk assessments within specific contexts rather than relying on static categories.⁶²

Such an approach is also evident from the specific provisions of the relevant regulation. According to Art. 5 of the AIA, the use of remote biometric identification systems in real time in public spaces for criminal prosecution is allowed only if deemed necessary for specific objectives: locating victims of crimes such as abduction or trafficking, preventing significant and immediate threats to life or safety, or identifying suspects in serious crimes. Each instance of usage must be pre-authorised by a judicial or independent administrative authority based on objective evidence of necessity and proportionality.⁶³ In emergencies, the system may be used without prior authorisation, provided that approval is requested within 24 h; if denied, data must be immediately deleted. All usage must comply with safeguards on data protection, necessity, proportionality, and minimal data retention. Member States must establish detailed guidelines and notify relevant supervisory bodies, with the European Commission receiving aggregated annual reports to ensure adherence to fundamental rights.⁶⁴ However, systems solely intended for biometric verification, where the purpose is simply to confirm that a person is who they claim to be, are excluded from this category. Additionally, certain AI systems have been designed for biometric categorisation, which involve classifying individuals based on sensitive or protected attributes inferred from certain characteristics. Another subset includes AI systems for emotion recognition, aimed at detecting and interpreting individuals' emotional states.

The market placement, deployment, or use of AI systems for risk assessments aimed at evaluating or predicting the likelihood of a person committing a criminal

60 Cancela-Outeda, 2024, p. 3.

61 Ebers, 2024, pp. 7, 11–21.

62 Ibid.

63 Zulehner, 2024, pp. 15–16.

64 Lynch, 2024, pp. 3–4.

offense, based solely on profiling or assessments of personal traits and characteristics, is prohibited. This ban does not apply to AI systems used to support human judgement in determining a person's involvement in criminal activity, provided this assessment is based on objective and verifiable facts directly linked to criminal activity.⁶⁵ Similarly, the market placement, deployment, or use of AI systems that create or expand facial recognition databases by indiscriminately collecting facial images from the internet or CCTV footage is also prohibited.⁶⁶

According to Art. 6(2) and Annex III, 6(a-d) of the AIA, in the realm of criminal prosecution, AI systems are permitted under Union or national law for specific purposes. These include systems used by law enforcement to assess the risk of an individual becoming a victim of crime, and those employed as polygraphs or similar investigative tools. Additionally, AI can be used to evaluate the reliability of evidence in investigations or prosecutions. Some systems are further employed to assess the likelihood of an individual committing or re-committing a crime, not only based on profiling as outlined in Directive (EU) 2016/680 but also through analysis of personal traits and prior criminal behaviour of individuals or groups.

According to Arts. 9–14, high-risk AI systems are subject to strict conditions to safeguard citizens' security, privacy, and fundamental rights. Prior to deploying such systems, a comprehensive risk and impact assessment on fundamental rights must be conducted to identify potential risks to individuals and society. Transparency is essential, requiring systems to be explainable and accessible so that users can understand their outputs, facilitating the verifiability of decisions. High-risk AI systems also demand human oversight, ensuring that they do not operate autonomously without human assessment and intervention. The use of high-quality, accurate data further minimises the risk of incorrect results, which is particularly crucial in high-risk applications.

This approach classifies systems based on the risk they pose, with certain systems being prohibited, and others designated as high-risk, subject to strict conditions for their use. The primary objective is to achieve a balance between safeguarding human rights and fundamental freedoms and harnessing the potential advantages these systems can offer. This regulatory framework also encompasses systems applied within criminal proceedings, underscoring its critical importance. While the current sectoral approach is suitable, future regulation, potentially in the form of a directive or another more adaptable instrument, may be necessary to address the specific complexities associated with AI use in criminal proceedings.

65 Regarding predictive policing systems for individual profiling, see Rossbach, 2023, p. 169.

66 Ibid.; Lala, 2024, pp. 42–43.

4.2. Council of Europe Framework Convention on AI and Human Rights, Democracy, and the Rule of Law

The Council of Europe's AI Framework Convention represents a ground-breaking development in international AI governance, setting a precedent as the first legally binding treaty dedicated to AI. Anchored in a human rights-based approach, this AI Framework Convention seeks to address the fundamental risks AI poses to human rights, democracy, and the rule of law. It envisions an AI regulatory landscape grounded in the principles of privacy, transparency, and non-discrimination.⁶⁷ This approach notably aligns AI regulation with pre-existing human rights frameworks, ensuring that the expansion of AI technologies does not come at the cost of individual rights and social justice. A unique characteristic of the AI Framework Convention lies in its global applicability and jurisdictional reach. While current AI regulations, such as the AIA, apply regionally, the AI Framework Convention has the potential to reach beyond Europe. The current signatories, in addition to the EU, include the United States of America (USA), the United Kingdom (UK), Israel, Norway, and other countries. This represents a broad coalition of states that have accepted two identical definitions of AI, encompassing some of the leading countries in AI development, such as the USA, Israel, and the UK.⁶⁸ With active participation from states outside the EU, it promises a level of harmonisation in AI governance previously unattained in this field. Such global applicability is particularly apt for AI technologies that inherently cross borders, affecting multiple jurisdictions through their expansive data processing, decision-making capabilities, and implications for personal privacy. Consequently, the Convention addresses the cross-border challenges associated with AI, from data protection to issues of accountability in digital environments, while aiming to set a consistent standard for AI development and deployment on an international scale.

Another critical dimension of the AI Framework Convention is its commitment to a full lifecycle regulation – an approach that governs AI systems through each stage of their existence, from design and development to application and decommissioning. By encompassing every phase, the Framework Convention ensures that regulatory oversight extends to adaptive AI systems that may evolve in ways unforeseen at the initial deployment stage. Such a lifecycle approach thus fosters a framework of accountability, ensuring that AI technologies always meet established ethical and legal standards, particularly as these systems integrate deeper into decision-making

67 Van Kolschooten and Shachar, 2023, pp. 2–4.

68 Council of Europe, 2024, Chart of signatures and ratifications of Treaty 225 – Framework Convention on Artificial Intelligence.

processes that directly impact individuals.⁶⁹ Nonetheless, the broad, sector-neutral scope of the AI Framework Convention brings both advantages and challenges. While the sector neutrality of the Convention positions it as a flexible, cross-sectoral regulatory framework, this general approach may fail to fully capture the nuanced risks AI poses in specific domains.⁷⁰ For instance, AI applications in particular contexts may require specialised provisions to address unique ethical, legal, or technical concerns. The absence of sector-specific guidelines in the Convention could limit its efficacy in translating general human rights principles into targeted protections within highly specialised or sensitive domains.

It may significantly impact specific aspects of criminal procedure, especially traditional aspirations for procedural efficiency and the protection of defence rights. The AI Framework Convention, emphasising human rights protection through mandatory risk assessments and adherence to principles of transparency, privacy, and non-discrimination, has the potential to enhance safeguards for individuals involved in criminal proceedings. A key feature of this regulation is its potential to protect the rights of suspects and defendants via a mandatory risk assessment conducted before AI systems are applied in a criminal context. In criminal proceedings, this regulation could mandate that AI tools used during investigation, evidence analysis, and even sentencing undergo strict ethical and legal evaluations. Such requirements may influence traditional processes, particularly where AI tools might otherwise jeopardise the right to a fair trial, access to defence, or individual privacy. Moreover, the transparency obligation imposed by the regulation may limit the use of *black box* AI systems, namely, those whose decision-making processes are not easily explainable or accessible to defendants or their legal teams. By enforcing transparency, the regulation helps guard against potential biases or errors in automated systems, which is critical in procedures impacting individual freedom and rights. This emphasis also aligns with broader principles of fairness and public accountability in criminal proceedings.

In summary, the Council of Europe's AI Framework Convention is a critical, unprecedented step in establishing a human rights-centred regulatory framework for AI.⁷¹ With its full lifecycle approach, international reach, and foundation in fundamental rights, it has the potential to shape the global landscape of AI governance. However, its broad scope and ambitious objective to serve as a universally applicable instrument underscore the importance of balancing flexibility with specificity, ensuring that the Convention remains both impactful and resilient amid the evolving demands of global AI regulation. While the current form of the AI Convention

69 Council of Europe, 2024, Explanatory Report to the Council of Europe Framework Convention, p. 6, paras. 23–25.

70 Smuha, 2020, pp. 591–604.

71 Niklas, 2021, pp. 528–530.

provides a framework for safeguarding rights within criminal proceedings, its effectiveness in this realm will depend on how specifically it is applied to criminal justice AI systems.

5.

Discussion and Conclusion

Since the earliest stages of criminal procedural law development, external factors have continually shaped criminal procedures. Although some traditional influences persist, a new disruptive factor has emerged, facilitated by technological advancement – namely, AI. To assess whether AI indeed qualifies as a disruptive factor, it is essential to establish its presence and role within modern criminal proceedings. Recent judicial cases demonstrate the use of encrypted communication content as evidence, particularly in cases involving platforms such as ANOM, SKY ECC, and EncroChat. While this study examines only a selection of examples, the substantial number of arrests, suspects, asset confiscations, and other outcomes suggests that these technologies are becoming integral to modern investigative practices.⁷² Similarly, facial recognition technologies have broadened in application, not only within commercial domains but also significantly within criminal investigations and law enforcement. Cases such as *Edward Bridges v. South Wales Police* and *Videmo360* exemplify the legal and procedural implications of these systems.⁷³ Beyond these cases, numerous examples reflect the growing reliance on facial recognition by law enforcement agencies. In the Netherlands, systems including CATCH are employed for real-time surveillance, while in Croatia, law enforcement is currently implementing similar technologies for police use.⁷⁴ In addition to identification purposes, these technologies are increasingly used for tracking and evidentiary purposes, which can raise significant concerns. Given the expanding presence of cameras and surveillance systems, it is evident that both the quality and frequency of these technologies in criminal proceedings are unlikely to decrease. Among the listed AI-driven systems, risk assessment tools were among the earliest to be integrated into criminal procedure. Notably, *Loomis v. Wisconsin* stands as a landmark case regarding the application of COMPAS, although many similar systems now exist. If we consider predictive policing systems as a subset of risk assessment tools, these applications have the longest and most extensive presence in criminal proceedings, as supported by judicial precedents. Moreover, when factoring in relatively benign systems, such

⁷² Burić et al., 2023, pp. 244–249.

⁷³ Novokmet, Tomičić and Vidaković, 2023, pp. 548–549.

⁷⁴ Montag et al., 2021, pp. 61–67.

as those for transcribing statements from witnesses, defendants, and experts, and tools for researching case law and even legal assistance bots, it becomes evident that AI is embedded in criminal procedure. The presence of AI in this field is poised only to increase, making it an influence that cannot and should not be ignored.

The previous conclusions are supported by the existence of numerous global, supranational, regional, and national initiatives aimed at regulating AI and its applications. While not all initiatives specifically address the use of AI in criminal proceedings, two of the most significant regulatory frameworks – the AIA and AI Framework Convention – demonstrate a concerted effort to mitigate the risks posed by AI to fundamental human rights and freedoms. The EU's risk-based approach in the AIA underscores the necessity of balancing the risks and benefits of AI, particularly highlighting the high-risk nature of AI systems used by law enforcement. Certain AI applications are outright prohibited, while others are permitted only under strict conditions.

Through this regulatory framework, covering the 27 EU member states and the broader European legal context, a clear message is conveyed: the use of AI in criminal proceedings must be regulated to safeguard individual rights. This regulation substantiates the argument that AI profoundly impacts modern criminal procedure. Provisions within Arts. 5 and 6 of the AIA outline prohibitions on specific high-risk AI uses, as detailed in Annex III. Additionally, Arts. 9–14 set out stringent requirements for high-risk systems, demonstrating the recognition that certain AI applications carry risks too substantial for unregulated implementation in criminal contexts. This approach and regulatory framework highlight the significant influence of AI systems in favour of state authorities, specifically in the context of criminal prosecution. This influence requires careful limitation, as excessive discretion in AI usage can tilt the balance towards state authority, often at the expense of defendants' rights, thus favouring the efficiency of prosecution over the right to defence. The Council of Europe's regulation is equally crucial and holds broader influence, as several non-EU countries, including the USA and Israel, have joined and signed the AI Framework Convention. The approach to AI regulation is not sector-specific, meaning there are no unique provisions solely for criminal proceedings. However, the key principle lies in applying regulatory standards to the entire lifecycle of AI systems, which plays a vital role in balancing fundamental human rights and freedoms with the benefits and risks of AI use. This inclusive approach consequently encompasses AI systems used in criminal proceedings as well. While there are criticisms of human rights as an imperfect concept,⁷⁵ and consequently of this regulatory approach, the alignment between the Council of Europe's regulation and the EU's framework, especially per Art. 1 of the AI Framework Convention, creates a comprehensive approach to AI

75 Smuha, 2020, pp. 91–104.

governance. This framework seeks to mitigate the efficiency-driven risks posed by AI while strengthening protections for human rights and fundamental freedoms. Within the context of criminal procedure, it is essential that the utility and efficiency of AI systems align with the objective of ensuring an effective defence. As such, the following critical question remains: Have these legal frameworks achieved an adequate balance between leveraging AI's benefits and safeguarding defendants' rights within criminal proceedings?

The introduction of AI in criminal proceedings raises the question of whether it disrupts the relative balance of traditional principles in today's mixed-type criminal procedure. Addressing this issue requires an examination of both the technical characteristics and legal challenges associated with AI technologies, as highlighted by judicial decisions regarding three primary categories of systems. One key category involves systems used to decrypt, intercept, and admit encrypted communications as evidence, which has generated a host of legal questions. First, transnational investigations, often involving cooperation across multiple continents, pose challenges regarding the control and legality of actions performed across different jurisdictions. This issue is further complicated by differences in legal frameworks governing the mass interception of communications, as not all systems regulate this concept in the same way. This discrepancy raises significant questions about the legality of evidence acquisition and its admissibility when transferred for use in national courts, especially in countries that were not directly involved in investigative and joint actions. Consequently, these legal complexities place a heavier burden on the defence, requiring familiarity not only with domestic criminal law but also with EU law and the laws of multiple foreign jurisdictions. This added layer of complexity can place defendants at a disadvantage, particularly in ensuring that evidence used against them complies with legal standards across varied legal systems. Assuming the legality of the evidence obtained, the sheer volume of intercepted data often poses a major challenge for the defence, as it may consist of hundreds of millions of messages. According to ECtHR practices, unrestricted access to all data for the defence is typically unfeasible.⁷⁶ Additionally, even if such access were permitted, few law firms have the resources required for such extensive review. This volume of data complicates the duty of the state attorney and court to identify facts both harmful and favourable to the defendant, as not all data may be incriminating.⁷⁷ Recognising this issue, the ECtHR has endorsed the involvement of the defence in developing criteria for searching relevant data to ensure an effective defence.⁷⁸ A second issue arises from the lack of transparency in decryption technologies. For instance, in the ANOM

⁷⁶ ECtHR, *Rook v. Germany*, 2019, paras. 65–69.

⁷⁷ Republic of Croatia, 2008, Criminal Procedure Code, Art. 9(1).

⁷⁸ ECtHR, *Sigurður Einarsson and Others v. Iceland*, 2019, paras. 90–91.

cases, the FBI did not disclose technical details of its decryption systems, which prevents the defence from challenging the validity of technical evidence, an essential part of the right to a fair trial. Access to source code for independent verification remains a significant barrier. Even if this obstacle could be resolved, few experts are equipped to analyse such complex systems, and the costs associated with their services are substantial. Furthermore, the duration required for thorough technical examinations could extend the criminal proceedings beyond legally acceptable limits, thus disadvantaging the defendant by delaying the resolution of their case. The lack of qualified experts in smaller countries presents a disproportionate burden on the defence, often necessitating the search for experts outside national borders. The challenge of explainability in AI systems is also a significant issue; the processes and operational mechanics of these systems are often opaque, and if they cannot be clearly explained, or if access to the source code is restricted or there is a lack of qualified experts to interpret it, the defence's options become considerably limited. Although these communication tools are generally available as legal applications, they might benefit defendants in some cases, potentially aiding the commission of offenses. However, their decryption and use as evidence threatens not only the right to defence, an essential element of the right to a fair trial under the ECHR, but also the right to privacy in correspondence, as enshrined in Art. 8 of the Convention. The utilisation of these systems by criminal prosecution agencies marks a substantial advancement, enabling quicker evidence collection, enhanced mobility across jurisdictions, and the opportunity to operate within legal frameworks that may favour prosecution, often leading to so-called forum shopping for evidence as *Burić et al.* noted.⁷⁹ Consequently, it is evident that prosecution bodies are becoming significantly more effective, encountering fewer obstacles in evidence gathering than traditional methods, which presents new challenges for the defence. Therefore, the emphasis has shifted markedly towards prosecutorial efficiency.

Facial recognition technology has diverse applications, from verifying a person's identity to detecting emotions or facial expressions, and potentially assessing the truthfulness of statements. However, the most contentious use is real-time facial recognition, where decisions are made almost instantaneously based on recognition results. This rapid processing poses risks, as system accuracy remains questionable, and any immediate response can lead to invasive actions against individuals. Given these concerns, the AIA takes a restrictive stance, limiting the use of such technology. Accuracy issues are especially problematic. As highlighted in the case *Edward Bridges v. South Wales Police*, it is essential to delete personal data immediately if individuals not actively under identification are involved; however, this requirement complicates accuracy checks. Regarding criminal procedure, real-time facial recognition

⁷⁹ Burić et al., 2023, p. 266.

should be excluded from procedural stages where the *in dubio pro reo* principle applies, as this technology cannot guarantee 100% accuracy. Novokmet, Tomičić, and Vidaković argue that such inaccuracies render it incompatible with the presumption of innocence.⁸⁰ Another concern is the considerable discretion granted to police in deploying these systems and compiling watchlists of potential suspects. This degree of control allows authorities to determine which individuals are targeted by the system, raising questions about proportionality, oversight, and potential biases in law enforcement. Individuals are typically unaware that they are on surveillance lists or subject to recognition by facial recognition systems, nor are they given the opportunity to challenge the results. Such systems can be integrated with smart devices, such as cameras and doorbells, allowing access to civilian-recorded databases. If a dispute arises, the defence may rely on an expert to interpret technical aspects – a complex and resource-intensive task. Another issue involves the retention of recordings and their potential use for prosecutorial purposes. For example, if individuals participating in protests are identified by these systems, they may experience a chilling effect on their freedom of expression, as the possibility of future criminal charges may discourage their participation. This resembles a modern, adapted form of the historical legal concept of *absolutio ab instantia*, where suspicion based on pre-existing evidence could trigger new investigations or even criminal proceedings. While, in theory, such systems might benefit the defence by confirming that the defendant's identity is distinct from the perpetrator's, they overwhelmingly serve law enforcement. These technologies enable authorities, particularly the police, to analyse large crowds and act based on recognition results without the individuals' knowledge. The restrictions in the AIA regarding real-time recognition are thus a positive step towards rebalancing the scales between prosecutorial efficiency and the defendant's rights to robust defence.

Assessing the risk of re-offending or offending for the first time is a complex and contentious task, even without AI. Any risk assessment has significant implications, potentially affecting measures from pre-trial detention to restrictions through precautionary conditions. The transparency of AI systems in this context is particularly problematic; even if the decision-making parameters of AI were understood, the defence would still face challenges in contesting the evaluation criteria. For an effective defence, it is essential to know and comprehend the AI's decision-making basis; yet, algorithmic processes inherently lack the individualisation central to criminal procedural principles. Risk assessments for criminal justice decisions are expected to be case-specific, particularly in the determination of penalties. The highly algorithmic nature of AI in these assessments can undermine this expectation, making it extremely difficult for the defence to challenge decisions, especially

80 Novokmet, Tomičić and Vidaković, 2023, pp. 557–559.

compared with traditional judgments that the court is required to explain thoroughly – a requirement the ECtHR has established as a foundational standard for fair proceedings.⁸¹ This situation raises the possibility of automating court decisions, which poses risks to judicial independence and fairness. The AIA addresses this concern by classifying systems used as decision-support tools for such judicial determinations as high-risk in Art. 6(2) and ANNEX III(8)(a). This classification aims to enhance oversight and mitigate risks associated with over-reliance on automated systems in legal settings. Beyond criminal law, the *SCHUFA* case offers relevant insights. The CJEU underscored that AI-based auxiliary tools, here in the context of credit scoring, can qualify as automated decisions if they operate without adequate human oversight.⁸² This perspective reinforces the importance of human control in decisions influenced by AI, regardless of the specific domain. Extending this to predictive policing, where systems forecast potential offenders, victims, or crime locations, the AIA takes a cautious approach by limiting individual profiling. Specifically, the AIA restricts profiling individuals as potential criminals, deeming it appropriate only as an auxiliary tool to support human judgement based on verified and objective facts. This regulatory step aims to prevent over-reliance on AI predictions and ensure that such decisions remain grounded in human assessment, thus safeguarding against the erosion of individual rights in criminal proceedings. In essence, these systems generate suspects for actions that have not been committed, and that may never be, without extending the rights typically afforded to suspects. Consequently, any associated risk assessment falls upon the defendant, and the opacity, lack of explanations, and inherent *black box* nature of these systems further complicate their position. While these technologies significantly boost efficiency, allowing for a less personalised approach to risk assessment and streamlining processing for courts and law enforcement, this efficiency often comes at the expense of individual rights. In cases of individual profiling, the person being assessed remains unaware of their status and of the rights that would apply to them as a formal suspect.

The application of AI systems in criminal proceedings is set to expand both in quality and quantity, offering increasing appeal for criminal prosecution bodies and courts due to their advantages. These developments are reshaping traditional criminal procedure, pressing modern criminal law to seek adjustments to accommodate and regulate such technologies. Current regulatory attempts, though largely sectoral, represent positive steps towards balancing efficiency with the traditional principles of criminal law. However, the use of AI remains largely skewed towards enhancing prosecutorial effectiveness, placing the defence in a more challenging position. This

81 ECtHR, *Peša v. Croatia*, 2010, para. 91; ECtHR, *Perica Oreb v. Croatia*, 2013, paras. 107–108; ECtHR, *Orban v. Croatia*, 2013, para. 51.

82 CJEU, *OQ v Land Hessen, SCHUFA Holding AG*, 2023, paras. 40–50.

imbalance is evident in the regulatory efforts that, while aiming to preserve human rights and freedoms, reflect a clear tilt towards supporting the prosecution. The defence's position is weakened as AI systems grant prosecutorial bodies enhanced tools for investigation and evidence gathering, often with limited transparency and accountability. Within the framework of the ECtHR, the concept of human rights and freedoms is upheld; yet, the need to limit or even restrict AI use indicates its profound impact, effectively granting prosecutorial authorities a higher level of efficiency, often at the expense of the defendant's right to a robust defence.

Bibliography

- Bayer, V. (1995) *Kazneno procesno pravo – odabrana poglavlja, Knjiga II. Povijesni razvoj kaznenog procesnog prava*. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske.
- Beccaria, C. (1990) *O zločinima i kaznama*. 2nd expanded and revised edn. Translated by Cvitanić, A. Biblioteka znanstvenih djela, vol. 57. Split: Književni krug.
- Burić, Z., Engelhart, M., Novokmet, A., Roksandić, S. (2023) 'Upotrebljivost rezultata masovnog nadzora komunikacije kao dokaza u hrvatskom kaznenom postupku – slučaj SKY ECC', *Hrvatski ljetopis za kaznene znanosti i praksu*, 30(2), pp. 243–274; <https://doi.org/10.54070/hlj.30.2.2>.
- Cancela-Outeda, C. (2024) 'The EU's AI Act: A framework for collaborative governance', *Internet of Things*, 27, Article 101291; <https://doi.org/10.1016/j.iot.2024.101291>.
- Cihon, P., Maas, M.M., Kemp, L. (2020) 'Fragmentation and the Future: Investigating Architectures for International AI Governance', *Global Policy*, 11(5), pp. 545–566; <https://doi.org/10.1111/1758-5899.12890>.
- Damaška, M. (1995) 'Izazovi slobodnoj ocjeni dokaza', *Hrvatski ljetopis za kazneno pravo i praksu*, 2(1), pp. 41–55.
- Damaška, M. (2001a) 'Models of Criminal Procedure', *Zbornik Pravnog fakulteta u Zagrebu*, 51(3–4), pp. 477–516.
- Damaška, M. (2001b) *Dokazno pravo u kazneno postupku: oris novih tendencija*. Zagreb: Pravni fakultet u Zagrebu, Poslijediplomski studij iz kaznenopravnih znanosti.
- Damaška, M. (2013) 'Potraga za pravičnim postupkom u doba inkvizitorne procedure', *Hrvatski ljetopis za kazneno pravo i praksu*, 20(1), pp. 167–202.
- Damaška, M. (2021) *Dokaz Krivnje: Od rimsko-kanonskog do suvremenog prava*. Zagreb: Školska knjiga.
- Derenčinović, D., Dragičević Prtenjača, M. (2022) 'Croatia: National Regulations in the Shadow of a Common Past' in Váradi-Csema, E. (ed.) *European Challenges and Central European Responses in the Criminal Science of the 21st Century*. Miskolc – Budapest: Central European Academic Publishing, pp. 71–98; https://doi.org/10.54171/2022.evcs.cls_3.
- Ebers, M. (2024) 'Truly Risk-Based Regulation of Artificial Intelligence - How to Implement the EU's AI Act', *SSRN Electronic Journal*, pp. 3–30; <https://doi.org/10.2139/ssrn.4870387>.

- Europol (2021) '800 criminals arrested in biggest-ever law enforcement operation against encrypted communication'. [Online]. Available at: <https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication> (Accessed: 28. October 2024).
- Faraldo Cabana, P. (2023) 'Technical and legal challenges of the use of automated facial recognition technologies for law enforcement and forensic purposes' in Završnik, A., Simončič, K. (eds.) *Artificial Intelligence, Social Harms and Human Rights: Critical Criminological Perspectives*. Cham: Palgrave Macmillan, pp. 35–54; https://doi.org/10.1007/978-3-031-19149-7_2.
- Goel, S., Shroff, R., Skeem, J., Slobogin, C. (2021) 'The accuracy, equity, and jurisprudence of criminal risk assessment' in Vogl, R. (ed.) *Research Handbook on Big Data Law*. Cheltenham: Edward Elgar Publishing, pp. 9–28; <https://doi.org/10.4337/9781788972826.00007>.
- Hamburg Data Protection Authority (2023) *Prüfbericht zur Gesichtserkennungssoftware Videmo360*. Hamburg: Hamburg Data Protection Authority. [Online]. Available at: <https://www.datenschutz-hamburg.de> (Accessed: 28. October 2024).
- *Harvard Law Review* (2017) 'State v. Loomis, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing', *Harvard Law Review*, 130(5), pp. 1530–1537.
- Iustinianus. (1963) *Digesta*. Krueger, P. and Mommsen, T. (eds.) 2. Nachdruck der Ausg. Berlin 1963. Hildesheim; Berlin: Weidmann.
- Karsai, K. (2021) 'Algorithmic Decisions within the Criminal Justice Ecosystem and their Problem Matrix', *Revue Internationale de Droit Pénal*, 92(1), pp. 13–30.
- Kaspar, J., Harrendorf, S., Butz, F., Höffler, K., Sommerer, L., Christoph, S. (2023) 'Artificial Intelligence and Sentencing from a Human Rights Perspective' in Završnik, A. and Simončič, K. (eds.) *Artificial Intelligence, Social Harms and Human Rights, Critical Criminological Perspectives*. Cham: Palgrave Macmillan, pp. 3–34; https://doi.org/10.1007/978-3-031-19149-7_1.
- Krapac, D. (1994) 'Kako odabrati tip kaznenog postupka za 2000. godinu?', *Zbornik Pravnog fakulteta u Zagrebu*, 44(5–6), pp. 517–528.
- Krapac, D. (1995) *Engleski kazneni postupak*. Zagreb: Pravni fakultet u Zagrebu.
- Krapac, D. (2020) *Kazneno procesno pravo*. Prva knjiga: Institucije. 8th edn. Zagreb: Narodne novine.
- Lala, F. (2023) 'Data Collection via Web Scraping: Privacy and Facial Recognition after Clearview', *i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 16(2), pp. 34–45; <https://doi.org/10.6092/issn.1825-1927/18872>.
- Levy, E. (1938) 'Statute and Judge in Roman Criminal Law', *Washington Law Review*, 13(4), pp. 291–304.

- Lynch, N. (2024) 'Facial Recognition Technology in Policing and Security–Case Studies in Regulation', *Laws*, 13(3), pp. 1–14; <https://doi.org/10.3390/laws13030035>.
- Ljubanović, V., Novokmet, A., Tomičić, Z. (2020) *Kazneno procesno pravo: izabrana poglavlja*. Osijek: Pravni fakultet Osijek.
- Montag, L., Mcleod, R., De Mets, L., Gault, M., Rodger, F., Peřka, M., (2021) *The Rise and Rise of Biometric Mass Surveillance in the EU: A Legal Analysis of Biometric Mass Surveillance Practices in Germany, the Netherlands, and Poland*. Brussels: European Digital Rights (EDRI). [Online]. Available at: https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf (Accessed: 30 October 2024).
- Mousourakis, G. (2021) 'Crime, Criminal Justice, and the Jury Courts in Late Republican Rome', *The Hiroshima Law Journal*, 45(2), pp. 164–204; <https://doi.org/10.15027/51609>.
- Niklas, J. (2021) 'Human Rights–Based Approach to AI and Algorithms: Concerning Welfare Technologies', in Barfield, W. (ed.) *The Cambridge Handbook of the Law of Algorithms*. Cambridge: Cambridge University Press, pp. 271–290.
- Nikolinakos, N.Th. (2023) *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies – The AI Act*. Cham: Springer; <https://doi.org/10.1007/978-3-031-27953-9>.
- Novokmet, A., Tomičić, Z., Vidaković, I. (2023) 'Facial recognition technology in EU criminal justice – human rights implications and challenges', *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 7, pp. 525–570; <https://doi.org/10.25234/eclic/27461>.
- Novokmet, A., Tomičić, Z., Vinković, Z. (2022) 'Pretrial risk assessment instruments in the US criminal justice system–what lessons can be learned for the European Union?', *International Journal of Law and Information Technology*, 30(2), pp. 1–22; <https://doi.org/10.1093/ijlit/eaac006>.
- Novoselec, P., Bojanić, I. (2013) *Opći dio kaznenog prava*. 4th edn. Zagreb: Pravni fakultet Sveučilišta u Zagrebu.
- Oerlemans, J.-J., Royer, S. (2023) 'The future of data-driven investigations in light of the Sky ECC operation', *New Journal of European Criminal Law*, 14(4), pp. 434–458; <https://doi.org/10.1177/20322844231212661>.
- Quattrocchio, S. (2020) *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*. Cham: Springer; <https://doi.org/10.1007/978-3-030-52470-8>.
- Roodt, C. (2004) 'A Historical Perspective on the Accusatory and Inquisitorial System', *Fundamina: A Journal of Legal History*, 10, pp. 136–157.
- Rossbach, N. (2023) 'Innocent Until Predicted Guilty: How Premature Predictive Policing Can Lead to a Self-fulfilling Prophecy of Juvenile Delinquency', *Florida Law Review*, 75(1), pp. 167–194.

- Simović, M., Šikman, M. (2023) 'Sadržaj šifrovane komunikacije (Ennetcom, Encro-Chat, Sky.ecc, ANOM, Exclu) kao dokaz u krivičnom postupku', *Pravo i Pravda*, 21(1), pp. 227–254.
- Smuha, N. A. (2020) 'Beyond a Human Rights-based approach to AI Governance: Promise, Pitfalls, Plea', *Philosophy and Technology*, 33(4), pp. 91–104; <https://doi.org/10.1007/s13347-020-00403-w>.
- van Kolschooten, H., Shachar, C. (2023) 'The Council of Europe's AI Convention (2023–2024): Promises and Pitfalls for Health Protection', *Health Policy*, 138, pp. 1–5; <https://doi.org/10.1016/j.healthpol.2023.104935>.
- Završnik, A. (2018) 'Big data: What Is It and Why Does It Matter for Crime and Social Control?', in Završnik, A. (ed.) *Big Data, Crime and Social Control*. London: Routledge, pp. 3–28; <https://doi.org/10.4324/9781315395784-1>.
- Zulehner, B. (2024) 'EU Artificial Intelligence Act: Regulating the Use of Facial Recognition Technologies in Publicly Accessible Spaces', *European Union Law Working Paper No. 91*. Stanford-Vienna Transatlantic Technology Law Forum, pp. 1–37. [Online]. Available at: <http://tllf.stanford.edu>. (Accessed: 28. October 2024).

Legislation

- Council of Europe (2024) 'Chart of signatures and ratifications of Treaty 225: Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225)'. [Online]. Available at: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyenum=225> (Accessed: 29 September 2024).
- Council of Europe (2024) *Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Council of Europe Treaty Series No. 225. Strasbourg: Council of Europe. [Online]. Available at: <https://rm.coe.int/1680afae67> (Accessed: 29 September 2024).
- European Commission (2020) *White Paper on Artificial Intelligence: A European approach to excellence and trust*. COM (2020) 65 final. Brussels: European Commission. [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065> (Accessed: 28 October 2024).
- European Union (2024) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) No 2018/858, (EU) No 2018/1139 and (EU) No 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Official Journal of the European Union, OJ L, 2024/1689, 12 July 2024. [Online]. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (Accessed: 28 October 2024).

- Republic of Croatia (2008) Criminal Procedure Code, Official Gazette Nos. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19, 130/20, 80/22 and 36/24.

Case law

- European Court of Human Rights (2010) Peša v. Croatia, Application no. 40523/08, judgment of 8 April 2010.
- European Court of Human Rights (2013) Perica Oreb v. Croatia, Application no. 20824/09, judgment of 31 October 2013.
- European Court of Human Rights (2013) Orban v. Croatia, Application no. 56111/12, judgment of 19 December 2013.
- European Court of Human Rights (2015) Šoš v. Croatia, Application no. 26211/13, judgment of 1 December 2015.
- European Court of Human Rights (2019) Sigurður Einarsson and Others v. Iceland, Application no. 39757/15, judgment of 4 June 2019.
- European Court of Human Rights (2019) Rook v. Germany, Application no. 1586/15, judgment of 25 July 2019.
- European Court of Human Rights (2023) Glukhin v. Russia, Application no. 11519/20, judgment of 4 July 2023.
- Court of Justice of the European Union (2023) OQ v Land Hessen, SCHUFA Holding AG, Case C-634/21, judgment of 7 December 2023, ECLI:EU:C:2023:957.
- Court of Justice of the European Union (2024) Criminal proceedings against M.N. (EncroChat), Case C-670/22, judgment of 30 April 2024, ECLI:EU:C:2024:372.
- Court of Appeal of England and Wales (Civil Division) (2020) R (on the application of Bridges) v Chief Constable of South Wales Police and Others, [2020] EWCA Civ 1058, judgment of 11 August 2020.
- Finnish Supreme Court (2023) KKO:2023:14 – Admission of ANOM messages into evidence, Diary no. R2022/712, judgment of 23 February 2023, ECLI:FI:KKO:2023:14.
- Hoge Raad der Nederlanden (2024) ECLI:NL:HR:2024:192, judgment of 13 February 2024.

