2024

ARTIFICIAL INTELLIGENCE AND ORGANISED CRIME

AI ACTION SUMMIT

EL PACCTO 2.0
EU-LAC Partnership on justice and security

Funded by the European Union

Edition: EL PACCTO 2.0 programme
Calle Almansa 105
28040 Madrid, Spain.

Coordinated by:

Marc Reina Tortosa
Senior Executive Manager of EL PACCTO 2.0
Emilie Breyne
Project Officer of EL PACCTO 2.0

Authors:

Cristos Velasco, Jean Garcia Periche, Juan De Dios Gómez Gómez y Miguel Bueno Benedí

With reviewing by:

Alfonso Peralta Gutiérrez

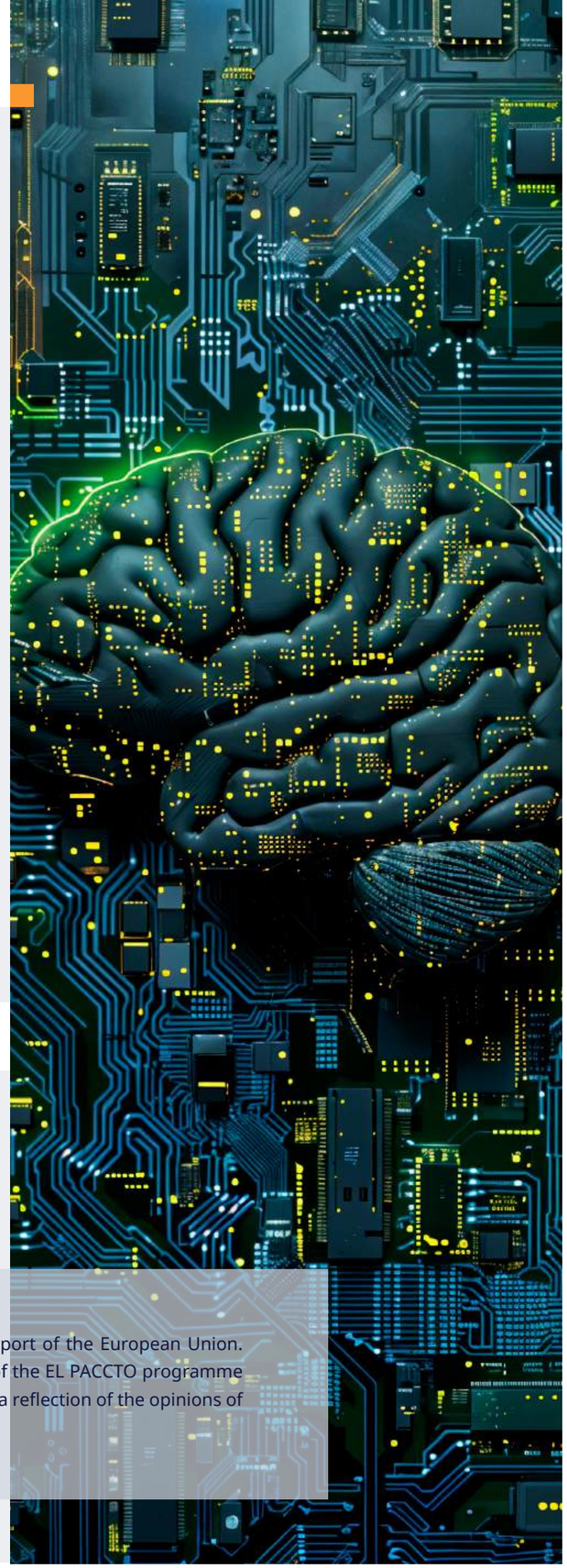
This document was produced with the contribution of the following institutions:

Expertise France

Foundation for the Internationalisation of Public Administrations

DOI: 10.5281/zenodo.16740421
Non-comercial edition. Madrid, November 2024
Updated, August 2025

This document was prepared with the financial support of the European Union. The content of this publication is the responsibility of the EL PACCTO programme and its authors, and should in no way be considered a reflection of the opinions of the European Union.



INDEX

ABBREVIATIONS

AIAB	European Commission AI Advisory Board
ALC	Latin America and the Caribbean
ALPR	Automatic Licence Plate Recognition
ANDJE	National Legal Defence Agency of the State of Colombia
AVENUE	“Analysis of Video Evidence with Novel Enhanced Understanding Engine” project
AVIDICUS	“Assessment of Video-Mediated Interpreting in the Criminal Justice System“ project
IDB	Inter-American Development Bank.
BKA	Bundeskriminalamt
Blockchain	Blockchain technology
CaaS	Crime-as-a-Service
CAF	Development Bank of Latin America and the Caribbean
CAI	Council of Europe Committee on Artificial Intelligence
CEF	Connecting Europe Facility
CENIA	Chilean National Centre for Artificial Intelligence
ECLAC	Economic Commission for Latin America and the Caribbean
CEPEJ	European Commission for the Efficiency of Justice
CJI	Ibero-American Judicial Summit
CJNG	Jalisco New Generation Cartel
C4	Command, Control, Communications and Computing Centre of Colombia
DDOS	Denial of service attacks
USA	United States of America
EL PAcCTO 2.0	European, Latin American and Caribbean Technical Assistance Programme against Transnational Organised Crime
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
Frauke	“Fraud Analysis Using Knowledge Extraction” project
FRICoRe	“Fundamental Rights in Courts and Regulation” project
GDO	Organised crime groups
HRCN	High Risk Criminal Networks
AI	Artificial Intelligence
GAI	Generative Artificial Intelligence
iBorderCtrl	Project to improve border control through the use of advanced technologies
CI	Criminal investigation
iCOP	“Identifying and Catching On-line Predators” project
ILIA	Latin American Artificial Intelligence Index
INSPECTr	“Intelligence Network and Secure Platform for Evidence Correlation and Transfer” project
Interpol	International Criminal Police Organisation
JuLIA	“Justice, Fundamental Rights and Artificial Intelligence Applications” project
MARCELL	“Multilingual Resources for CEF.AT in the Legal Domain” project
ML	Machine Learning
NCMEC	National Centre for Missing and Exploited Children
OECD	Organisation for Economic Co-operation and Development
OAS	Organisation of American States
OLGA	“On-line-Strafverfahrensregister für Organisierte Kriminalität und Geldwäsche” project
UN	United Nations Organisation
PCC	Primeiro Comando da Capital
PLN	Natural Language Processing
PRISMA	Recidivism Risk Profile for Requesting Security Measures
RasS	Ransomware as a Service
REIA	European Regulation on Artificial Intelligence
ROXANNE	“Real-time network, text, and speech analytics for combating organised crime and terrorism” project
SCJN	Supreme Court of Justice of the Mexican Nation
STOA	European Parliament Panel on the Future of Science and Technology
TAJ	Traitement d’Antécédents Judiciaires
TENSOR	“Retrieval and analysis of heterogeneous data for predicting and mitigating violent actions” project
EU	European Union
UNESCO	United Nations Educational, Scientific and Cultural Organisation
UNICRI	United Nations Interregional Crime and Justice Research Institute Centre for Artificial Intelligence and Robotics
VioGén	Comprehensive Monitoring System in cases of Gender-based Violence
VMI	Video-mediated interpreting

INTRODUCTION

The adoption of AI-based systems and technologies has seen tremendous growth since the introduction of ChatGPT in November 2022. The use of AI systems is extremely useful in various areas of the economy such as education, logistics and transport and in general, in the provision of digital services for citizens. The integration of AI systems into the work and activities of security forces and authorities of the justice system, including the judiciary, is of great significance since it offers versatile and powerful tools to analyse large amounts of data, identify criminal patterns and behaviours and even more advanced issues related to predictive surveillance and the prediction of sentences against subjects accused of a crime, which allows criminal justice authorities, on the one hand, to optimise the work and effectiveness of their investigations by offering faster response times, and on the other hand, the possibility of allocating and managing human and financial resources more efficiently.

However, AI systems are also being used and exploited for the benefit of organised crime without the need for advanced technical skills or abilities. Criminals can use AI to facilitate and enhance their attacks by maximising opportunities for obtaining faster profits, exploiting new victims and creating more innovative criminal business models, while reducing the chances of being caught. For example, the automation of attacks through the use of AI-controlled bots that have the ability to boost their activities on a large scale such as denial of service attacks (DDOS), the propagation and distribution of malicious programs (malware), the identification of images on social networks to exploit victims of human trafficking or crimes of sexual abuse and exploitation, the creation of phishing emails with greater precision and with the possibility of adapting them to the specific characteristics of their victims, automation of documentary forgeries, massive violations of intellectual and industrial property, using manipulative techniques to persuade people to behave unwantingly, even trying to influence an electoral process or deceive the judge with false evidence in a trial, or the use of deepfakes to impersonate their victims and subsequently commit crimes of extortion and fraud. All of these behaviours and vectors present challenges and opportunities that authorities in the justice system must address and explore in order to offer concrete responses to victims of this type of crime.

In this context, this study aims to provide a comprehensive overview of the interactions between AI and organised crime in Latin America, the Caribbean and the European Union, giving examples of actions taken, threats or public cases, as well as existing work tools and highlighting both the dangers and opportunities presented by this technology. Furthermore, the study explores these dynamics, providing a comprehensive view of how AI is being used by both criminal groups and law enforcement in Latin America, and the social and ethical implications of this technological evolution in the field of organised crime.

In particular, the study seeks: (i) to identify the main legislative and policy developments on AI currently developed by international and regional bodies, the scope of existing legislation in the EU, and to review the current status of national strategies on AI developed mainly in LAC countries; (ii) to provide an analysis of the main conducts and crimes committed through the use of AI tools; (iii) to provide a mapping and analysis of the AI tools currently used by justice and security sector institutions in the EU and in LAC countries to strengthen the administration of justice and the fight against organised crime, and; (iv) to propose specific actions and activities to address the link between AI and crime so that they can be implemented and developed by the countries of the European Union EL PACCTO 2.0 Programme (Europe, Latin America and Caribbean Assistance Programme against Transnational Organised Crime) taking into account gender challenges and the protection of the fundamental rights of the parties in the criminal process.

The information provided is a snapshot of the current moment that must be interpreted as such since AI technology evolves very quickly and some tools, systems or applications developed and mentioned in this study may become obsolete in a matter of a few years or even months. Furthermore, crime trends vary widely from country to country and even between regions and sub-regions. However, the use of AI tools by organised crime groups (OCGs), particularly high-risk criminal networks (HRCNs), can be expected to rise, and in some cases even increase exponentially in the coming years.

BLOCK 1: ANALYSIS OF CONTEXT AND CHALLENGES

1.1. CONTEXT

Artificial intelligence (AI) has transformed multiple sectors of global society, providing new opportunities for economic and social development, as well as significant challenges, especially in the fight against organised crime. In Latin America, where organised crime has traditionally embraced activities such as drug and arms trafficking, AI has expanded the scope and sophistication of criminal operations. This technological adoption poses new challenges for law enforcement agencies, which already face limited resources and fragile institutional structures in several countries of the region.

AI has introduced new forms of crime that go beyond traditional practices. For example, Europol has pointed to Crime-as-a-Service (CaaS), which allows criminals without technical expertise access to sophisticated tools in the digital underworld, increasing their ability to carry out complex attacks[1]. This has made it easier for emerging technologies, such as AI, to become a key driver of criminal activities. Similarly, in South Africa, identity theft crimes increased by 284% between 2021 and 2022, driven by the use of AI in creating fake identities and financial fraud[2].

One particular example of sophisticated fraud linked to the use of AI occurred in China, where an individual was tricked into transferring nearly $500,000 to a scammer who used face-swapping and voice-mimicking technology to impersonate a close friend. Although the authorities managed to stop some of the money, the incident demonstrated how AI is being used to carry out high-level financial fraud[3].

In Latin America, organised crime groups have leveraged AI in a variety of ways by using advanced tools to increase the effectiveness of their operations. Drug cartels in Mexico, for example, have begun to use AI-controlled drones not only to transport drugs, but also to carry

1 Europol. (2017). Europol. European Union Serious and Organised Crime Threat Assessment (SOCTA). Retrieved from https://www.europol.europa.eu/activities-services/main- reports/european-union-serious-and-organised-crime-threat-assessment-2017.

2 ENACT, (2023) AI and organised crime in Africa. Sigsworth, R., ENACT Observer (2023). Retrieved from https://enactafrica.org/enact-observer/ai-and-organised-crime-in-africa.

3 UNODC, (2024). Casino Underground Banking Report 2024. UNODC Publications (2024). Retrieved from https://www.unodc.org/roseap/uploads/documents/Publications/ 2024/ Casino_Underground_Banking_Report_2024.pdf

out physical attacks on members of other cartels or to disrupt rival supply chains[4]. These drones have become a key tool for smuggling, allowing borders to be crossed more easily and avoiding conventional security controls. In many cases, these drones operate autonomously, which is why they have been called “the new drug mules”[5].

AI is also transforming the way cartels optimise their smuggling routes. Using machine learning models, cartels can analyse route data, border patrol schedules and shipping methods to predict the best times and locations to transport drugs, reducing the risk of detection. Furthermore, the use of face recognition systems has allowed cartels to identify undercover agents, further complicating law enforcement efforts to infiltrate these organisations.[6] In 2018, an armed drone was used to attack the home of Baja California State Public Security Secretary Gerardo Sosa Olachea in the town of Tecate, along the US-Mexico border. At least two drones appear to have been used in the attack. The first was carrying audio and video equipment, as well as two improvised explosive devices (IEDs) that failed to detonate after falling in the official’s courtyard, while the second was carrying out surveillance[7].

This possible use of remote-action robots or lethal autonomous weapons systems (LAWS), in cases of terrorism and narco-terrorism, can lead not only to indiscriminate effects and damage due to lack of significant human control, with disastrous consequences for security and human life, but also to potentially allowing members of criminal and terrorist organisations to operate remotely from the environment where an action is taking place and provide them with better personal protection in a scenario of war, explosions and, for example, in environments contaminated by chemical agents or catastrophic scenarios[8].

4 ENACT, (2023) AI and organised crime in Africa. Sigsworth, R., ENACT Observer (2023). Retrieved from https://enactafrica.org/enact-observer/ai-and-organised-crime-in-africa.

5 idem

6 National School of Political and Administrative Studies. Artificial Intelligence – a Double-Edged Sword. Organised Crime`s AI v. Law Enforcement`s AI

7 ASMANN, P. (15 August 2018). Are armed drones the weapon of the future for Mexico’s cartels? InSight Crime. https://insightcrime.org/news/brief/armed-drones-weapon-future-mexico-cartels/

8 LAMAS LOPEZ, F., & PERALTA GUTIERREZ, A. (2023). Public International Law Framework and Military Uses of Artificial Intelligence in the EU. Revista Electrónica De Estudios Internacionales, (46), 505–525. https://doi.org/10.36151/reei.46.17

Other ways in which criminal groups are using AI include exploiting satellite imagery from platforms like Google Earth to plan smuggling routes with precision, real-time monitoring of the movements of security forces and the manipulation of social networks through data mining and automatic content generation, tools that allow them to manage their operations more efficiently[9]. In a similar way to legitimate businesses, criminal organisations use AI for supply chain management and risk mitigation[10].

AI's ability to predict vulnerabilities has also been used in blackmail, extortion and defamation schemes. Traditional crimes such as extortion and terrorism are now carried out using new methods, including automated content generation, which facilitates the creation of child pornography and the manipulation of social networks to influence public opinion and protect the interests of organised crime[11]. Criminals have also begun developing their own AI software, using unrestricted models to generate malware such as ransomware, which encrypts data and demands ransoms[12].

However, law enforcement in Latin America and the Caribbean is also leveraging AI as a tool in its fight against organised crime. Technologies such as predictive analytics, pattern recognition and Automatic Licence Plate Recognition (ALPR) help law enforcement agencies to process large amounts of data such as financial records, surveillance footage and social media data, improving their ability to identify and track criminal networks.[13] Despite these advances, the capacity to effectively implement these technologies is still limited in many countries in the region, underscoring the need to strengthen institutions and resources to address the growing impact of AI on organised crime.

As criminal organisations in Latin America continue to embrace AI, traditional forms of crime such as drug trafficking, arms smuggling and money laundering are being transformed. The use of AI not only allows these groups to operate more stealthily, but also gives them the ability to scale their operations exponentially. One of the most notable examples, as we have discussed, is the use of AI-controlled drones for surveillance and the transportation of contraband across borders, allowing criminals to operate with unprecedented autonomy and bypass traditional methods of border control and surveillance. These advances not only increase the efficiency of criminal organisations, but also make the task of law enforcement more difficult.

Furthermore, AI has also facilitated the optimisation of financial frauds. Cases such as deepfakes and the automation of scams through chatbots have allowed criminals to broaden the scope of their activities. These chatbots, like LoveGPT, are capable of generating automated conversations on dating apps to emotionally scam victims, asking for money under false emergencies or presenting fraudulent investment opportunities. This type of fraud demonstrates the ability of AI not only to automate processes, but to do so on a scale that would have been impossible without theuse of technology. Furthermore, some of the most powerful criminal groups in Latin America, such as the Cártel Jalisco Nueva Generación (CJNG) in Mexico and the *Primeiro Comando da Capital* (PCC) in Brazil, are involved in this type of fraud, suggesting that the technology is not limited to small groups, but is also used by large criminal organisations.

Another key aspect is phishing, a technique that has evolved considerably thanks to advances in AI. Previously, phishing was limited to simple, easily identifiable emails. However, today criminals can personalise their messages using language patterns that imitate trusted people or institutions, increasing the success rate of these frauds. In Brazil, a cybercrime group called PINEAPPLE has used these techniques to send emails that imitate the federal tax service, successfully tricking victims into downloading malware when trying to access fake documents (ENACT, 2023). Not only does this technique present a challenge for law enforcement, it also reveals how AI is refining and professionalising criminal methods.

Furthermore, the creation of malware has been facilitated by AI, leading to an increase in cyberattack sophistication. While popular AI models such as ChatGPT are designed to reject malicious requests, there are solutions such as WormGPT that are advertised without any restrictions, and of course without the company assuming any kind of responsibility for illicit uses, using AI to develop malicious software or adapt tools for criminal use. This represents a "democratisation" of cyberattacks where cybercriminals no longer need to meet high costs, have technical knowledge or time; it is cheap, easy, simple, fast and automated[14]. Banking malware in Brazil is an example of how criminals are using these tools to steal sensitive information in almost the same way as legitimate software would, making law enforcement even more difficult.

Faced with these challenges, authorities in Latin America are beginning to use AI in their operations, although progress has been uneven. In countries with greater resources, such as Brazil and Mexico, technologies such as Automatic Licence Plate Recognition (ALPR) and predictive analysis tools have been implemented that allow suspicious vehicles to be tracked and criminal activities to be anticipated. However, in many nations in the region, the lack of adequate infrastructure and the scarcity of resources limit the ability to effectively adopt these technologies.

Despite the technological advances available, the fight against organised crime using AI in Latin America and the Caribbean faces structural and ethical challenges. Legal frameworks regulating the use of these technologies are not fully developed in many countries, and international collaboration is essential to combat transnational criminal networks operating across borders. What's more, predictive policing and other AI tools raise privacy and human rights concerns, requiring a careful balance between public security and individual freedoms[15].

From the use of deepfakes and drones to fraud optimisation and malware creation, AI has enabled criminal organisations to evolve and increase their reach in unprecedented ways. However, it also offers powerful tools for law enforcement, which, if properly implemented, could level the battlefield and significantly improve authorities' ability to combat organised crime.

REGIONAL INITIATIVES

The European Union – Latin America and the Caribbean Digital Alliance[16] was created and launched in Colombia in March 2023 and consists of an informal cooperation framework based on shared values, open to all LAC countries and EU Member States who will be able to participate through their respective governments and agencies related to the digital agenda. The aim of the Alliance is to foster the development of secure, resilient and human-centred digital infrastructures based on a values-based framework, ensuring a democratic and transparent environment and emphasising privacy and digital rights, seeking in particular to promote cooperation in a wide range **of topics, including dialogue on digital policies and AI between the EU and LAC countries. As part of this Alliance, it was agreed to create two**

9 Europol, (2020). Malicious Uses and Abuses of Artificial Intelligence, Trend Micro Research, European Union Agency for Law Enforcement Cooperation 2020. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/malicious_uses_and_abuses_ of_artificial_intelligence_europol.pdf.

10 ENACT, (2023) AI and organised crime in Africa. Sigsworth, R., ENACT Observer (2023). Retrieved from https://enactafrica.org/enact-observer/ai-and-organised-crime-in-africa.

11 Caldwell, M., Andrews, J.T.A., Tanay, T. et al. (2020) AI-enabled future crime. Crime Sci 9, 14 (2020). Retrieved from https://doi.org/10.1186/s40163-020-00123-8

12 idem

13 AIplusInfo, (2023). How Will Artificial Intelligence Affect Policing and Law Enforcement? Artificial Intelligence + (2023). Retrieved from https://www.aiplusinfo.com/blog /artificial-intelligence-ai-and-policing

14 MARTIN, Nacho. El Independiente. (9 November 2024). WormGPT: The unrestricted ChatGPT used by cybercriminals. El Independiente. https://www.elindependiente.com/futuro/inteligencia-artificial/2024/11/09/wormgpt-el-chatgpt-sin-restricciones-que-usan-los-ciberdelincuentes/

15 Deloitte, (2021). Surveillance and Predictive Policing Through AI. Study Overview by Deloitte Insights (2021). Retrieved from https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive- policing-through-ai.html

16 European Commission, "Global Gateway: EU, Latin America and the Caribbean partners launch the EU-LAC Digital Alliance in Colombia", press release 14 March 2023, at: https://ec.europa.eu/commission/presscorner/detail/es/ip_23_1598

coordination platforms: the D4D (Digital for Development) Centre[17] for European partners and participants, and the United Nations Economic Commission for Latin America and the Caribbean (ECLAC), which will be the coordinating body for partners from LAC countries.

The Inter-American Development Bank (IDB) has an initiative known as "fAIr LAC+"[18] which is an initiative made up of private sector companies, academic groups, government agencies and specialised international organisations whose purpose is to promote the ethical and responsible use of AI in LAC countries. This initiative has created a set of guidelines, including an ethical self-assessment guide for the public sector, designed to enable the mitigation of ethical risks associated with the use and application of new technologies aimed at public sector institutions and organisations[19]. fAIr LAC+ has generated academic partnerships and projects such as GuIA[20] that address discussions related to AI systems' ethics, principles, standards and policies, and specific problems in LAC.

The Economic Commission for Latin America and the Caribbean (ECLAC), the National Centre for Artificial Intelligence of Chile (CENIA), with the support of the Inter-American Development Bank (IDB), the Development Bank of Latin America and the Caribbean (CAF) and the Organisation of American States (OAS), in 2023 created a Latin American Artificial Intelligence Index (ILIA)[21] to evaluate a set of elements related to infrastructure, human capital, data availability, regulations, strategic areas and citizen participation to offer indicators and metrics on the level of development in the adoption of AI in LAC and to identify the main challenges in the region. The index comprises three dimensions: (i) enabling factors, which includes infrastructure, data and talent development; (ii) research, adoption and development, which includes three sub-dimensions: Research, Innovation and Development and Adoption, and; (iii) governance, which includes three subdimensions: vision and institutionality, international and regulation[22].

The launch of the second version of ILIA was presented by ECLAC and CENIA on 24 September 2024. The index includes 19 countries and among the three countries that obtained the best score are Chile (73.07), followed by Brazil (69.30) and Uruguay (64.98). According to ECLAC, Chile, Brazil and Uruguay have not only made progress in the implementation of AI-based technologies, but are also directing their national strategies towards the consolidation and expansion of these technologies in all sectors of their economy and society. They also have a favourable environment that promotes research, development and adoption of technologies, promoting innovation and application of AI.

The Second Latin American and Caribbean Ministerial Summit on Artificial Intelligence was held in Cartagena, Colombia on 8 and 9 August 2024. High-level representatives from 16 countries, as well as representatives of the European Union, participated in this summit. During this summit, a Declaration for the Governance of Artificial Intelligence Ecosystems and the Promotion of AI Education in an Ethical and Responsible Manner in Latin America and the Caribbean was agreed upon[23].

17 See: https://d4dhub.eu/

18 See: https://fairlac.iadb.org/

19 The IDB's ethical self-assessment guide for the public sector can be found at: https://view.genially.com/62aa57549a8ebc001038afe0

20 See: https://proyectoguia.lat/

21 The Latin American Artificial Intelligence Index (ILIA) portal is located at: https://indicelatam.cl/

22 ECLAC/CENIA, "Latin American Artificial Intelligence Index (ILIA)", Library of the National Congress of Chile. Department of Studies, Extension and Publications, 7 August 2023 at: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/34598/1/Indice_Latinoamericano_de_Inteligencia_Artificial.pdf

23 The portal of the Second Latin American and Caribbean Ministerial Summit on Artificial Intelligence, including the declaration and the proceedings, can be found at: https://mintic.gov.co/cumbre-ia/secciones/Cumbre-Ministerial-de-IA/Memorias/

RELEVANT COURT DECISIONS

In the judicial field, a recent ruling by the Constitutional Court of Colombia stands out in a case brought by a mother who requested exemption from the collection of payments and fees for services and medications for the treatment of her son with autism disorder. A second instance judge in the country used ChatGPT to formulate legal questions about the fundamental right to health of minors diagnosed with autism spectrum disorder, including the questions and answers in the grounds of his judgement.

The Review Chamber of the Constitutional Court concluded that there was no replacement of the judicial function by ChatGPT, because the second instance judge used AI after having justified and made the decision. However, the Constitutional Court in its ruling warned about the implications of using GAI and the importance of evaluating the proper use of tools such as ChatGPT and recommended the application of ethical criteria and respect for higher mandates to guarantee citizens' fundamental rights. It urged the officials and employees of the Judicial Branch to apply the principles of (i) transparency, (ii) responsibility, (iii) privacy, (iv) non-substitution of human rationality, (v) seriousness and verification, (vi) risk prevention, (vii) equality and equity, (viii) human control, (ix) ethical regulation, (x) adaptation to good practices and collective standards, (xi) continuous monitoring and adaptation and (xii) suitability and ordered the Higher Council of the Judiciary to adopt a guide in relation to the implementation of GAI in the Judicial Branch, especially regarding the use of ChatGPT[24].

24 Judgement, T-323 of 2024. Constitutional Court of the Republic of Colombia. Second Review Chamber, at: https://www.corteconstitucional.gov.co/relatoria/2024/T-323-24.htm

1.2. TYPES OF AI

There are different types and classifications related to the concept of AI that have been developed by the scientific community. Relevant AI classifications for criminal justice authorities include:

- **Natural Language Processing (NLP).** This is a sub field of computer science and AI that uses machine learning to enable systems to understand and communicate through human language. NLP enables digital systems and devices to recognise, understand and generate text and speech by combining computational linguistics based on statistical models, machine learning and deep learning.

- **Machine Learning (ML).** Machine learning is based on mathematical models trained with data that learn based on experiences. Through machine learning, algorithms can make predictions or decisions without the need to be programmed. There are three subcategories of ML algorithms that are essential for research: (i) supervised learning, (ii) unsupervised learning, and (iii) reinforcement learning.

- **Deep Learning.** Deep learning is a subset of machine learning methods based on neural networks with representation learning. Deep learning enables many applications and services to improve automation and perform analytical tasks without human intervention.

- **Facial Recognition.** Facial recognition is a category of biometric technology that analyses a person's facial features to analyse and confirm their identity. Facial recognition is commonly used in security systems to identify suspects and victims of crime. This technology compares digital images or video frames with previously stored facial prints, allowing for the rapid identification of people in public spaces and even in places with large crowds.

- **Generative AI.** Generative artificial intelligence refers to the use of AI to create content, such as text, images, music, audio and videos. Generative AI is based on foundational models, i.e. large AI models, that can multi task and perform pre-configured tasks such as summarising, questioning and answering, classification, etc. Furthermore, by requiring minimal training, basic models can be adapted to specific use cases with very limited sample data.

1.3. CHALLENGES

AI offers great opportunities to improve and optimise administration of the justice system but at the same time it also presents great technical, legal and international cooperation challenges that countries will have to solve through the creation of national strategies on AI, public policies designed for the public and private sectors, updating of national legal frameworks to penalise conduct committed through AI systems, training and capacity building of justice system operators in the management of technologies and especially the creation of public-private partnerships so that the use of these technologies can be better understood, have a greater impact and resolve problems that arise in the use and implementation of these technologies - such as biases, discrimination against certain groups in society, misinformation - jointly between national regulatory authorities, justice system authorities and developers and providers of AI technologies with the support and expertise of international and regional organisations and academic and civil society groups specialised in the matter.

1.4. GENDER CHALLENGES

Analysing AI issues from a gender perspective is also crucial, as technologies can reproduce, amplify or even create new forms of gender-based discrimination and violence.

AI relies on large volumes of data to train its predictive models, and if these data contain gender biases or reflect pre-existing inequalities, AI systems perpetuate these patterns, disproportionately affecting women and traditional-gender non-conforming people. The use of artificial intelligence systems in employment, worker management and access to self-employment, in particular for the recruitment and selection of individuals, for decision-making affecting the terms of the employment relationship, promotion and termination of work-related contractual relationships that cause serious discrimination in public or private employment, as well as essential private services and essential public services and benefits may lead to discrimination and bias against individuals on the basis of their ideology, religion or beliefs, family situation, ethnicity, race or nation, national origin, sex, age, sexual or gender orientation or identity, gender reasons, aporophobia or social exclusion, illness or disability.

In the context of organised crime, this can lead to under-representation of the differential impacts suffered by women, such as human trafficking, gender-based violence and sexual exploitation.

Related to this, a UN study suggests that AI algorithms applied in areas such as security and justice tend to be trained with data that fail to adequately represent women and vulnerable groups. For example, in facial recognition systems, algorithms have been shown to have higher error rates for women and especially for black women, which can affect the correct identification of victims and perpetrators in the context of organised crime. Specifically, a report by AI Now Institute introduced the idea that facial recognition systems developed in the USA have a significantly higher error rate for African-American women compared to Caucasian men, which could translate into problems of misidentification or failure to identify victims and offenders in networks of sexual exploitation or human trafficking[25]. This is the case of Amazon's facial analysis service Rekognition, which has already demonstrated worse gender and racial biases than comparable tools, biases that took the form of literally 'not seeing' dark-skinned women, while being more competent at detecting light-skinned men.

25 West, S.M., Whittaker, M. and Crawford, K. (2019). Discriminating Systems: Gender, Race and Power in AI. AI Now Institute. Available at https://ainowinstitute.org/ discriminatingsystems.html.

And not just in facial recognition, according to an audit conducted by independent researchers at the University of Southern California (USC, in the USA). In 2021, a study by the U.S. Food and Drug Administration (FDA) revealed that Facebook's ad serving system shows different job openings to women and men even though the jobs in question require the same qualifications, thereby hiding certain jobs from women despite their having the same training. Researchers were unable to figure out why the system somehow detects the current demographic distribution of these jobs, because Facebook does not want to explain how its ad serving system works.[26]

International bodies such as the Council of Europe and the UN[27] have warned about the risks and systemic biases posed by AI systems that have the potential to harm and disadvantage vulnerable groups in society, including women and girls. The UNESCO Report entitled: *Systematic Prejudices. An investigation of Prejudices against women and girls in major language models*[28] contains some examples of major AI-based systems that often perpetuate and even extend and amplify structural and social human biases targeting women and girls and proposes a list of recommendations and actions for both policy makers and AI developers to mitigate the risks of systematic biases posed by some of the major language models currently in use.

Organised crime affects women differently from men, especially in areas such as human trafficking, drug trafficking, and labour and sexual exploitation. The lack of gender perspective in the design and application of AI systems can result in these realities not being adequately prioritised or made visible in crime investigation and prevention processes. In other words, if detection and prevention tools focus on male-dominated crimes, such as arms or drug trafficking, crimes that predominantly affect women and girls could be overlooked.

On the other hand, women, particularly young women and those from marginalised communities, face increasing forms of digital violence. The use of AI by organised crime to spread non-consensual sexual content or extort victims has been documented in several countries. If monitoring systems are not designed to identify this digital violence from a gender perspective, they may not be effective in detecting it. According to studies by Amnesty International, women are the main target of cyberbullying and digital violence. Criminal networks have stepped up their use of deepfakes and other digital content manipulation methods to extort and exploit women[29].

In 2019, in Bogotá, a project was publicised by the National University of Colombia, the District Secretariat of Security, Coexistence and Justice and the applied mathematics company Quantil, which would be financed to the tune of 3 billion pesos from the Science, Technology and Innovation Fund of the General Royalties System and which aimed, in thirty months, to build models to describe four problems related to crime, security and coexistence in Bogotá (López, 2019): murders, property crimes with the use of violence, personal injuries and the dynamics behind citizens' perception of security, in such a way that the four traditional "w" questions (when, where, who and why) could be predicted and anticipated. Of course, Professor Francisco Gómez, from the Department of Mathematics at the National University of Colombia, recognised that one of the main challenges of the project was to identify and correct biases[30].

Another worrying aspect may be women's scarce and limited participation in the development of AI and technology policies. According to UNESCO reports[31], a minority of AI professionals worldwide are women, which limits the diversity of perspectives in the creation of technologies aimed at combating organised crime. Lack of equitable participation not only reinforces existing biases, but also undermines the ability to create inclusive solutions that protect all sectors of society.

Finally, the use of AI in crime surveillance and prevention can lead to the unfair criminalisation of women in vulnerable situations, such as sex workers or migrants. Without careful consideration of context, algorithms may classify these women as potential criminals, reinforcing negative stereotypes and increasing their marginalisation.

1.5. HUMAN RIGHTS CHALLENGES

The algorithms and data used in the training and operation of AI systems can generate false information that can put people's fundamental rights at risk. This is the case of police prediction systems in which, if the data used are not updated, verified and audited regularly, they can present information biases that jeopardise individuals' right to privacy, put them at risk of being discriminated against and even violate their right to enjoy a fair and impartial trial[32].

The European Union's system for the protection of fundamental rights is one of the most complete and complex, as different institutions and judicial bodies are involved in ensuring that these rights are duly protected in accordance with the Treaty on the Functioning of the European Union, the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights.

It should be highlighted that international organisations have prepared documents and recommendations on the protection of human rights in relation to the use and implementation of algorithms in the context of data processing in the judicial system, and especially the Council of Europe's Study on the human rights dimensions of automated data processing techniques and their possible regulatory implications[33], which examines the effects of the use of algorithms and the way in which human rights are exercised and guaranteed in accordance with international human rights law, including the principles of the rule of law within judicial proceedings.

The Recommendation of the Committee of Ministers of the Council of Europe on the impact of algorithmic systems on human rights of April 2020 states that there are significant human rights challenges associated with the increasing reliance on algorithmic systems in everyday life, including with regard to the right to a fair trial; the right to data privacy and protection; the right to freedom of thought, conscience and religion; the right to freedom of expression; the right to freedom of assembly; the right to equal treatment, and economic and social rights[34].

26 HAO, Karen trad. MILUTINOVIC Ana (14 April 2021). Facebook's AI discriminates against women in job ads. Technology Review. https://www.technologyreview.es/s/13219/la-ia-de-facebook-discrimina-las-mujeres-en-los-anuncios-de-trabajo

27 United Nations, "Artificial intelligence reproduces gender stereotypes", 7 March 2024 at: https://news.un.org/es/story/2024/03/1528182

28 UNESCO, " Challenging systematic prejudices: an investigation into bias against women and girls in large language models ", 2024 at: https://unesdoc.unesco.org/ark:/48223/pf0000388971

29 In *Toxic Twitter: Violence and Abuse Against Women On-line* (2018), available at https://www.amnestyusa.org/wp-content/uploads/2018/03/Toxic-Twitter.pdf

30 LÓPEZ B., Joaquín M. The artificial intelligence system to anticipate crimes in Bogotá. In: La República. 15 April 2019 Available at: https://www.larepublica.co/internet-economy/asi-seria-elsistema-de-inteligencia-artificial-para-adelantarse-a-crimenes-en-bogota-2854179

31 For example, "I'd Blush if I Could" available at https://unesdoc.unesco.org/ark:/48223/pf0000367416 or " Artificial intelligence and gender equality: key findings of UNESCO's Global Dialogue" available at https://unesdoc.unesco.org/ark:/48223/pf0000374174

32 Council of Europe,"Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. A*dopted by the Committee of Ministers on 8 April 2020*", see Recommendation Appendix Paragraph A number 4 at: https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900016809e1154%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

33 Council of Europe, "Algorithms and human rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, 2018" en: https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

34 European Union Agency for Fundamental Rights (FRA),"Bias in Algorithms. Artificial Intelligence and Discrimination" 8 December 2022, available at:https://fra.europa.eu/en/publication/2022/bias-algorithm

The Committee of Ministers entrusted the European Committee on Crime Problems (CDPC) with the responsibility of overseeing and coordinating the activities of the Council of Europe in the field of crime prevention and control, taking into account its "Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law (2020)"[35]. Following these projects, at the 77th plenary session of the CDPC held in Strasbourg from 3 to 6 December 2019, the Working Group was tasked with "*conducting a feasibility study identifying the scope and main elements of a future Council of Europe instrument on AI and criminal law, preferably a convention*" [36]. Specifically, it has been tasked with drafting a legal instrument on criminal liability related to the use of AI, which is expected to be drafted by the end of 2025. The first CDPC Discussion Paper on criminal liability related to AI systems will be presented at the 86th Plenary Meeting of the Council of Europe, Palais de l'Europe, Strasbourg, from 20 to 22 November 2024[37].

Taking into account also the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS no. 225) and other important documents prepared by the Committee on Artificial Intelligence such as "Possible elements of a legal framework on artificial intelligence, based on Council of Europe standards on human rights, democracy and the rule of law (2021); Towards the regulation of AI systems (2020); Feasibility study on a legal framework on the design, development and application of AI based on Council of Europe standards (2020). Taking into account the Convention on Cybercrime (Budapest Convention, ETS no. 185) [38].

The work of the Committee of Ministers of the Council of Europe with the Member States and, in particular, in the recommendations should not be forgotten: Legal aspects of "autonomous" vehicles: Resolution 2346 (2020) and Recommendation 2187 (2020[39]); Justice through algorithms: the role of artificial intelligence in policing and criminal justice systems: Resolution 2342 (2020) and Recommendation 2182 (2020)[40]

At the European level, the study requested by the LIBE Committee of the European Parliament on Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights stands out, the aim of which is to assess recent developments in relation to AI in the field of law enforcement and criminal justice, with a view to reviewing its impact on EU fundamental rights and submitting policy recommendations to the European Parliament. The study contains a detailed analysis of the main related European laws impacting the protection of human rights, case analyses and the work of the institutions responsible for their enforcement, including a section on AI and criminal justice[41].

The 'black box' effect through which trained algorithms can generate responses, results and outputs raises certain doubts and questions about their ability to make decisions or predictions that lack a clear and logical explanation regarding their basis. According to Europol, in the field of law enforcement, the opacity of the 'black box' poses a major challenge. "When an AI-powered system raises concerns about a person's potential threat or recommends that police officers deploy patrols in specific areas, it is imperative that law enforcement officers and those affected by such decisions understand the underlying logic." Europol notes that

35 Council of Europe European Committee on Crime Problems (CPDC), 'Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law', 2020. Available at: https://rm.coe.int/cdpc-2020-3-feasibility-study-of-a-future-instrument-on-ai-and-crimina/16809f9b60

36 CDPC – List of decisions – 77th plenary session, CDPC (2019) 23, point 7, p. 4.

37 CDPC meeting: 86th Plenary Session 20-22 November 2024 at: https://rm.coe.int/cdpc-2024-oj2-en-draft-agenda-november-2024-2788-1036-6986-v-1/1680b22c02

38 Council of Europe, 'Convention on Cybercrime', ETS No.185, 2001. ; Council of Europe, 'Chart of signatures and ratifications of the Convention on Cybercrime'.

39 Text adopted by the Standing Committee, acting on behalf of the Assembly, on 22 October 2020 (see Doc. 15143 report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Ziya Altunyaldiz) at: http://www.europeanrights.eu/public/atti/Resolution_2346_(2020)_ENG.pdf See also Recommendation 2187 (2020): http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileId=28817

40 Text adopted by the Standing Committee, acting on behalf of the Assembly, on 22 October 2020 (see Doc. 15156, report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Boriss Cilevičs) at: https://pace.coe.int/en/files/28805/html . See also Recommendation 2182 (2020): https://pace.coe.int/en/files/28806

41 European Parliament, "Protecting Fundamental Rights within the Union" at:https://www.europarl.europa.eu/about-parliament/en/democracy-and-human-rights/fundamental-rights-in-the-eu

the absence of this critical information opens the door to the possibility of bias, error or misinterpretation, raising fundamental questions of accountability and fairness.[42]

To address the challenges posed by the 'black box' effect in AI systems, ethical principles such as transparency, reliability, explanation, impartiality and other concepts such as human-in-the-loop are beginning to gain relevance at the international level precisely to prevent AI systems from transgressing and violating the fundamental rights of individuals.

AI systems should not replace human judgment and decisions, but should be used as a tool that can guide and assist decision-making by authorities and law enforcement in criminal investigations, including those related to cross-border organised crime.

42 EUROPOL, "AI and Policing. The Benefits and Challenges of Artificial Intelligence for Law Enforcement. An Observatory Report from the Europol Innovation Lab", 2024, p.35 at: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing

BLOCK 2: INTERNATIONAL REGULATIONS, STRATEGIES AND OTHER NON-BINDING INITIATIVES

2.1. LEGISLATION AND STRATEGIES

COUNCIL OF EUROPE FRAMEWORK CONVENTION ON ARTIFICIAL INTELLIGENCE

The Council of Europe's Committee on Artificial Intelligence (CAI) and its predecessor group CAHAI, a group of experts comprising representatives from industry, government, academia and civil society, have been mandated to create a legal instrument on AI since 2019.

In 2022, the CAI began drafting the text of the convention together with the 46 Member States of the Council of Europe. The negotiation and consultation process lasted more than 2 years. The *Framework Convention on Artificial Intelligence*[43] was opened for signature by Council of Europe States Parties on 5 September 2024 in Vilnius, Lithuania and is the first binding international treaty aimed at ensuring that the use of AI systems is fully compatible with human rights, democracy and the rule of law[44].

The scope of the framework convention is quite broad and includes all activities within the life cycle of AI systems carried out by both public authorities and private players acting on their behalf and that have the potential to interfere with human rights, democracy and the rule of law. Activities related to the protection of national security are excluded. Among some of the provisions contained in the framework convention:

- It calls on countries to adopt measures and implement a list of general principles related to the life cycle of AI systems, such as human dignity, autonomy, transparency and oversight, accountability, fairness and non-discrimination, privacy and data protection, trustworthiness and safe innovation.
- A section recommending that countries adopt and maintain measures to ensure the availability of accessible and effective judicial remedies to citizens for potential human rights violations resulting from activities within the life cycle of AI systems.
- Establishment of safeguard measures to protect the rights of affected persons.
- A chapter urging countries to adopt or maintain measures for the identification, assessment, prevention and mitigation of risks posed by AI systems, considering actual and potential impacts on human rights, democracy and the rule of law, as well as other provisions related to the rights of persons with disabilities, children, the promotion of digital literacy and digital skills and the safeguarding of human rights, as well as
- provisions relating to the Conference of the States Parties (which will be the monitoring body), international cooperation and implementation of control and monitoring mechanisms.

As of the date of this study, this instrument has been signed by 10 countries (Andorra, Georgia, Iceland, Norway, the Republic of Moldova, San Marino, the United Kingdom, Israel, the United

43 Council of Europe Framework Convention on Artificial Intelligence, Human Rights and the Rule of Law, CETS No. 225, Vilnius 5.IX.2024 at: https://rm.coe.int/1680a-fae3c

44 Council of Europe, "The Framework Convention on Artificial Intelligence" at: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

States and the EU[45]). It requires ratification by 5 countries - including 3 members of the Council of Europe - to officially enter into force. Countries such as Argentina, Costa Rica, Mexico, Peru and Uruguay have taken part in negotiating the convention.

The implementation of this convention will require that countries that sign and ratify it have to create, adopt and implement national legal frameworks consistent with the provisions of that instrument, including the development of national strategies and policies related to AI systems that include the dimension of the protection of fundamental rights of people.

EUROPEAN REGULATION ON ARTIFICIAL INTELLIGENCE

The European Union, through institutions such as the European Commission, the European Parliament (through its various committees AIDA, IMCO and LIBE) and the European Council, have played a decisive and key role in generating and promoting a legal framework on AI with the aim of protecting people's rights against the risks generated by the use of AI systems during their life cycle based on the categorisation of the level of risk they present to society and establishing prohibitions on certain practices that violate the democratic principles of the EU and citizens' freedoms[46].

The final text of the European Regulation on AI (REIA) was published in the Official Journal of the European Union on 12 July 2024[47]. The REIA officially entered into force on 1 August 2024 and will be implemented gradually, over a period of two years, with some exceptions: general provisions and prohibitions will apply after six months; governance rules and obligations for general-use AI models will apply after twelve months; and rules for AI systems embedded in regulated products will come into force after three years[48].

The REIA will regulate provisions in other European secondary laws in accordance with their entry into force. The REIA text contains 180 recitals and a total of 113 articles distributed across thirteen chapters that establish a set of general rules to address the risks created specifically by AI systems and applications, which:

- Prohibits AI practices that pose unacceptable risks to the individual;
- Establishes requirements for AI systems intended for applications considered high risk;
- Contains specific obligations for suppliers, distributors and importers of AI applications;
- Requires a conformity assessment to be carried out before a given AI system is put into service or placed on the market in the EU;
- Establishes compliance measures after a given AI system is placed on the market;
- Establishes a governance structure at European and national level in which various institutions and regulatory authorities will participate to ensure compliance, as well as fines and sanctions in the event of non-compliance by AI application providers[49].

45 See table of signatures and ratifications at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225

46 For a summary of the various EU institutions that have participated in the creation, negotiation and implementation of the European Regulation on AI, see: Centre for AI and Digital Policy (CAIDP), *Artificial Intelligence and Democratic Values Index 2023*, pp. 56-77, available at: https://www.caidp.org/reports/aidv-2023/

47 See: Regulation (EU) 2024/1689 of 13 June 2023 establishing harmonised rules on artificial intelligence and amending Regulations (EC) no. 300/2008, (EU) no. 167/2013, (EU) no. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

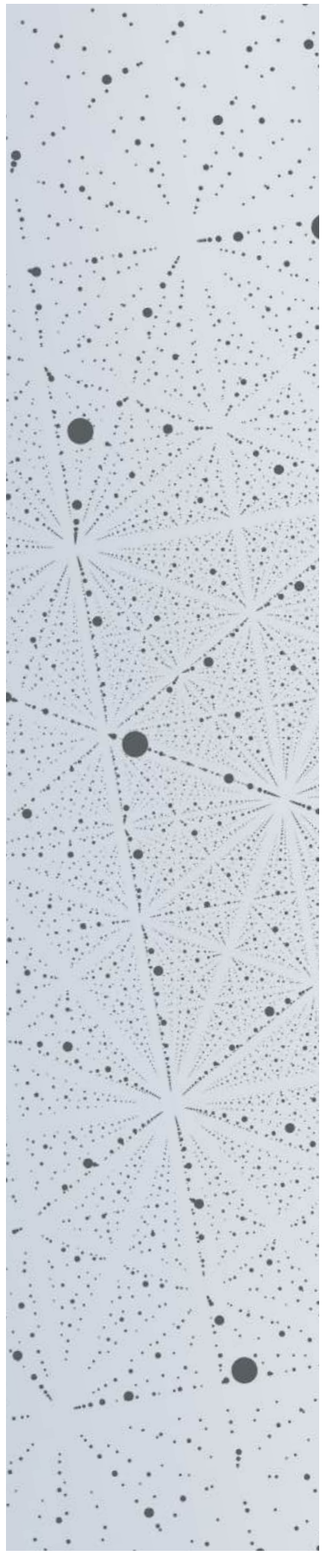
48 For a time line and key dates relevant to the implementation of the REIA, see: https://artificialintelligenceact.eu/ai-act-implementation-next-steps/

49 European Commission AI Act https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

The REIA establishes some exceptions. Paragraph 4 of Article 2 provides that the Regulation shall not apply to public authorities of third countries or international organisations when they use AI systems within the framework of international agreements for the purposes of law enforcement and judicial cooperation with the EU or with one or more EU Member States, provided that such third country or international organisation offers sufficient guarantees with regard to the protection of individuals' fundamental rights and freedoms.

Some of the provisions relevant to law enforcement and investigative authorities of the justice system established by the REIA include:

- Annex III, which includes eight areas of categorisation of High Risk systems referred to in Art. 6 Section 2. Section 6 of Annex III includes: "Ensuring compliance with the law, to the extent that its use is permitted by applicable Union or national law" and provides for five additional cases:
  - AI systems intended for use by law enforcement authorities, or on their behalf, or by Union institutions, bodies, offices and agencies in support of law enforcement authorities, or on their behalf, to assess the risk that a natural person might become a victim of a criminal offence.
  - AI systems intended to be used bylaw enforcement authorities, or on their behalf, or by Union institutions, bodies, offices and agencies in support of law enforcement authorities, such as polygraphs or similar tools;
  - AI systems intended to be used by law enforcement authorities, or on their behalf, or by Union institutions, bodies, offices and agencies in support of law enforcement authorities to assess the reliability of evidence during the investigation or prosecution of criminal offences;
  - AI systems intended to be used by law enforcement authorities, or on their behalf, or by Union institutions, bodies, offices and agencies in support of law enforcement authorities to assess the risk that a natural person will commit a criminal offence or reoffend, taking into account not only the profiling of natural persons referred to in point (4) of Article 3 of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;



- AI systems intended to be used by law enforcement authorities, or on their behalf, or by Union institutions, bodies, offices and agencies in support of law enforcement authorities for profiling natural persons, as referred to in point (4) of Article 3 of Directive (EU) 2016/680, during the detection, investigation or prosecution of criminal offences

→ Paragraph 7 of Annex III "Migration, asylum and border control management, insofar as their use is permitted by applicable Union or national law".

→ Section 8 of Annex III "Administration of justice and democratic processes" includes section a): "AI systems intended to be used by or on behalf of a judicial authority to assist a judicial authority in the investigation and interpretation of facts and the law, as well as in ensuring compliance with the law on a particular set of facts, or to be used in a similar manner in alternative dispute resolution"

Art. 5, section 1 h) of the REIA establishes that the use of remote "real-time" biometric identification systems in public spaces for law enforcement purposes is prohibited, unless their use is strictly necessary to achieve one of the following objectives:

→ "the selective search for specific victims of kidnapping, human trafficking or sexual exploitation of human beings, as well as the search for missing persons;

→ the prevention of a specific, significant and imminent threat to the life or physical safety of natural persons or of a genuine and present or actual and foreseeable threat of a terrorist attack;

→ the location or identification of a person suspected of having committed an offence for the purposes of a criminal investigation or prosecution or of executing a criminal penalty for any of the offences listed in Annex II which are punishable in the Member State concerned by a custodial sentence or detention order of a maximum duration of at least four years."

The uses provided for in the REIA are subject to the authorisation of a judicial body or other independent administrative body and to compliance with necessary and proportionate safeguards and conditions in relation to the use, in particular with regard to time, geographical and personal limitations in accordance with numerals 2, 3, and 4 of Art. 5 of the REIA.

REGIONAL AND NATIONAL STRATEGIES

The European Commission initially presented a communication on 25 April 2018 containing the **EU Strategy on Artificial Intelligence** which includes various objectives: (i) positioning of the EU in a competitive international landscape; (ii) boosting of the EU's technological and industrial capacity and the adoption of AI across the economy; (iii) bringing AI closer to small businesses and potential users; (iv) ensuring the establishment of an appropriate ethical and legal framework, based on EU values and in line with the EU Charter of Fundamental Rights[50].

According to information from the European Commission[51] and the European Association of Communication Agencies[52], by 2022, twenty EU Member States and Norway had a national strategy on AI. However, very few EU countries have a specific AI strategy for law enforcement and justice authorities.

50 European Commission, 'Communication from the Commission. Artificial Intelligence for Europe " COM(2018) 237 final, 25.4.2018. available at: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0237

51 European Commission JRC Technical Report. AI Watch National Strategies on Artificial Intelligence: A European Perspective. 2022 Edition, available at: https://op.europa.eu/en/publication-detail/-/publication/54e385d8-eac0-11ec-a534-01aa75ed71a1

52 See https://eaca.eu/news/national-ai-strategies-in-europe/

For their part, some LAC countries have begun to develop national strategies on AI in order to establish a framework of policies and guidelines that can be useful for the public and private sectors in the development and use of AI systems. The OECD Recommendation on Artificial Intelligence and the UNESCO Recommendation on the Ethics of Artificial Intelligence are gaining momentum in some countries in the region to develop broader national AI strategies that include the ethical principles and recommendations of these bodies.

The OECD reports that seven LAC countries have already developed or are in the process of developing a national AI strategy, including Argentina, Brazil, Chile, Colombia, Mexico, Peru and Uruguay. This body indicates that most LAC countries, even if they lack an AI strategy, have already published a broader national digital government strategy, or a linked digital agenda or programme that includes components that act as foundational bases for AI (for example, interoperability, infrastructure, analytical tools and processes, integration of services, etc.), although this is not usually incorporated as a main objective53. The organisation reports that countries such as Ecuador, Costa Rica, the Dominican Republic and Panama are already exploring national strategies on AI, although to date they have not been officially adopted and published by their respective governments. The Costa Rican government, through the Ministry of Science, Innovation, Technology and Telecommunications (MICITT), published its National Artificial Intelligence Strategy 2024-2027 in the third week of October 2024[54].

While national AI strategies in the region address very broad issues in different areas related to the adoption of AI technologies in areas of the public sector such as financing, education, health, innovation and development and aspects of governance, none of them make particular reference to how they should be addressed by the criminal justice sector, including the judiciary.

53 OECD/CAF Development Bank of Latin America (2022), "Artificial Intelligence strategies in Latin America and the Caribbean", in The Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean, OECD Publishing, Paris, pp.24-25. DOI: https://doi.org/10.1787/03c4e7eb-es. For an analysis of the National AI Strategies in Argentina, Chile, Colombia, Mexico and Uruguay, see: CeTyS "Artificial Intelligence in Latin America and the Caribbean. Ethics, Governance and Policies", ISN 2684-0278, pp. 134-147, at: https://proyectoguia.lat/wp-content/uploads/2020/10/compilado-espanol-compressed.pdf

54 The National Artificial Intelligence Strategy 2024-2027 of Costa Rica at: https://observatorioecuadordigital.mintel.gob.ec/wp-content/uploads/2024/10/Estrategia-Nacional-de-IA-Costa-Rica-.pdf

2.2. RELEVANT NON-BINDING INTERNATIONAL PRINCIPLES AND INITIATIVES

ETHICAL GUIDELINES FOR TRUSTWORTHY AI FROM THE HIGH LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (HLEG)

In 2018, the European Commission established an independent high-level expert group whose mandate was to facilitate and advise the European Commission in the development of the European strategy on AI. Among the deliverables of this group is a document on *Ethics Guidelines for Trustworthy AI* published in April 2019. The document sets out a definition of trustworthy AI and develops seven key principles along with a concrete check-list intended to help verify the application of each of these principles. The principles contained in the guide include: (i) human agency and oversight; (ii) technical robustness and security; (iii) privacy and data governance; (iv) transparency; (v) diversity, non-discrimination and equity; (vi) social and environmental well-being, and; (vii) accountability.

This document was one of the first international guidelines to develop a definition of AI systems and general ethical principles for the development and use of AI technologies.

OECD RECOMMENDATION ON ARTIFICIAL INTELLIGENCE

The OECD Council adopted a Recommendation on Artificial Intelligence on 22 May 2019[55]. This is the first intergovernmental regulation that aims to foster innovation and trust in AI systems and promote the responsible management of reliable AI, ensuring respect for human rights and democratic values among the member countries of the organisation.

The Recommendation contains a section on responsible management of trustworthy AI that sets out five complementary principles relevant to all stakeholders: (i) inclusive growth, sustainable development and well-being; (ii) respect for the rule of law, human rights and democratic values, including equity and privacy; (iii) transparency and explainability; (iv) robustness, safety and security, and; (v) accountability. This section further calls on the different AI actors to promote and implement these principles within their respective activities and functions.

The second section offers five recommendations addressed to Member and non-Member countries that have adhered to the Recommendation for them to implement the following within their national policies: (i) investing in AI research and development; (ii) fostering an inclusive ecosystem that enables AI; (iii) implementing an interoperable AI-enabling governance and policy environment; (iv) developing human capacity and preparing for labour market transformation, and; (v) fostering international cooperation for trustworthy AI.

The OECD has an AI policy observatory whose purpose is to disseminate the work of the organisation, monitor the work of the adhering countries in the implementation of the principles established in the recommendation and promote cooperation with the different international and regional organisations that are working on AI policies[56].

The Artificial Intelligence Recommendation was amended in 2024 to update the definition of "AI system" and clarify the scope of some of the principles, including addressing safety issues, so that if AI systems are at risk of causing harm or showing undesirable behaviour, they can be safely overridden, repaired, and/or revoked through human interaction, among other things.[57]

It highlights the OECD's work in developing a classification of AI systems[58]; a catalogue of tools and metrics on trustworthy AI[59]; and a tool for monitoring AI incidents[60] whose purpose is to help AI practitioners, policy makers and various stakeholders to obtain relevant information on the risks and harms that AI systems can generate.

UNESCO RECOMMENDATION ON ETHICS AND ARTIFICIAL INTELLIGENCE

UNESCO adopted a *Recommendation on the Ethics of Artificial Intelligence* on 23 November 2021, the main objective of which is to establish a universal framework of values, principles and actions to guide countries in formulating laws, policies or other instruments related to AI, in accordance with international law[61].

55 OECD Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. Adopted on 22.05.2019 and amended on 03.05.2024 at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

56 OECD Policy AI Observatory at: https://oecd.ai/en/ai-principles

57 For some relevant aspects of the review of the OECD Recommendation on AI, see: OECD, "Report of the Implementation of the OECD Recommendation on Artificial Intelligence" C/MIN(2024)17, 24 April 2024 at: https://one.oecd.org/document/C/MIN(2024)17/en/pdf

58 OECD (2022), "OECD Framework for the Classification of AI systems", *OECD Digital Economy Papers*, No. 323, OECD Publishing, Paris, at: https://doi.org/10.1787/cb6d9eca-en

59 OECD.AI Policy Observatory, Catalogue of Tools & Metrics for Trustworthy AI at: https://oecd.ai/en/catalogue/overview

60 OECD.AI Policy Observatory, OECD AI Incidents Monitor (AIM) at: https://oecd.ai/en/incidents

61 UNESCO, "Recommendation on the ethics of artificial intelligence" Adopted on 23 November 2021, SHS/BIO/PI/2021/1, 2022 at: https://unesdoc.unesco.org/ark:/48223/pf0000381137

This recommendation contains four main objectives and also a section on 'Values' which includes four areas among which the following stand out: "respect for, protection and promotion of human rights and fundamental freedoms and human dignity"; as well as a section with ten 'Principles': (i) Proportionality and safety; (ii) Security and protection; (iii) Equity and non-discrimination; (iv) Sustainability; (v) Right to privacy and data protection; (vi) Human oversight and decision-making; (vii) Transparency and explainability; (viii) Responsibility and accountability; (ix) Awareness and education, and; (x) adaptive and multi-stakeholder governance and collaboration.

The Recommendation also includes eleven areas of policy action in different fields and a monitoring and evaluation mechanism based mainly on three methodologies related to the assessment of the ethical impact of AI technologies, the state of readiness to assist Member States and the ex ante and ex post evaluation regarding the effectiveness and efficiency of policies and incentives related to AI ethics.

UNESCO, in collaboration with an international organisation, a research centre, a foundation and the government of Japan, created an Observatory on Global AI Governance and Ethics[62] whose purpose is to show information on the current state of preparation of its member countries in the ethical and responsible adoption of AI in accordance with its recommendation. The observatory also has an AI Ethics and Governance Laboratory, which brings together contributions, research, toolkits and good practices in the implementation of the three documents that said organisation has generated: (i) the Recommendation on AI Ethics[63], (ii) the methodology for assessing country readiness (RAM)[64], and; (iii) the Ethical Impact Assessment[65].

The following UNESCO reports and initiatives are highlighted:

A global toolkit on AI and the rule of law for the judiciary, which aims to provide judicial operators with the necessary knowledge and tools to understand the benefits and risks of using AI in their activities and to provide guidance on the instances, principles and regulations of international human rights law and emerging case law that underpin the responsible use of AI[66].

Two reports on AI according to its Country Readiness Assessment (RAM) methodology from two LAC countries: Mexico[67] and Chile[68].

62 UNESCO, Global AI Ethics and Governance Observatory at: https://www.unesco.org/ethics-ai/en?hub=32618

63 See: https://unesdoc.unesco.org/ark:/48223/pf0000381137

64 See: https://unesdoc.unesco.org/ark:/48223/pf0000385198_spa

65 See: https://unesdoc.unesco.org/ark:/48223/pf0000386276

66 UNESCO, "Global Toolkit on AI and the Rule of Law for the Judiciary" 2023, at: https://unesdoc.unesco.org/ark:/48223/pf0000387331_eng

67 See: https://unesdoc.unesco.org/ark:/48223/pf0000390568?posInSet=2&queryId=d8165a01-53a2-4058-b878-84794bf39668

68 See: https://unesdoc.unesco.org/ark:/48223/pf0000387216_spa

The company recently announced a strategic alliance with the Superior Council of the Judiciary of Colombia to promote the ethical use of AI in the country's judicial system. The alliance aims to develop guidelines and capabilities on the responsible use of AI in judicial offices mainly in four key areas, including capacity development through training and capacity building workshops[69].

OTHER RELEVANT INITIATIVES

The United Nations General Assembly adopted General Resolution 78/L.49 on 11 March 2024[70] containing some guidelines and directives related to AI governance. Among the recommendations contained in this instrument, number 5 stands out:

> *"It stresses that human rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle of artificial intelligence systems; it calls upon all Member States and, where appropriate, other stakeholders to refrain from or cease using artificial intelligence systems that are impossible to operate in accordance with international law or that pose undue risks to the enjoyment of human rights, in particular for those in vulnerable situations, and it reaffirms that individuals' rights must also be protected on-line, including throughout the life cycle of artificial intelligence systems."*

The United Nations Interregional Crime and Justice Research Institute (UNICRI) Centre for Artificial Intelligence and Robotics and Interpol, together with a multi-sectoral group of experts and with the financial support of the European Union, developed a document known as the '*Artificial Intelligence Toolkit. Responsible AI Innovation for Law Enforcement*[71].'

This AI Toolkit aims to help law enforcement improve their understanding and development in the use of AI systems in a manner aligned and consistent with legislation and regulations on human rights protection, ethical and policing principles, and innovation in the use of this type of tools. It contains information and practical examples to assist law enforcement agencies in complying with ethical principles and foundations in the process of innovation and use of AI tools in the scope of their activities and even contains a guide for the development of an AI strategy aimed at police units with an explanation of the steps and activities that must be carried out and implemented.

Future UNICRI activities include using an interactive portal-based version of the toolkit, providing further training to agencies on responsible AI innovation, providing targeted mentoring to senior positions in key police units, and expanding understanding of the limitations and factors influencing the use of AI by law enforcement and security forces[72].

69 UNESCO, "UNESCO and Colombia: Leaders in the ethical and responsible use of AI in the Judiciary" 10 October 2024 at: https://www.unesco.org/es/articles/unesco-y-colombia-lideres-en-el-uso-etico-y-responsable-de-la-ia-en-el-poder-judicial

70 UN General Resolution 78/L.49, Seizing the opportunities of safe, secure and reliable systems of artificial intelligence for sustainable development, 11 March 2024, in: https://digitallibrary.un.org/record/4040897?v=pdf

71 UNICRI, INTERPOL "Responsible AI Innovation in Law Enforcement. AI Toolkit " Revised February 2024 at: https://unicri.it/sites/default/files/2024-02/03_Organisational_Roadmap_Feb24.pdf

72 UNICRI, "The Toolkit for Responsible Artificial Intelligence Innovation in Law Enforcement" at: https://unicri.it/topics/Toolkit-Responsible-AI-for-Law-Enforcement-INTERPOL-UNICRI

BLOCK 3: MAIN CRIMES COMMITTED USING AI TOOLS

As has happened on other occasions with new technologies that have emerged, AI will be exploited by criminals for their illicit activities to the greatest extent possible. In the specific case of organised crime, its vast financing facilities will eliminate any economic barriers that may limit the integration of AI into criminal proceedings. We have witnessed these types of episodes in which new technologies are used very efficiently by organised crime. This is the case, for example, of the use that criminal organisations have made of cryptographic technologies to guarantee the secrecy of their communications with encrypted communications platforms such as ENCROCHAT and SKYECC[73]. Another factor that will undoubtedly boost the integration of AI into criminal proceedings is the lack of compliance on its part with any type of legal regulations established at national or international level to avoid the harmful effects of this technology. It is therefore to be expected that the degree and pace at which AI is incorporated into the procedures used by organised crime will pose an extraordinary challenge for society and, in particular, for the authorities and organisations responsible for actively combating this scourge.

Blauth et al. (2022)[74] distinguish the ways in which AI can be used with malicious intent in two categories: on the one hand, those in which the vulnerabilities of AI itself are abused (abuse of AI) and, on the other, those in which AI is used (AI-enabled and AI-enhanced crimes) to commit a crime. Within the first category, we find malicious activities such as attacks on the integrity of AI models, the criminal exploitation of unintended and unexpected AI results, the manipulation of high-speed

73 Operation Trojan Shield/Green Light demonstrated the massive criminal use of this technology by criminal organisations around the world. https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

74 Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. IEEE Access, 10, 77110–77122. https://doi.org/10.1109/ACCESS.2022.3191790

algorithmic trading AI systems used in the stock market, or inference attacks that allow the deanonymisation of data used to train algorithms.

As regards the second category, i.e. those malicious uses that leverage AI to enable or facilitate crime, Bhelauth et al. (2022) distinguish between attacks based on social engineering that use deception and phishing to manipulate humans, disinformation and fake news attacks, hacking attacks, which include malware, deepfakes and repetitive attacks, and finally autonomous weapons systems.

Hayward and Maas (2021)[75], for their part, identify AI as a potentially criminogenic phenomenon, both in the sense of its capacity to escalate existing crimes and to facilitate new digital transgressions. These authors establish three criminogenic categories of AI. The first is that of crimes against AI, along the lines of what Blauth et al. (2022) call AI abuse, and they consider AI as the surface or object that suffers the attack. The second category identified by Hayward & Maas (2021) is that of AI crimes (AI as a tool), which corresponds to the category labelled by Blauth et al. (2022) AI-enabled and AI-enhanced attacks. Finally, Hayward & Maas (2021) establish a category that they label crimes committed by AI, which could have an origin in results not expected by the developers of an AI, and which inevitably gives rise to the debate on the legal status of AI algorithms and their possible liability.

From a documentary review point of view, King et al. (2020)[76] identify some crime typologies that can be facilitated by AI, which they call AI-Crime (AIC), and which have been covered in the scientific

75 Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. Crime, Media, Culture, 17(2), 209–233. https://doi.org/10.1177/1741659020917434

76 King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. Science and Engineering Ethics, 26(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0

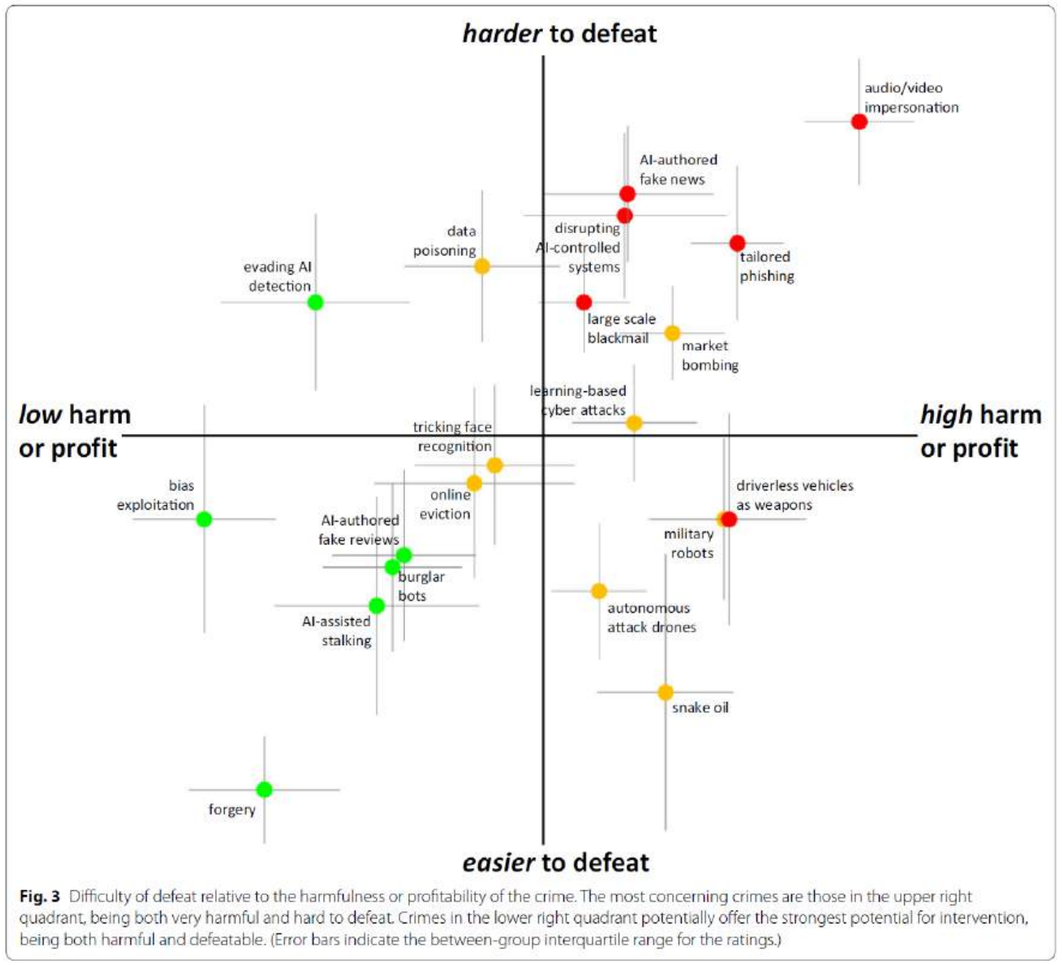


Fig. 3 Difficulty of defeat relative to the harmfulness or profitability of the crime. The most concerning crimes are those in the upper right quadrant, being both very harmful and hard to defeat. Crimes in the lower right quadrant potentially offer the strongest potential for intervention, being both harmful and defeatable. (Error bars indicate the between-group interquartile range for the ratings.)

literature. Firstly, they mention the area of trade, financial markets and insolvency. In this case, the literature analysed raises uncertainty about the possible use of AI in market manipulation, price fixing or in possible crimes of collusion against competition. Another area of crime identified is that of drugs, in which the literature reviewed suggests that AI can be used as an instrument for the trafficking and sale of these illicit substances, from the use of autonomous vehicles for their transport, to the use of machine learning algorithms for advertising the sale of substances through bots on social networks. As regards crimes against persons, the literature focuses on cases of harassment and torture, for example, in relation to harassment through bots on social networks or the use of fake content systematically or not against a person. Regarding sexual crimes, the literature refers to the impact of AI on both sexual assault and abuse and on paedophilia, although the issue is contentious and this involvement of AI in sexual crimes remains a matter of debate as a hypothetical area of AIC. Finally, King et al. (2020) find that the literature connects forgery and identity theft through AIC with non-corporate theft and fraud, and imply the use of machine learning in corporate fraud. In the case of non-corporate theft and fraud, the literature contemplates the use of AI for the collection of an individual's personal data in a first phase and for identity theft in a second.

Another interesting study is that carried out by Caldwell et al. (2020)[77], published in the journal Crime Science, in which they identified and evaluated possible uses of AI for criminal interests.

77 Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. Crime Science, 9(1). https://doi.org/10.1186/s40163-020-00123-8

The study involved representatives from academia, the police, the armed forces, government and the private sector. There were four criteria according to which these possible malicious uses of AI were catalogued: harm to victims, criminal benefit, possibility of criminal execution and the difficulty of counteracting them. The study's findings identified 18 possible uses of AI for criminal or terrorist activity, with 6 of them being most worrying: identity theft via video or audio, tailored phishing, the use of autonomous vehicles as weapons, fake news, large-scale blackmail and sabotage of AI-controlled systems. Below is the graph produced by Caldwell et al. (2020) in their work and which summarises the results of the study because it is considered to be of high interest.

The use of AI tools and technologies is already beginning to be used and exploited by organised crime groups in LAC countries. Examples of some criminal behaviours in which AI tools were used to perpetrate crimes include the following:

3.1. FINANCIAL AND BANKING FRAUD

Cybercrime is one of the areas most affected by the adoption of AI. Advanced algorithms are used to automate attacks such as phishing and financial or banking fraud.

In 2021, Europol, in collaboration with law enforcement authorities from several EU countries, dismantled an international cybercriminal network known as BazarCall, which used AI to carry out large-scale phishing attacks against European and other businesses. This network used AI and advanced social engineering techniques to analyse on-line behaviour, segment potential victims and to send highly personalised fraudulent emails to high-level employees.

BazarCall targeted organisations in the financial and technology sectors, where emails impersonated trusted suppliers or managers, urging employees to make bank transfers or open attachments containing malware. The main objective was to gain access to confidential information and execute fraudulent money transfers.

One of the most notable cases was the attack on the technology company Eurofins Scientific, a global leader in laboratory analysis, which suffered multimillion-dollar losses due to illegal bank transfers facilitated by the attackers' AI. The network also targeted companies in other key sectors in Germany, France, the Netherlands and the UK, infiltrating corporate systems via emails designed to evade traditional fraud detection systems.

Interpol's Financial Fraud Assessment report[78] indicates that there have been recent cases in member countries of the organisation in which deepfake photographs have been generated to open on-line bank accounts in order to expand the networks of mules that provide their services to organised crime. The report notes that there is recent evidence that Latin American criminal groups such as Commando Vermelho, Primeiro Comando da Capital (PCC) and the Mexican Cartel Jalisco Nueva Generación (CJNG) are involved in committing financial fraud.

Money laundering using AI is also on the rise, allowing criminal organisations to conceal the illicit origin of their income through automated transactions and complex financial networks that evade traditional controls.

78 INTERPOL Global Scam Threat Assessment (2023), Interpol.

In 2023, Italian and German authorities, in collaboration with Europol, dismantled a sophisticated transnational money laundering criminal network that used AI and advanced technologies to move illicit funds through cryptocurrencies. This organisation used AI algorithms to identify the safest and fastest routes to transfer money between different cryptocurrency accounts, hiding the illicit origin of the funds.

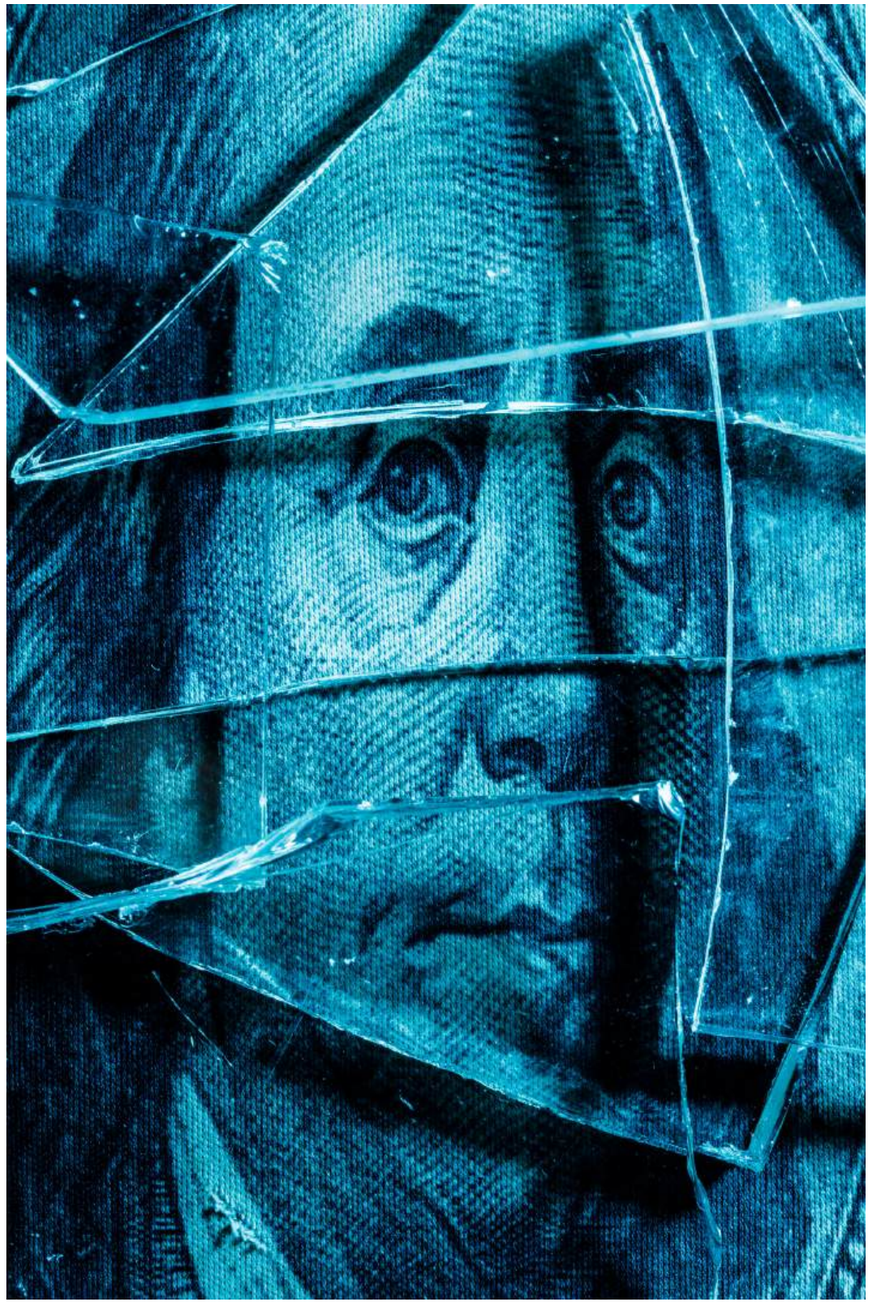
The scheme involved a combination of traditional money laundering and the use of cryptocurrency platforms, taking advantage of regulatory loopholes in certain jurisdictions. The network used AI tools to analyse large volumes of financial transactions and detect vulnerabilities in money laundering monitoring systems, bypassing traditional controls by banking authorities. This approach allowed them to move funds between different jurisdictions in a matter of minutes, making it difficult for regulatory agencies to detect and track the money.

One of the most notable cases of this operation occurred in Italy, where the network laundered money through cryptocurrency platforms such as Binance and Kraken, facilitating rapid transfers to countries with lax or non-existent regulations on the use of cryptocurrencies. Assets worth more than €40 million in cryptocurrencies and property in various parts of Europe were ultimately seized. The operation, dubbed "Operazione Colossus", was coordinated by the Guardia di Finanza in Italy and the Bundeskriminalamt (BKA) in Germany, with technical support from Europol and international financial crime experts.

Finally, algorithmic trading is understood as a process of executing orders through automated and pre-programmed trading instructions to take into account variables such as price, timing and execution volume. In turn, so-called high-frequency trading (HFT) is a subtype of algorithmic trading that follows investment strategies supported by complex mathematical models and focuses on taking advantage of market inefficiencies and short-term price movements.

HFT systems carry out a large number of small purchase and/or sale transactions in very short periods of time, with strategies previously designed to execute operations in microseconds and thus take advantage of the small price fluctuations that occur in these periods. This has contributed to the emergence of flash crashes: sudden and unexpected falls in a very short time, followed by a rapid recovery in the price of securities or assets in a market. This leads to increased volatility and great uncertainty in financial markets[79]. HFT has become a prominent trading strategy in today's financial markets that is gaining traction as its systems are refined.

The integration of AI into HFT has revolutionised financial markets by offering benefits such as faster and more accurate decisions, and greater efficiency and risk management. However, as García



Pedroviejo and Marina[80] point out, ethical and regulatory challenges arise due to the complexity and diversity of AI algorithms. The concern lies in the possibility of chain reactions, the accentuation of market volatility and the possible manipulation of prices and the market through the execution of illicit strategies aimed at market manipulation, such as spoofing and layering as Januário[81] claims. In Brazil, the BM&FBovespa Supervisão de Mercados defines layering as "an abusive practice that creates artificial liquidity in the asset book through layers of offers at successive price levels with the aim of influencing investors to exceed the barrier created by the layer and generate business on the opposite side of the book" and spoofing as "an abusive practice that creates artificial liquidity with offers of sizes outside the standard of the order book with the aim of influencing investors to exceed the artificial offer and generate business on the opposite side of the book"[82]

As this author says, in the United States, the case *USA v. Coscia,* tried in 2015 became famous. The Defendant was a partner and manager of an investment firm that adopted HFT and implemented an algorithm that allowed offers to be sent and cancelled in a very short time. With this, he earned approximately $1.4 million in just 10 weeks, by buying and selling contracts on 10 markets of the CME Group and 3 markets of the ICE Future Europe Exchange. On 26 October 2015, he was sentenced to 36 months in prison and two years of probation[83].

A second strategy that can be mentioned is the so-called quote stuffing. This is the rapid and successive introduction/cancellation of large quantities of orders, causing market volatility and congesting the system, thus making it difficult for other traders to act and react to the large amount of information produced.

In terms of the market and consumers, criminal offences relating to intellectual and industrial property must be included. There have been several reports recently[84] [85] that OpenAI could face a potential lawsuit from actress Scarlett Johansson after she claimed that the voice of ChatGPT maker's now withdrawn chatbot Sky sounded eerily similar to herself.

79 HERNANDO CUÑADO, J. (29 June 2023). Will artificial intelligence take over financial markets? The Conversation. https://theconversation.com/llegara-la-inteligencia-artificial-a-controlar-los-mercados-financieros-205942

80 JOSEFINA GARCÍA, JON MARINA Use of artificial intelligence in the stock market (high-frequency trading). Pérez Llorca Techlaw 2024. https://www.perezllorca.com/wp-content/uploads/2024/03/04-TechLaw-IA_IA-y-Sectores-Regulados.pdf

81 Januário, Túlio Felippe Xavier (2024). Market manipulation and new technologies: the case of high frequency trading VVAA, CALAZA, FONTESTAD AND SUAREZ, Paideia: Legal-procedural perspectives in a changing digital world. COLEX

82 Januário (2024) with quotes from Torres, Marcos José Rodrigues et. al., 2016. Painel: Monitoração de ofertas — Spoofing e layering Workshop sobre Monitoração de Práticas Abusivas de Ofertas, de Prevenção à Lavagem de Dinheiro e de Controles Internos de Suitability. In: BM&FBovespa Supervisão de Mercado — BSM. Available at: https://www.bsmsupervisao.com.br/assets/file/noticias/Monitoraca_Ofertas.pdf [accessed: 04.07.2023]; Costa, Isac Silveira da, 2018. High frequency trading..., op. cit., p. 216-217.

83 Costa, Isac Silveira da, 2018. High frequency trading..., op. cit., p. 230-232. See also: Sousa, Susana Aires de, 2020. "Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial. In: Rodrigues, Anabela Miranda (coord.). A inteligência artificial no direito penal. Coimbra: Almedina, 2020, p. 59-94, p. 64.

84 Hart, R. (4 May 2024). The conflict between Scarlett Johansson and OpenAI could lead to a war between celebrities and AI companies. Forbes Argentina. Accessed 1 June 2024. Available at: https://www.forbesargentina.com/innovacion/javier-milei-entusiasmo-ceos-apple-google-meta-openai-empresarios-software-locales-esperan-una-nueva-era-gracias-ia-n53767

85 Pérez Colomé, J. (21 May 2024). Scarlett Johansson didn›t let ChatGPT use her voice, but OpenAI did anyway: "I was angry, I couldn't believe it." El PAIS. Accessed 1 June 2024. Available at: https://elpais.com/tecnologia/2024-05-21/scarlett-johansson-no-permitio-que-chatgpt-usara-su-voz-pero-openai-lo-hizo-igualmente-me-enfade-no-podia-creerlo.html

This could be the second time Johansson has taken legal action over the same issue. The news broke a few months ago. Johansson appeared in a 22-second ad posted on X/Twitter for an artificial intelligence image-generating app called Lisa AI: 90s Yearbook & Avatar.

The ad, reported by Variety[86], begins with an old clip of Johansson behind the scenes of Marvel's "Black Widow."

3.2. IDENTITY THEFT

Criminal organisations in the region use AI tools to create convincing fake audios and videos, imitating voices or images of victims' relatives. This technology has been used to commit fraud and extortion. For example, in countries like Peru and Argentina, criminals are using deepfakes to simulate the voices of kidnapped relatives and demand ransom payments and extortion[87].

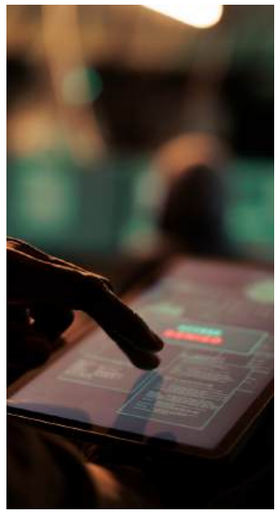
In this area, one of the most emblematic frauds was that which occurred at the English design and engineering company Arup in May 2024, in which the criminals used past video conferences of the company's executives to train the AI tool and recreate a scenario in which the financial director, together with other employees, requested different deposits and bank transfers to be made to one of his employees at his offices in Hong Kong. The employee agreed to make the transfers and it is estimated that the company reported a loss of around $25.6 million dollars[88]. There is no similar case reported in any LAC country.

AI tools have also been used to commit scams related to missing migrants, with criminals generating fake images of their victims to convince their families or relatives that they have been kidnapped in exchange for ransom payments[89]. On the US-Mexico border, criminal groups are reported to be using and manipulating images to scam families of missing migrants.

A video of a young man has gone viral showing how his mother sends him a series of audio messages via WhatsApp, asking him for money. This entire situation is recorded with the mother close by and the audios show errors in diction and from the audios they insist that he not do it to the usual account because she does not have the card to withdraw the money from that usual account and they send her the transfer information for another person. This type of attack is known as vishing, in which AI is used to clone a person's voice to impersonate their identity and send a false message to request money or personal information, all justified by a request close to the victim[90].

In Mexico, criminals managed to impersonate businessman Carlos Slim, whose image was manipulated with AI and used to promote investment schemes among the Mexican population through a phishing link that promised large daily profits[91].

In the area of cryptocurrency transaction and exchange, a cybersecurity company reports about an innovative AI tool used by criminal organisations that has the ability to evade two-factor authentication (2FA) systems by using deepfakes, and through the false identity created by the criminals, they try to use it in the authentication process with cryptocurrency exchange companies to later carry out cryptocurrency-related transactions[92].



3.3. RANSOMWARE AS A SERVICE (RASS)

AI can be used to optimise the effectiveness of ransomware attacks. Algorithms can dynamically alter ransomware code to evade detection by cybersecurity systems, identify valuable files to encrypt, and even decide on ransom amounts. There is evidence that the ransomware group 'BlackCat' used AI techniques and tools in 2023 to bypass traditional cybersecurity defences and spread rapidly across networks, encrypting victims' data before demanding ransom payments[93].

According to TRM Labs, ransomware operators are increasingly leveraging and using AI to improve the efficiency and impact of their attacks, such as automating ransomware campaigns, allowing criminal groups to generate more convincing phishing emails, identify system vulnerabilities more efficiently and optimise ransomware attacks[94].

3.4. PHISHING AND SOCIAL ENGINEERING

Criminals are using advanced AI models based on ChatGPT and similar chatbots to generate more convincing phishing emails and text messages at scale, making social engineering attacks targeting victims more sophisticated and harder to detect. According to security firm Keeper, there has been a 51% increase in AI-powered phishing attacks[95]. Examples can be found in FraudGTP and Metasploit.

FraudGTP is a product sold on the dark web and Telegram that works similarly to ChatGPT but creates content to facilitate cyberattacks. It was first identified and advertised by Netenrich threat research team members in July 2023[96].

86 Shanfeld, E. (1 November 2023). Scarlett Johansson Takes Legal Action Against AI App That Ripped Off Her Likeness in Advertisement. Variety. Accessed 1 June 2024. Available at: https://variety.com/2023/digital/news/scarlett-johansson-legal-action-ai-app-ad-likeness-1235773489/

87 El Comercio, "Voices of people are cloned with AI to scam or fake kidnappings: at least 55 cases in Peru", 16 July 2023, at: https://elcomercio.pe/lima/clonacion-de-voz-para-estafar-con-inteligencia-artificial-como-funciona-esta-modalidad-y-que-recomendaciones-seguir-inseguridad-deepfake-ciberdelincuencia-hackers-secuestros-noticia/

88 FORTUNE, "A deepfake 'CFO' tricked the British design firm behind the Sydney Opera House in $25 million scam", 17 May 2024 at: https://fortune.com/europe/2024/05/17/arup-deepfake-fraud-scam-victim-hong-kong-25-million-cfo/

89 ASMANN, Parker. InSight Crime, "4 Ways AI is Shaping Organised Crime in Latin America" 15 August 2018, at: https://insightcrime.org/news/four-ways-ai-is-shaping-organized-crime-in-latin-america/

90 RIOS, Juan. Infobae. (October 29 2024). Be careful on WhatsApp: they copy your mother's voice, use AI to create the scam and steal money from the bank. Infobae. https://www.infobae.com/tecno/2024/10/29/cuidado-en-whatsapp-copian-la-voz-de-tu-mama-usan-ia-para-crear-la-estafa-y-roban-dinero-del-banco/

91 El Economista, "Slim's new investment platform is fake; they use AI to defraud", 26 November 2023, at: https://www.eleconomista.com.mx/finanzaspersonales/Nueva-plataforma-de-inversiones-de-Slim-es-falsa-utilizan-IA-para-defraudar-20231126-0023.html

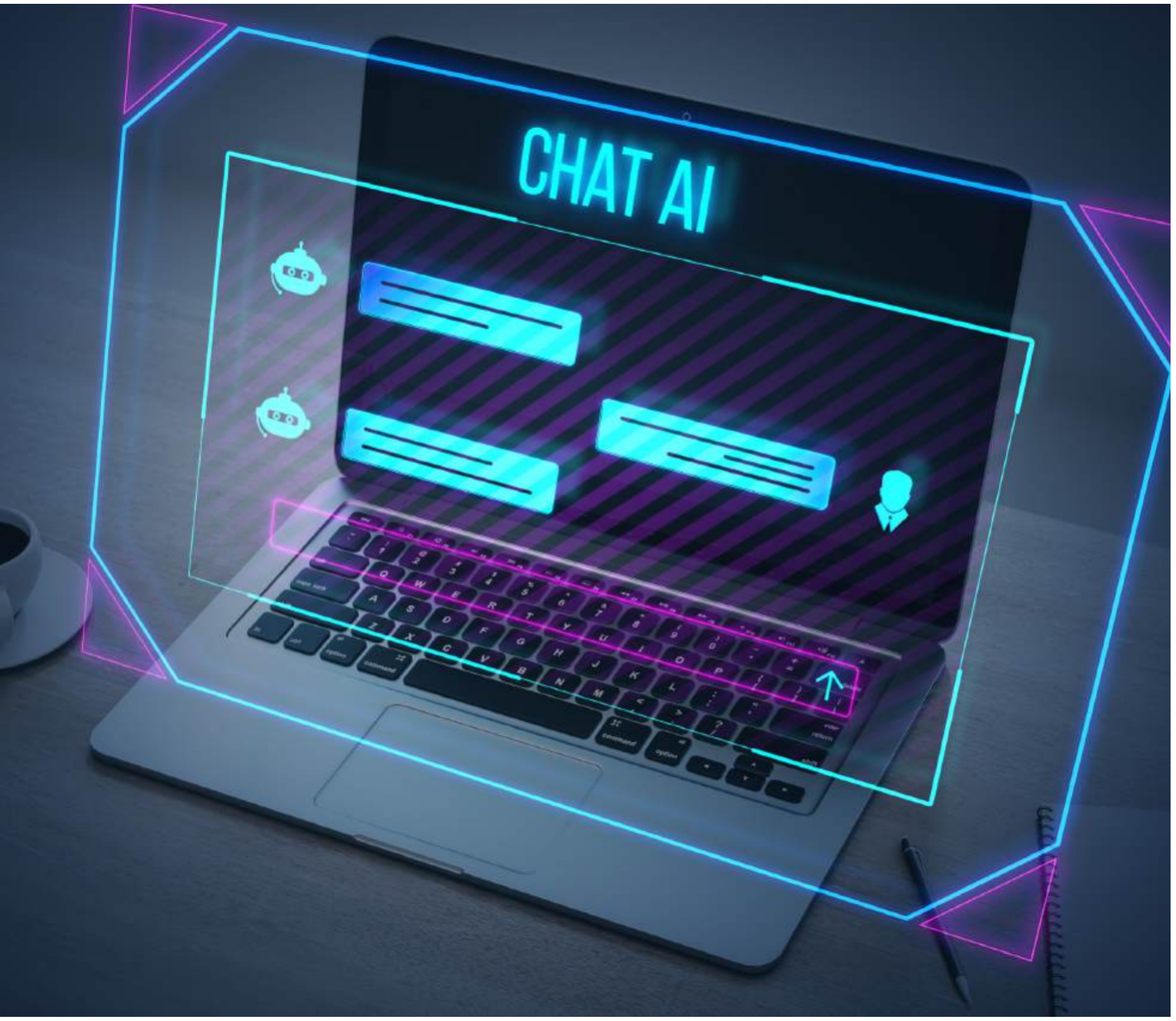
92 TechInformed, "Deepfake cybercrime tool threatens crypto exchanges" 15 October 2024 at: https://techinformed.com/deepfake-cybercrime-tool-threatens-crypto-exchanges/

93 Centre for Internet Security (CIS), "Breaking down the BlackCat Ransomware Operation" at: https://www.cisecurity.org/insights/blog/breaking-down-the-black-cat-ransomware-operation

94 TRM, "Ransomware in 2024: Latest Trends, Mounting Threats, and the Government Response", 11 October 2024, at: https://www.trmlabs.com/post/ransomware-in-2024-latest-trends-mounting-threats-and-the-government-response

95 Keeper, "How AI is making phishing attacks more dangerous," 13 September 2024 at:https://www.keepersecurity.com/blog/es/2024/09/13/how-ai-is-making-phishing-attacks-more-dangerous/

96 AMOS, Zac. (2023/08/11) What is FraudGPT? HackerNoon. https://hackernoon.com/lang/es/que-es-fraudegpt



Criminal groups are using AI systems to optimise the selection and recruitment of young people and minors to carry out illicit activities such as romance scams, cryptocurrency investment scams, extortion and kidnappings.

Similarly, artificial intelligence combined with social engineering can be used to influence an electoral process through armies of bots.

Another possibility for committing crimes using LLMs is the so-called *prompt injection. According to Kosinski and Forrest*[97], a prompt injection is a type of cyber attack against large language models (LLMs). Hackers disguise malicious inputs as legitimate prompts, manipulating generative AI (GenAI) systems to leak sensitive data, spread misinformation, or worse.

Within the scams category, one of those possible through these technologies such as *deepfake is procedural fraud, in such a way that an attempt is made to deceive the judge with false evidence in a trial.*

97 KOSINSK M. AND FORREST A. (26 March 2024. Prompt injection. IBM Research. Retrieved from https://www.ibm.com/es-es/topics/prompt-injection

3.5. HUMAN TRAFFICKING: ON-LINE RECRUITMENT AND EXPLOITATION

AI is also revolutionising human trafficking, particularly in the recruitment and exploitation of victims through digital platforms. Criminal networks use AI to identify vulnerable individuals and target them more accurately, exploiting patterns of on-line behaviour as evidenced in several recent UNODC reports on human trafficking in Europe.

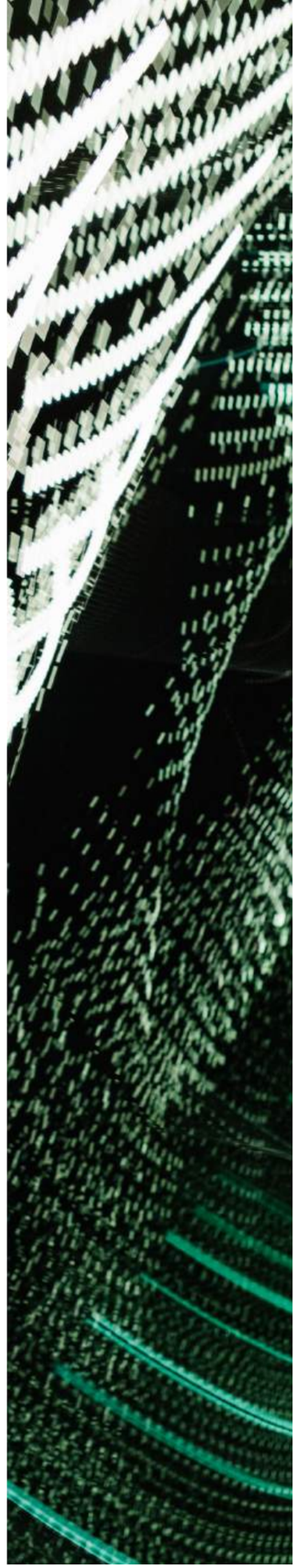
An example of this is what happened in 2022, where the Spanish National Police and the French National Gendarmerie, in a joint operation with Europol, dismantled a sophisticated human trafficking network that used artificial intelligence to recruit and exploit young women from Eastern Europe and North Africa. This criminal network, specialised in sexual exploitation, used advanced AI algorithms to identify, manipulate and attract victims through social networks and on-line dating platforms.

The AI algorithms used by this criminal network analysed the psychological and socio-economic profiles of potential victims, segmenting young women in vulnerable situations, such as poverty, unemployment or family problems. The AI systems were able to filter these data from the victims' on-line interactions, social media comments and search activity. Using this information, the criminals personalised messages and offered false job opportunities in Western Europe, such as jobs in the fashion industry, hospitality or domestic work.

Once trust was established, the victims were convinced to travel to countries such as Spain and France, where, upon arrival, their documents were confiscated and they were forced to work in prostitution networks. The victims came mainly from Romania, Bulgaria, Morocco and Algeria, countries with high levels of vulnerability to this type of exploitation.

The network also used AI to bypass social media and advertising platforms' content moderation systems, hiding its illegal sexual services ads. These algorithms were able to change keywords and ad content to avoid detection by the platforms' automated filters. They posted on classified ads and social media sites like Facebook and Instagram, offering services that were actually covers for sexual exploitation.

The ads were frequently changed, adapting language to local regulations and using manipulated images to avoid detection by content control systems, making it extremely difficult for authorities to track criminal activity in real time.



3.6. CRIMES OF SEXUAL ABUSE AND EXPLOITATION

GAI systems have the ability to generate and transform text and images of children and adolescents with sexual abuse and exploitation content on a large scale and with such precision that they are very difficult to identify and distinguish[98]. According to NCMEC, the prevalence of child sexual abuse and exploitation content generated through GAI is extremely difficult to estimate and since 2023 the organisation has begun to include a classification with statistics regarding the number of reports provided with content of sexual abuse and exploitation generated by GAI systems through CyberTipline[99]. Furthermore, the use of sex robots for child abuse has begun to be detected, either remotely or under the control of artificial intelligence or autonomous systems, or in a more mechanical manner. However, they can be constructed using 3D printers and plans developed by AI or people for both legal and illegal purposes[100] [101].

3.7. CYBERVIOLENCE BEHAVIOURS

There are free and paid AI applications that allow images of women to be generated, reproduced and edited to show them naked through the use of deepfakes[102]. According to WIRED, non-consensual explicit content created by deepfake bots via Telegram has increased exponentially. The publisher reports that there are at least 50 bots currently active that serve more than 4

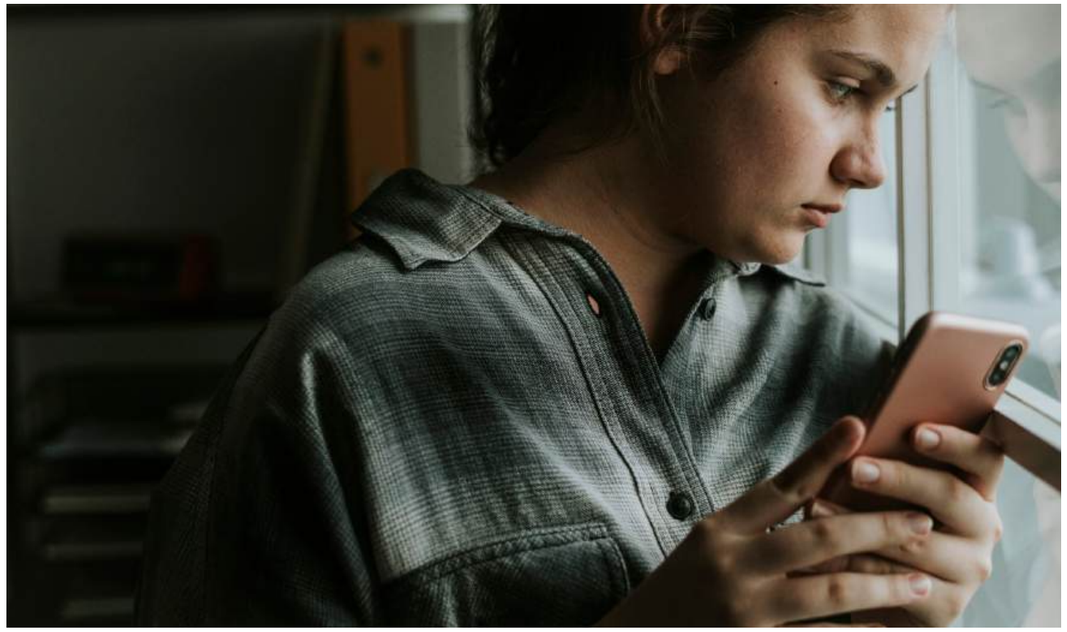
98 For a description of the types of abusive and exploitative images and content generated with AI, see: Centre for Artificial Intelligence and Robotics at the United Nations Interregional Crime and Justice Research Institute (UNICRI), "Generative AI. A New Threat for On-line Child Sexual Exploitation and Abuse", 2024, pp. 9-13 at: https://unicri.it/News-Generative-AI-Threat-Child-Sexual-Exploitation-Abuse

99 "Generative AI. A New Threat for On-line Child Sexual Exploitation and Abuse", *op. cit*, p. 13.

100 The paedophile who was building a sex robot for a minor Available at: https://www.elpatagonico.com/el-pedofilo-que-estaba-construyendo-un-robot-sexual-un-menor-n5992054

101 Durán San Juan, Isabela. (2024). How will robots and artificial intelligence transform sexual relations in the future? Infobae. Available at: https://www.infobae.com/tecno/2024/04/12/como-los-robots-y-la-inteligencia-artificial-transformaran-las-relaciones-sexuales-del-futuro/

102 See: https://nudify.info/download-apps-like-deepnude-alternatives/



million requests monthly on the Telegram platform and that are used to attack thousands of women and girls around the world[103].

Although cyberviolence is generally committed by social circles close to the victims, it has the potential to create serious harm and psychological impact on women, girls and vulnerable LGBT groups. This is what is mainly called Technology-facilitated violence against women and girls (TFVaWG) and which already has its own name due to its current impact.

In Peru, there was a case in August 2023 in a private school where students generated and edited deepfake images of their classmates with naked bodies and shared and marketed them outside the school circle[104]. This type of activity can have future re-victimisation repercussions since the images can end up circulating on the DarkNet and can subsequently be used for criminal purposes by stalkers, extortionists and paedophiles.

In Argentina, a case is reported in October 2024 in a school in the town of San Andrés in the Buenos Aires district of San Martín where an under-age student used AI applications to manipulate photos of his classmates obtained from the social networks to turn them into nudes and subsequently market the edited images through the Discord application. It is reported that 22 female students were victims of this crime, all under 18 years of age[105]. The Almendralejo file in Spain (2023) is another case of manipulation of photographs and videos showing naked minors using AI applications and tools.

This type of activity can have serious future repercussions of re-victimisation since the images can end up circulating on the DarkNet and can subsequently be used for criminal purposes by stalkers, extortionists and paedophiles.

103 WIRED, "Millions of People Are Using Abusive AI 'Nudify' Bots on Telegram" 15 October 2024, at: https://www.wired.com/story/ai-deepfake-nudify-bots-telegram/#intcid=_wired-right-rail_c0163b39-a6b8-486b-8f60-b788683ebd84_popular4-1-reranked-by-vidi

104 Infobae, "Chorrillos: Schoolchildren who altered photos of classmates with AI and marketed them were not expelled, 29 August 2023 at: https://www.infobae.com/peru/2023/08/29/chorrillos-escolares-que-alteraron-fotos-de-sus-compaeras-con-ia-para-venderlas-no-fueron-expulsados/

105 Clarín, "Scandal at a school in San Martín: a student is reported for selling AI-manipulated photos of his classmates naked" 14 October 2024, at: https://www.clarin.com/policiales/escandalo-colegio-san-martin-denuncian-alumno-vendia-fotos-manipuladas-ia-companeras-desnudas_0_hqEbfd1Plm.html?srsltid=AfmBOoqd3x3x-znnG_za1bJ_yPAkS9QnoX6HxZjyMUm7TUIahZCxAckV

BLOCK 4: USE OF AI TOOLS BY JUSTICE AND SECURITY INSTITUTIONS

4.1. AI IN JUSTICE INSTITUTIONS

AI has emerged as a key support tool for justice institutions, offering solutions that enable not only faster analysis of large volumes of information, but also the optimisation of judicial decision-making. This section of the study focuses on how courts, judges, prosecutors and other legal players are using AI in the fight against organised crime, particularly in Latin American countries, where criminal networks are highly sophisticated. Furthermore, AI also has the potential to reduce the workload of courts by automating repetitive tasks and facilitating access to legal information, which is also key in the fight against organised crime, as it allows for more effective management of the complex cases that these criminal networks represent.

Such is the relevance that, in the European Union, the European Commission for the Efficiency of Justice (CEPEJ) is advancing in its efforts to use AI in judicial systems, with emphasis on the creation of certification mechanisms for AI tools and services. During the 42nd Plenary Meeting in June 2024, several projects related to AI and cyberjustice were highlighted, including contributions from CEPEJ's working groups on justice quality (CEPEJ-GT-QUAL) and cyberjustice (CEPEJ-GT-CYBERJUST).

In relation to the above, we highlight two important points. On the one hand, CEPEJ has developed the Ethical Charter on AI in Judicial Systems, which establishes key principles for the use of AI in judicial systems. These principles include transparency, non-discrimination and respect for fundamental rights, ensuring that AI applications respect fairness in judicial processes and that automated decisions are auditable and understandable. In other words, it aims to guide both technology developers and justice legislators and professionals, promoting the implementation of these principles in several European countries, organising training and events to raise awareness as to the risks and benefits of using AI in justice.

Furthermore, it is working on an impact assessment mechanism for AI products used in European judicial systems, which aims to ensure that the tools developed both by the public and private sectors comply precisely with the ethical guidelines established in the Ethical Charter on AI in Justice. This initiative seeks to ensure that algorithms and technological tools respect the principles of transparency, impartiality and human control, which are fundamental in the judicial field.

In addition to the above, among current projects, CEPEJ has worked on the creation of a Cyberjustice and AI Resource Centre, which provides information on technological tools applied in the judicial field. This centre not only facilitates the exchange of good practices between Member States, but also provides guidance on the risks and benefits of using AI in courts. The Resource Centre focuses on public sector systems, whether implemented by or relevant to the judiciary. This may include publicly available academic models or general purpose AI systems (e.g. ChatGPT,

Co-Pilot), but does not include systems geared towards lawyers or law firms (LegalTech). Entries are collected through members of the CEPEJ European Cyberjustice Network (ECN). The network is made up of individuals from almost all Council of Europe member states and observers, responsible for the digitalisation of national judicial systems. The information collected is discussed and categorised by the CEPEJ Artificial Intelligence Advisory Board (AIAB).

It has also established the AI Advisory Board (AIAB), which provides expert guidance on putting the principles of the Charter into operation. The Council is currently working on an assessment tool that will enable judicial authorities to evaluate their AI systems' compliance with established ethical principles. The assessment process aims to bring the CEPEJ Charter into operation by providing a set of checks, key measures and safeguards that decision-makers within the judicial system should follow when purchasing, designing, developing, implementing and/or using AI in judicial systems. It is based on evaluating AI products according to criteria related to transparency, quality and ethics. Tools that pass this filter are supposed to voluntarily comply with a higher ethical standard, which provides confidence to both justice operators and citizens who interact with these technologies. CEPEJ believes that the creation of an independent and standardised evaluation system to certify these products will ensure that AI systems are reliable and do not compromise the equality or fundamental rights of individuals involved in judicial processes. The AI Advisory Board is also currently working on an annual report that will provide a concise summary of the results of the ongoing monitoring of emerging artificial intelligence or other key cyberjustice tools applied in public justice systems (hereinafter collectively referred to as cyberjustice tools), conducted through the CEPEJ Resource Centre on Cyberjustice and Artificial Intelligence (hereinafter referred to as "the Resource Centre" or "the Centre"). A document on AI and efficiency in justice has also been prepared. CEPEJ has commissioned CEPEJ-SATURN and CEPEJ-GT-CYBERJUST to study the possible effects of the use of AI systems on court efficiency (see CEPEJ's 2024-2025 Activities Programme) and is currently developing another on Generative AI in courts.

Ultimately, these efforts seek to ensure that the technological solutions implemented respect fundamental rights, in accordance with the European Ethical Charter on the Use of AI in Judicial Systems, adopted in 2018[106], and underlining CEPEJ's commitment to the digital transformation of the European judicial system by ensuring that AI is used safely and efficiently in line with human rights.

This past June, the POLICY FOR THE USE OF ARTIFICIAL INTELLIGENCE IN THE ADMINISTRATION OF JUSTICE was approved by the General Secretariat of the CTEAJE[107] aimed at all workers in the Administration of Justice but which nevertheless has to be specifically ratified for adoption by the General Council of the Judiciary (CGPJ), the State Attorney General's Office (FGE), the Autonomous Communities with powers in matters of Justice and the Ministry of the Presidency, Justice and Relations with the Courts (MPJRC).

UNESCO has also launched an open consultation on new guidelines for the use of AI in judicial systems[108], which aim to ensure that AI technologies are integrated into judicial systems in a way that upholds justice, human rights and the rule of law. A draft set of guidelines developed following UNESCO's survey on the use of artificial intelligence by judicial operators.

One of the most comprehensive works for judicial operators developed to date appears in UNESCO's *Global Toolkit on AI and the Rule of Law for the Judiciary*[109]. This toolbox responds to these needs and provides judicial players (judges, prosecutors, state prosecutors, public attorneys, law universities and judicial training institutions) with the knowledge and tools necessary to understand the benefits and risks of AI in their work. The toolkit will assist judicial players in mitigating the potential human

106 See, https://protecciondata.es/wp-content/uploads/2021/12/Carta-Etica-Europea-sobre-el-uso-de-la-Inteligencia-Artificial-en-los-sistemas-judiciales-y-su-entorno.pdf

107 https://www.administraciondejusticia.gob.es/documents/7557301/7558184/CTEAJE-NOR-Politica+de+uso+de+la+IA+en+la+AJ+v1.0.pdf/ddc0eda1-950b-e926-b367-be511b16f2f9?t=1721386535984

108 https://unesdoc.unesco.org/ark:/48223/pf0000390781

109 https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa

rights risks of AI by providing guidance on relevant international human rights laws, principles, standards and jurisprudence that underpin the ethical use of AI.

INTERNATIONAL LEGAL COOPERATION PROJECTS AND INITIATIVES

In this section it is worth highlighting the INSPECTr Project (Intelligence Network and Secure Platform for Evidence Correlation and Transfer), which ran from September 2019 to August 2022. It was an initiative funded by the European Union within the framework of its Horizon 2020 programme and its main objective was to improve the digital and forensic capabilities of security forces and judicial institutions through the use of advanced technology.

INSPECTr addressed the challenges facing criminal justice systems in the fight against cross-border and organised crime by integrating a range of cutting-edge technological tools for the collection, analysis and exchange of information between different jurisdictions and which can be summarised as follows:

Big data analysis: INSPECTr used big data analysis to identify patterns and correlations in information flows, facilitating the early detection of complex and organised criminal activities. Real-time data processing capabilities enabled law enforcement agencies to efficiently extract key information, even in scenarios with large amounts of unstructured data, such as social media, encrypted communications, or international financial transactions. This improved the ability to identify transnational criminal networks, enabling a faster and more coordinated response.

Cognitive machine learning: The project also incorporated machine learning algorithms that enabled intelligence platforms to automate the detection of threats and patterns of criminal behaviour. By using cognitive machine learning, INSPECTr improved predictive analysis, helping justice institutions anticipate potential crime scenarios and optimise resource allocation. These technologies allowed for more precise classification of information, facilitating more informed judicial decision-making.

Blockchain for information security: Blockchain technology was key to ensuring the integrity and traceability of evidence in the judicial process. By integrating blockchain into the platform, INSPECTr was able to create a system that allowed every interaction and data transfer between different players to be tracked, ensuring that evidence was not altered in storage or transmission. This is especially relevant in cases of organised crime, where tampering with evidence can seriously compromise judicial proceedings.

Thanks to this technology, INSPECTr has enabled authorities to improve their capacity to manage complex investigations, enhance legal certainty in data transmission and ensure that judicial proceedings are more efficient and effective.

One of the most innovative aspects of the project was the development of a shared intelligence platform that facilitated cross-border collaboration between criminal justice agencies. International data sharing has been seen as critical to combating organised crime, which often operates across a number of countries. However, this exchange presented challenges such as compatibility between systems in different jurisdictions and the protection of the privacy of the individuals involved. The INSPECTr platform reduced the complexity and cost of information exchanges, providing a secure space where law enforcement and judicial systems could collaborate in correlating and analysing evidence. A crucial aspect was the interoperability of the judicial and security systems of different countries, allowing mutual access to databases, which accelerated the response time to international crimes. The platform also allowed for secure storage of information in the cloud, minimising the risk of data loss or manipulation.

Translation and interpretation are also very important in the field of international legal cooperation. In this regard, the EU has been funding various research projects that will certainly contribute or are contributing to the use of video conferencing in international legal cooperation. Among them, we can highlight **AVIDICUS (Assessment of Video-Mediated Interpreting in the Criminal Justice System)**. This was a three-stage project focused on assessing the reliability and quality of video-mediated interpreting (VMI) in criminal proceedings in order to improve judicial cooperation in Europe, which are as follows:

AVIDICUS I (2008-2011): The focus was on investigating the effects of using video conferencing in court interpreting and how this affects the quality and accuracy of communication.

AVIDICUS II (2011-2013): Focused on expanding the analysis with comparative studies at European level, exploring the use of video conferencing for interpreting in multiple judicial contexts.

AVIDICUS III (2014-2016): This addressed the practical implementation of video-mediated interpreting, providing specific training for both interpreters and legal professionals, thereby improving skills and mutual understanding during court proceedings.

Work is also being done on other artificial intelligence projects that enable machine translation. That is, the translation would be carried out by a computer program without human intervention, as is the case of the **eTranslation programme**, promoted by the European Commission under the Connecting Europe Facility (CEF) programme. This is a key tool for machine translation in cross-border court proceedings, including criminal trials conducted via video conference. Its main objective is to eliminate language barriers in the EU's single digital market by facilitating communication and judicial cooperation through high-quality machine translations in all official languages of the Union. This technology is being integrated into digital court platforms such as the European Justice Portal to ensure that parties involved in cross-border trials, including witnesses and defendants, can give evidence in their native language, with immediate automatic translations during video conferences. This is essential for criminal trials where language barriers can be an obstacle to the taking of evidence or testimony and thus contribute to the prosecution of complex criminal cases.

The MARCELL project (Multilingual Resources for CEF.AT in the Legal Domain) is an initiative that seeks to improve machine translations in the legal field, also within the framework of the Connecting Europe Facility (CEF) programme. Its main objective is to collect and structure large amounts of multilingual legal data from the national legislations of several European countries, in order to optimise the accuracy of machine translations in legal contexts, using the eTranslation tool. MARCELL focuses on processing legislative and regulatory documents in multiple languages, ensuring that specific legal terms are translated correctly and maintain their legal context. This is especially useful for cross-border trials, where language barriers can complicate the judicial process. The project covers 7 languages: Bulgarian, Croatian, Hungarian, Latvian, Romanian, Slovak and Slovenian, and works closely with public institutions in these countries to create reliable language resources. It therefore also supports eTranslation by providing linguistic data on specific legal sectors from various European countries, which improves the ability of AI to translate complex legal terms, resulting in better accessibility in cross-border procedures.

COURT CASE MANAGEMENT

It is increasingly known that AI enables greater efficiency in the processing of cases, facilitates the detection of patterns and improves cross-border cooperation between judicial agencies. In Europe, several member states have adopted advanced technological solutions to address these problems, including Germany and other countries with similar initiatives.

Germany highlights **OLGA (On-line-Strafverfahrensregister für Organisierte Kriminalität und Geldwäsche)**, or "On-line register of criminal proceedings for the fight against organised crime and money laundering"). This is a digital system developed to centralise and manage organised crime cases that allows prosecutors and judges to access a platform containing all the data from related investigations, providing a global and unified view of illegal activities and thus optimising the processing of long and complex procedures, helping to reduce judicial response time.

Also in Germany we find **Frauke (Fraud Analysis Using Knowledge Extraction)**. An AI project aimed at detecting fraud and money laundering patterns in large financial databases. Using machine learning algorithms, Frauke analyses suspicious transactions and behaviour, providing authorities with detailed reports that help prioritise investigations. This approach is especially useful in cases involving transnational organised crime, where financial flows are often opaque and dispersed.

In the UK, a Smart Court system uses AI tools to manage case flow and improve efficiency. This includes the implementation of technologies that facilitate data collection and analysis, allowing lawyers and judges fast access to relevant case information. This approach has also made it possible to identify patterns of organised crime, facilitating coordination between different judicial agencies.

France has introduced **TAJ** (Traitement d'Antécédents Judiciaires - Court Background Processing), a national database that stores criminal history data and is connected to AI systems to analyse patterns of criminal behaviour. This system helps law enforcement authorities track and manage multiple simultaneous investigations.

Furthermore, AI, specifically in the field of natural language processing (NLP), is emerging as a key tool for managing complex judicial proceedings in Europe. This technology makes it possible to automate tasks that have historically required a large amount of human resources and time, such as reviewing legal documents, searching for relevant jurisprudence and translating texts between different languages. The European Union has recognised the potential of NLP in modernising judicial systems and has promoted various initiatives to encourage its development and application.

In relation to this we find Horizon 2020. This is a European Union framework programme for research and innovation (2014-2020) that has funded projects aimed at creating AI technologies applicable to sectors such as justice and public governance. In the field of natural language processing, Horizon 2020 has promoted research to develop tools capable of analysing large volumes of legal documents and streamlining decision-making. This includes projects that enable judicial and legal authorities to search for precedents and regulations in multiple languages and in real time, thereby improving efficiency in judicial proceedings involving different jurisdictions or international contexts.

In this regard, through its Panel for the Future of Science and Technology (STOA - Scientific and Technological Options Assessment), the European Parliament has conducted studies on the impact of AI technologies, including natural language processing, on justice and other key sectors. These studies focus on how AI can assist judges, lawyers and administrative staff in managing lengthy and complex court proceedings. STOA has analysed the advantages of using AI to reduce human errors in the interpretation of regulations, to improve consistency in judicial decisions, and to offer more accessible tools for managing large amounts of information.

An example of this at the procedural level can be found in Estonia. Estonia has been a pioneer in the digitalisation of the judiciary, and is currently developing a system that incorporates artificial intelligence for the management of criminal cases. This system seeks to optimise the assignment of sentences, the monitoring of compliance with alternative measures and the analysis of large volumes of procedural data. Using AI, the system can identify patterns in court decisions and suggest corrective actions, making it easier to track convicts across the country.

4.2. AI IN SECURITY INSTITUTIONS

As in many other disciplines and fields, AI and its potential applications are a hot topic in the field of criminal investigation. In a recent article, Olowe et al. (2023)[110] analyses the existing literature on this issue, highlighting that studies to date are predominantly focused on the objective of generating proactive measures to deter and prevent crime through predictive estimates. The following table contains the bibliographic search parameters used by the author for his study.

Criteria	Metrics
Keywords	"crime" OR "criminal investigations" OR "police" OR "policing" AND "AI" OR "artificial intelligence" OR"facial recognition" OR "deep learning" OR "machine learning" OR "neural network" OR "natural language processing" OR "computer vision"
Year range	2012-2022
Subject area	Computer Science, Arts & Humanities, Psychology, Business, Management and Accounting, Decision Sciences, Social Sciences and Multidisciplinary
Document type Source Type	Journal Articles and IS Conference Papers Journal and Conference Proccedings
Publication stage Language	Final English

Table 1. Research protocol for bibliometric review

110 Olowe, O., Kawalek, P., & Odusanya, K. (2023). *Artificial Intelligence Adoption in Criminal Investigations: Challenges and Opportunities for Research*. https://aisel.aisnet.org/ukais2023

As can be seen in the table below, in this same study[111] the keywords of all the bibliography subject to the study on the application of AI to criminal investigation are analysed, concluding that the most frequently used terms are Machine Learning, Fraud Detection, Deep Learning, Malware, Cybersecurity and social networks.

Rank	Keyword	Occurrences
1	Machine Learning	27
2	Fraud Detection	19
3	Deep Learning	12
4	Malware	6
5	Cyber Security	5
6	Social Media	5
7	Intrusion Detection System	4
8	Cyberbullying	4
9	Artificial Intelligence	4
10	Class Imbalance	4
11	Crime Prediction	3
12	Twitter	3
13	Malware Detection	3
14	Anomaly Detection	3
15	Text Mining	3

Table 3. Top 15 most occurring author keywords

Machines equipped with AI, just like programs or software, can help investigators shorten the time spent on various tasks throughout different stages of the investigation process[112]. From case management and direction to staff management to reporting, AI-enabled systems enhance workflow automation and can provide assurance that management procedures are executed in a consistent and transparent manner. This efficiency frees up resources from operations and boosts the organisation's overall effectiveness[113].

Below are some of the applications of AI to criminal investigation that are being taken much into account.

111 Same

112 Singh Sankhla, M., Kumar, R., & Jadhav, E. B. (2020). Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation. *Seybold Report*, *15*(8). https://www.researchgate.net/publication/343826071

113 Varma Microsoft, P. (s. f.). *Transforming Law Enforcement Policies and Governance Procedures: The Benefits of AI Integration*. https://doi.org/10.5678/ijai.2020.12345

APPLICATIONS OF AI IN CRIMINAL INVESTIGATION

RISK ANALYSIS AND PREDICTIVE POLICING

Risk analysis is present in many stages of the criminal justice system in the United States, providing assessments regarding arrests, sentencing, corrective measures, or re-entry into prison[114]. It is reasonable to think that in the strict scope of investigation, assessments of a similar nature may be of interest to the investigator in relation to the profiling of criminals or the prioritisation of lines of investigation.

Indeed, algorithms can be deployed to contribute to legal advisory and decision-support tasks in the field of criminal investigation. AI capable of listening and deciding on small requests has been deployed and tested in Estonia. In these criminal justice environments, AI algorithms are mainly used to evaluate the profiles of those under investigation and the predictability of recidivism, mainly affecting the issuance of sentences[115] [116] [117].

In the United States, where AI is most widely deployed in the criminal justice system, it is worth highlighting the decision adopted by the Wisconsin Supreme Court on a risk analysis algorithm used in the prosecution of the case of Loomis v. Wisconsin (2016). This algorithm is known as Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), and in the ruling in question, the court ruled that the use of the algorithm did not constitute a violation of the defendant's right to a fair trial, since other arguments were used on which to base the decision, apart from the result of the algorithm[118].

Law enforcement agencies around the world have long been making predictions about the incidence of criminal activity, and deploying officers and police resources based on these risk assessments[119], but as mentioned, AI can also play a very relevant role in managing an investigation through data analysis and decision support, for example, by helping to define and prioritise lines of enquiry.

In the police field, the concept of risk analysis is directly related to the term predictive policing, which covers different methods of predicting criminal activity based on probability calculations. These methods assume that criminal activity is subject to the rules of probability and that predictions can therefore be made based on past data. But, indeed, this method can also be applied to identify potentially dangerous individuals. This predictive policing, unlike other forensic disciplines, is intended to have effects before the crime takes place[120] [121].

Indeed, the role of AI in crime prevention is becoming increasingly relevant, offering innovative solutions to improve security measures and reduce criminal activity[122]. Big Data in the criminal field allows the development of data-driven policing, that is, the development of police activity

114 Garrett, B. L., Rudin, C., Williams, L. N., Beale, S. S., Benjamin, S., Boyle, J., Buccafusco, C., Dellinger, W., Fergusen, A., Griffin, L., Grunwald, B., Helfer, L., Kang, S., Lemos, M., Meltzer, A., Park, H., Purdy, J., Rai, A., Siegel, N., … Weiner, J. (2023). *The right to a glass box: Rethinking the use of artificial intelligence in criminal justice*.

115 Simmler, M., Brunner, S., Canova, G., & Schedler, K. (2023). Smart criminal justice: exploring the use of algorithms in the Swiss criminal justice system. *Artificial Intelligence and Law*, *31*(2), 213-237. https://doi.org/10.1007/s10506-022-09310-1

116 Faqir, R. S. A. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. *International Journal of Cyber Criminology*, *17*(2), 77-94. https://doi.org/10.5281/zenodo.4766706

117 Kanwel, S., Imran Khan, M., & Usman, M. (2023). From Bytes to Bars: The Transformative Influence of Artificial Intelligence on Criminal Justice. *Qlantic Journal of Social Sciences*, *4*(4), 84-89. https://doi.org/10.55737/qjss.059046443

118 Same.

119 Garrett, B. L., Rudin, C., Williams, L. N., Beale, S. S., Benjamin, S., Boyle, J., Buccafusco, C., Dellinger, W., Fergusen, A., Griffin, L., Grunwald, B., Helfer, L., Kang, S., Lemos, M., Meltzer, A., Park, H., Purdy, J., Rai, A., Siegel, N., … Weiner, J. (2023). *The right to a glass box: Rethinking the use of artificial intelligence in criminal justice*.

120 Simmler, M., Brunner, S., Canova, G., & Schedler, K. (2023). Smart criminal justice: exploring the use of algorithms in the Swiss criminal justice system. *Artificial Intelligence and Law*, *31*(2), 213-237. https://doi.org/10.1007/s10506-022-09310-1

121 Singh Sankhla, M., Kumar, R., & Jadhav, E. B. (2020). Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation. *Seybold Report*, *15*(8). https://www.researchgate.net/publication/343826071

122 Kanwel, S., Imran Khan, M., & Usman, M. (2023). From Bytes to Bars: The Transformative Influence of Artificial Intelligence on Criminal Justice. *Qlantic Journal of Social Sciences*, *4*(4), 84-89. https://doi.org/10.55737/qjss.059046443

through decisions based on data analysis and not solely on intuition or past experiences[123]. At a higher scale of sophistication, AI-driven data analysis, i.e. based on the use of AI, strengthens security agencies in developing evidence-based strategies to address societal needs and emerging threats. By analysing large volumes of data, including crime statistics, social media feedback, and demographic trends, AI algorithms provide insight into underlying problems that may be going undetected, enabling law enforcement officials to decide on targeted interventions and efficiently allocate resources.[124] An example of this application could be an AI-based algorithm that assesses the risk of a gender-based violence attack taking place in a case registered in the VioGen system.

SERIAL CRIME DETECTION

By serial crime detection, we mean the activity aimed at determining which crimes were committed by the same person or by the same group of people. In response to this challenge, AI can analyse existing data to determine sets of crimes with similar modus operandi125.

In the case of Italy, the first predictive analysis software implemented in the country, KeyCrime, was developed in 2007 at the Milan Police Headquarters by the then State Police Assistant, Mario Venturi. This program integrates a big data computing activity that is capable of detecting serial crimes and predicting where, when and how the next criminal act might take place. In turn, it develops its premises based on four fundamental elements of each crime: its type, the objective, the modus operandi (including the objects, weapons and means of transport used) and the psychophysical characteristics of the perpetrator (including gestures, clothing, tattoos, piercings, scars or any visible object that might identify them). Thus, the analysis process has two different phases: the first is inductive, in which a specific crime is analysed in detail to identify the common elements with other crimes of similar characteristics and thus relate them to a single perpetrator; and the second is deductive, in which, after observing the key elements identified in the criminal series, it is possible to predict when, where and how the future crime will be committed, that is, the main "w" (where, when and how). KeyCrime would therefore enable more effective police protection. According to an audit, the application of the software in the Milan area has increased the probability of solving a serial crime by eight percentage points, reducing the number of robberies that criminal groups manage to commit before being arrested126.

In Spain, the Eurocop PredCrime127program has been developed. This project from the distant year of 2011 in collaboration with the Jaume I University of Castellón, is a system for predicting and preventing crime, the purpose of which is to create a risk forecast map for specific locations in a city and at specific times. It would be the "Spanish version of PredPol". In this case, the system does not mark grids, but heat maps with areas prone to the committal of a crime. The program has been tested by the Local Police of Castellón and Rivas-Vaciamadrid.

Within this type of application, we could highlight the use of this technique for the identification of serial killers by analysing data on solved and unsolved murders throughout a country or territory, the attribution of different illegal drug trafficking activities to the same criminal organisation or the detection and attribution of massive internet fraud campaigns with the same origin.

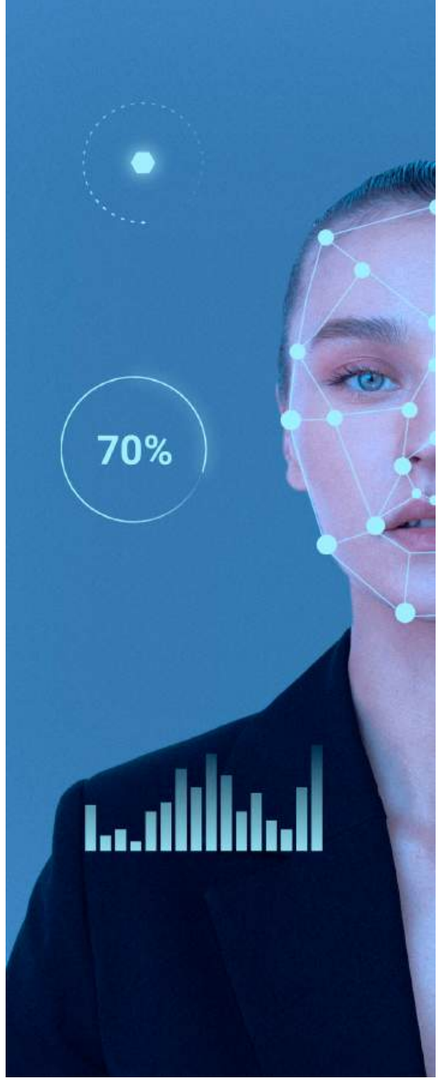
123 Abusamadov, K. (2024). Revolutionising Crime Prevention: The Role of AI and Big Data in Modern Law Enforcement. *Journal of law, market & innovation*, *I*(2), 21-25. https://doi.org/10.5281/zenodo.11928015

124 Varma Microsoft, P. (s. f.). *Transforming Law Enforcement Policies and Governance Procedures: The Benefits of AI Integration*. https://doi.org/10.5678/ijai.2020.12345

125 Garrett, B. L., Rudin, C., Williams, L. N., Beale, S. S., Benjamin, S., Boyle, J., Buccafusco, C., Dellinger, W., Fergusen, A., Griffin, L., Grunwald, B., Helfer, L., Kang, S., Lemos, M., Meltzer, A., Park, H., Purdy, J., Rai, A., Siegel, N., … Weiner, J. (2023). *The right to a glass box: Rethinking the use of artificial intelligence in criminal justice*.

126 VV.AA., HERRERA TRIGUERO, Francisco; PERALTA GUTIÉRREZ, Alfonso; TORRES LÓPEZ, Leopoldo Salvador. Chapter "Police use of artificial intelligence systems in the comparative field" p. 453 and following. Law and artificial intelligence. 2022. 24/10/2022 Editorial Universidad de Granada. 978-84-338-7049-0

127 https://www.eurocop.com/catedra-eurocop/proyectos-en-marcha/eurocop-pred-crime-sistemas-para-la-prediccion-y-prevencion-del-delito/#:~:text=El%20Proyecto%20Eurocop%20Pred%2DCrime,un%20crimen%20a%C3%BAn%20no%20producido.



FACIAL RECOGNITION

The use of AI applied to facial recognition techniques in the context of criminal investigation is one to which scientific literature most frequently refers128129. Automatic facial recognition is a technique that has been used for many years by investigators to, for example, identify people or anonymous suspects of a crime from an image of their face. Very powerful computer solutions are capable of detecting matches by comparing an anonymous image with thousands of other images of identified people, all in a matter of seconds. Generally, these capabilities have been limited by the need to have an anonymous image of a certain quality, which is not always possible. A limitation for these traditional solutions has also been firstly to have a database of quality identified images and secondly, high computing capacity. AI can certainly make these solutions more effective by allowing lower quality images to be compared, improving accuracy while reducing the number of false positives. AI does not suffer from fatigue like humans do, and certain ongoing developments are trying to make AI learn to identify faces just like humans would[130].

The Ministry of the Interior is training an algorithm for its new "automatic biometric identification system"[131] (ABIS). AI will help police identify suspected criminals. This system will only be activated in the event of serious crimes and is being developed by the French firm Thales.

The algorithm itself of this ABIS system is called Cogent and its operation is not an AI model that uses real-time and remote facial recognition AI to identify all citizens who walk in front of cameras in real time. Instead, it is "a scientific criminal system that allows the identification of persons detained or those who are accused of committing criminal offences based on prior information collected by legal obligation and the development of missions assigned to the State Security Forces and Corps." It is a computer program that the Spanish police will be able to apply to recordings and photographs of a possible crime scenario.

According to a written question in Congress[132], the tool aims to identify persons involved in actions carried out in criminal offences that make it necessary to apply the precautionary measure of detention or identification to transfer them to the judicial authority. To this end, the various recordings obtained

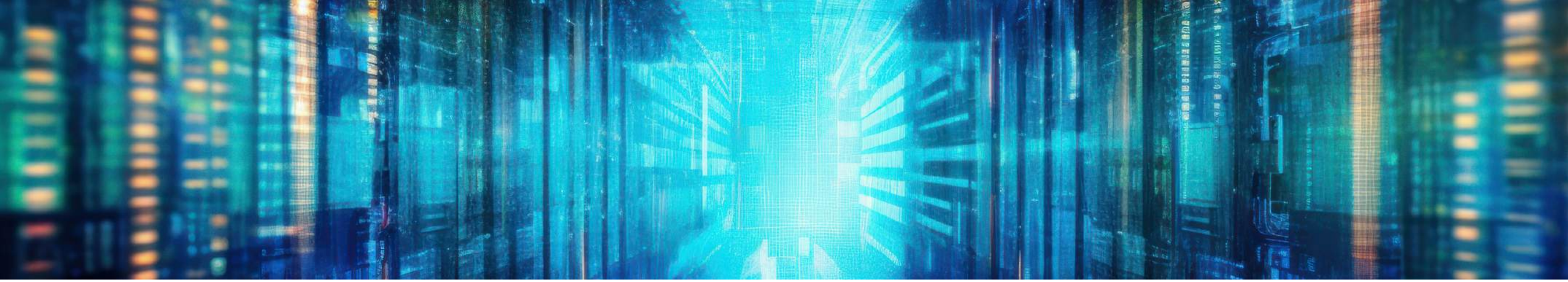
128 Same.

129 Kanwel, S., Imran Khan, M., & Usman, M. (2023). From Bytes to Bars: The Transformative Influence of Artificial Intelligence on Criminal Justice. *Qlantic Journal of Social Sciences*, *4*(4), 84-89. https://doi.org/10.55737/qjss.059046443

130 Same

131 AGUILAR, Alberto R. Interior acknowledges that it has not consulted the AEPD about the facial recognition algorithm that it is training for the police. Business Insider. 26 December 2022 Accessed 1 July 2023. Available at: https://www.businessinsider.es/interior-no-ha-consultado-aepd-antes-construir-ia-policial-1173474

132 Written question Congress 184/99831 10/01/2023 251055 AUTHOR: CORTÉS GÓMEZ, Ismael (GCUP-ECP-GC); SANTIAGO ROMERO, Enrique Fernando (GCUP-ECP-GC). Accessed 28 June 2023 and available at: https://www.congreso.es/entradap/l14p/e25/e_0255721_n_000.pdf



and processed by both public and private cameras that may have taken the image of the person responsible for the criminal offence will be used as a framework for consultation. The new ABIS FRS system performs an evaluation that consists of searching from an image (photograph or frame) taken during the committal of a criminal offence and comparing it with the undoubted images corresponding to the police record of detainees to determine the possible existence of one or more candidates. Once this result is obtained, facial recognition specialists will have to perform the same manual comparison process carried out to date on each image provided to confirm or discard the corresponding identification.

The Ministry of the Interior also maintains that the system allows the exercise of all data protection rights, that it complies with privacy regulations and that it has passed the proportionality test in relation to other means that can be or are being implemented (DNA, fingerprints, etc.).

In fact, the benefits to the party concerned are proven throughout the entire life cycle of the data, emphasising that automated decisions are not applied by the tool without human intervention and supervision.

As with all other rights of a person detained for committing an offence under the criminal code, when the system is used, it will be recorded in the corresponding proceedings and in the information provided to those involved.

Conservation and review periods are explained, which can last up to 20 years and in which the error rate or false negatives is 3%.

In other words, it is a high-risk system, the use of which is permitted a posteriori through judicial approval.

GUNSHOT DETECTION AND IDENTIFICATION

This application of AI would be based on the identification of patterns, for example, in an audio recording, in order to recognise a gunshot, and go further, trying to provide information on the type of weapon or ammunition used and even on the possible point of origin of the shot and its trajectory. These applications could even be embedded in smartphones or other portable devices that can assist officers on the ground in a situation **of firearms use.**[133] Of course, another application of this technique is forensic science, which would result from the post-processing of audio or video recordings of violent events in which firearms have been fired, such as in cases of murder or a terrorist attack.

Also, in relation to forensic ballistics, AI can be helpful in detecting patterns in the marks left by weapons on cartridges or projectiles, allowing forensic comparison processes to be automated and accelerated[134].

BIG DATA ANALYSIS

Criminal investigation, quite logically, has always relied significantly on data collection and analysis. In the case of forensic sciences, it also relies on filtering and evaluating the elements of interest collected for a case and comparing them with large amounts of data. In recent times, there have been disruptive advances in the development of these areas, all thanks to new techniques, typical of the digital age in which we live. Indeed, the data collected need to be analysed with the minimum possible effort, but with the maximum achievable precision. The vast amounts of data accessed in the context of investigations are enormous and growing[135], making data mining capabilities hitherto untapped in this domain a matter of urgency. In addition to all of the above, it is often necessary to add the enormous heterogeneity of the data with which it is necessary to work. An example of this is the case of electronic evidence obtained from the legal interception of the electronic communications of an individual under investigation, which may contain digital video or audio files together with texts and many other formats. In these cases, having AI-based data mining solutions that have computer vision or voice-to-text transcription capabilities, including translation into different languages, is a step forward with a huge impact on the investigators' work[136].

Specifically, police agencies are employing AI solutions of this nature, both for the detection of the preparatory stages of the committal of criminal acts and for the scrutiny and analysis of crimes already committed, including the identification of those responsible in both cases[137]. An example of this detection of preparatory phases of a crime could consist of the analysis of large amounts of banking and tax data to detect complex tax operations aimed at committing large-scale fraud. Another example is their possible use for the real-time analysis of large amounts of data from an organisation's electronic communications network, for the preventive detection of possible TTP[138] used by cybercriminals to perpetrate an attack or intrusion into the network.

For example, IBM Security i2 Analyst's Notebook is an IBM software product used for data analysis and investigation. It is a software tool based on the ELP (entity-relationship-property) methodology, which offers the user the possibility of knowing the relationships between data entities to discover

133 Singh Sankhla, M., Kumar, R., & Jadhav, E. B. (2020). Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation. *Seybold Report*, *15*(8). https://www.researchgate.net/publication/343826071

134 Same

135 An example of this is the large amount of digital information that can be stored on a single smartphone or the information resulting from the interception of electronic communications of a fibre optic line.

136 Simmler, M., Brunner, S., Canova, G., & Schedler, K. (2023). Smart criminal justice: exploring the use of algorithms in the Swiss criminal justice system. *Artificial Intelligence and Law*, *31*(2), 213-237. https://doi.org/10.1007/s10506-022-09310-1

137 Kanwel, S., Imran Khan, M., & Usman, M. (2023). From Bytes to Bars: The Transformative Influence of Artificial Intelligence on Criminal Justice. *Qlantic Journal of Social Sciences*, *4*(4), 84-89. https://doi.org/10.55737/qjss.059046443

138 Techniques, Tactics and Procedures.

patterns and information in the data. Analyst's Notebook is a tool commonly used for digital analysts in law enforcement, the military, and other government intelligence agencies, or in fraud departments of financial institutions, regulatory agencies, etc. It is part of the Human Terrain System (HTS), a US Army program that integrates social scientists with combat brigades.

Similarly, within the COPKIT project, in its data extraction phase we find the development of Named Entity Recognition – CKNER, a tool developed by the Austrian Institute of Technology (AIT). A service that integrates several state-of-the-art named entity recognisers, each with standard and domain-specific models trained on generic corpora, focusing on text data acquired through crawling darknet markets offering weapons and drugs, centring on short and poorly written texts.

And for example, in family criminal organisations, Relationship Extraction – CKRELEXT, a tool developed by the Austrian Institute of Technology (AIT), can be very useful within the same project. The REST Service for recognising relationships between entities (drugs, weapons, usernames, locations, etc.). It takes a text (for example, one or more paragraphs of text taken from a darknet marketplace advertisement) as input and produces a named entity graph as output. The component depends on entities recognised by CKNER.

From the same project in the same regard, the Connection Finder – CF, a tool developed by Legind Technologies (LTA), finds connections in graphs of entities (e.g. not limited to "people" or identities, but also heterogeneous) with uncertain links. It can be used in on-line investigations (including the dark web) to find relationships between various elements of digital identities (e.g. usernames, digital currency wallets, etc.), in relation to internal intelligence bases if available (and if possible graph fusion).

Regarding social networks, Haternet[139] identifies and monitors the evolution of hate speech on Twitter (currently X), visualising it using network analysis techniques, introduces a database on hate speech in Spanish, consisting of 6000 tagged tweets, and compares the classification by displaying its status and evolution.

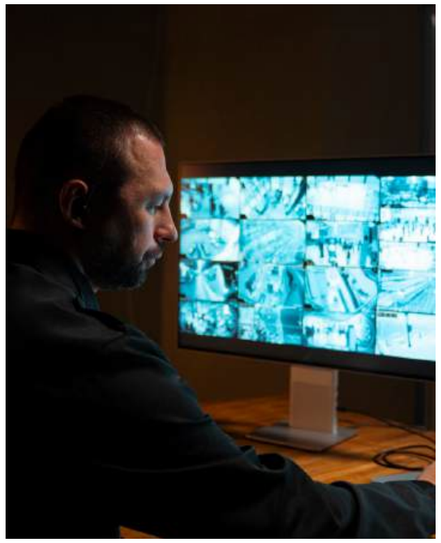
Indeed, the analysis of big data is essential to detect patterns and anomalies that could indicate potential cybersecurity breaches or fraudulent activities. By monitoring data traffic in real time, cybersecurity teams equipped with these AI capabilities can identify unusual patterns that characterise a cyberattack in its preparatory stages, such as unusual login attempts, spikes in data access requests, or anomalies in financial transactions[140].

139 Pereira-Kohatsu JC, Quijano-Sánchez L, Liberatore F, Camacho-Collados M. Detecting and Monitoring Hate Speech in Twitter. Sensors (Basel, Switzerland). 2019 Oct;19(21):E4654. DOI: 10.3390/s19214654. PMID: 31717760; PMCID: PMC6864473.

140 Abusamadov, K. (2024). Revolutionising Crime Prevention: The Role of AI and Big Data in Modern Law Enforcement. *Journal of law, market & innovation*, *I*(2), 21-25. https://doi.org/10.5281/zenodo.11928015

INVESTIGATIONS DEPARTMENT

Today, the execution of most criminal investigations requires investigators to handle massive amounts of data, which can often be heterogeneous and unstructured. We have seen that DL is especially effective when it comes to learning, processing and analysing unstructured data, so this technology and AI applications based on it can be of special interest in assisting investigators in decision-making. Solutions equipped with this type of machine learning, based on deep neural networks, can improve the analysis, organisation and management of a case, leading to decisions and recommendations on the case and on legal matters related to it[141].



ADVANCED COVERT SURVEILLANCE

The possibility of exploiting AI models and algorithms already trained for a multitude of tasks, some of which have already been mentioned, in real time, and with practically no latency perceptible to humans, is an indisputable reality. This immediacy expands a universe of new AI capabilities to investigative intelligence-gathering activities based on covert surveillance of those under investigation and their illicit activities. Physical and electronic surveillance operations carried out during investigations by IC agency officials can now benefit from capabilities only very recently suspected. For example, machine vision capabilities enable automatic real-time analysis of images obtained through covert imaging means, allowing patterns to be detected immediately, predicting potentially criminal activities before they occur and thus facilitating timely intervention or accurate and timely decision-making during surveillance. Indeed, computer vision can detect subtle indicators in the behaviour of subjects that are relevant to making any decision[142].

FORENSIC COMPARISON OF EVIDENCE

AI applied to forensic science has been used in judicial processes in the context of complex DNA mixtures. In cases of DNA mixtures from multiple, and sometimes anonymous, donors, AI algorithms have been designed to determine whether or not a subject may have contributed to a sample taken at a crime scene[143] [144] [145].

In the field of lophoscopy, AI also has something to add. DL has had considerable success in the field of computer vision and pattern recognition, since it makes human intervention unnecessary for the identification of characteristics of any sample. DL automatically learns to do these tasks by training with sufficient data provided to it. These advantages of AI make it especially attractive for improving the efficiency of the execution of various tasks related to the automatic identification and classification of fingerprints. This technology can substantially reduce the number of comparisons required to achieve a positive match, while adding accuracy[146].

141 Faqir, R. S. A. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. *International Journal of Cyber Criminology*, *17*(2), 77-94. https://doi.org/10.5281/zenodo.4766706

142 same.

143 Singh Sankhla, M., Kumar, R., & Jadhav, E. B. (2020). Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation. *Seybold Report*, *15*(8). https://www.researchgate.net/publication/343826071

144 Garrett, B. L., Rudin, C., Williams, L. N., Beale, S. S., Benjamin, S., Boyle, J., Buccafusco, C., Dellinger, W., Fergusen, A., Griffin, L., Grunwald, B., Helfer, L., Kang, S., Lemos, M., Meltzer, A., Park, H., Purdy, J., Rai, A., Siegel, N., … Weiner, J. (2023). *The right to a glass box: Rethinking the use of artificial intelligence in criminal justice*.

145 Kanwel, S., Imran Khan, M., & Usman, M. (2023). From Bytes to Bars: The Transformative Influence of Artificial Intelligence on Criminal Justice. *Qlantic Journal of Social Sciences*, *4*(4), 84-89. https://doi.org/10.55737/qjss.059046443

146 Singh Sankhla, M., Kumar, R., & Jadhav, E. B. (2020). Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation. *Seybold Report*, *15*(8). https://www.researchgate.net/publication/343826071

These techniques can also be applied in the field of graphics, which in some cases help to determine the sex of the author of a handwritten text. Other forensic areas of interest for the application of AI are ballistics, dating of death by blood analysis or dental identification[147].

Researchers from the DaSCI Institute (University of Granada) and the CITIC centre (University of A Coruña), in collaboration with the company Panacea Coop, have published a study that shows an improvement in the recognition of human remains by craniofacial superimposition, making decision-making by forensic experts much more objective.

Craniofacial superimposition is a forensic technique that supports decision-making when it comes to identifying bone remains. Specifically, it is based on the analysis of the superimposition of a found and unidentified skull (post mortem) on facial photographs (ante mortem) of missing persons[148].

DIGITAL FORENSICS

Forensic analysis of digital evidence is currently a daunting challenge for investigators. As already mentioned in previous sections, the amounts of digital data obtained from those investigated, from records on their electronic devices, can be enormous. In addition to the problem of quantity, there is also the problem of complexity, since the heterogeneity of the data and the encryption solutions that are commonly used by electronic devices, often in a way that is transparent to those under investigation, make it extremely difficult to interpret the information. AI solutions in this field focus on automating the analysis and correlation of data acquired during investigation and, based on their learning, presenting the investigator with the information that is of interest. These systems thus reduce the amount of data that investigators must personally analyse, and provide the subset of the total evidence that is most likely to constitute information of interest to the investigation.

Another branch of digital forensics is computer network forensics. Generally, the purpose of these analyses is to study network activity to detect the origin of network security policy violations or information security breaches[149].

Other Spanish artificial intelligence applications should also be mentioned, such as, firstly, 4nseek.es[150], which is a tool intended for security forces and bodies. Its purpose is to help officers combat child sexual abuse. It analyses the content of disks or partitions and, through different artificial intelligence techniques, is able to detect the appearance of signs of sexual abuse of minors in images or videos, offering the user a prioritised list of results.

Added to all of the above is the challenge posed by the use of AI for disruptive criminal purposes by criminals, unsuspected until the emergence of this new technology. Add to this the complexity of gathering cross-border evidence to conduct national investigations when an AI system has been involved in the committal or perpetration of unlawful conduct, and the difficulty for investigators increases exponentially[151].

147 same.

148 Práxedes Martínez-Moreno, Andrea Valsecchi, Pablo Mesejo, Óscar Ibañez, Sergio Damas. Evidence evaluation in craniofacial superimposition using likelihood ratios. Information Fusion (2024). https://doi.org/10.1016/j.inffus.2024.102489

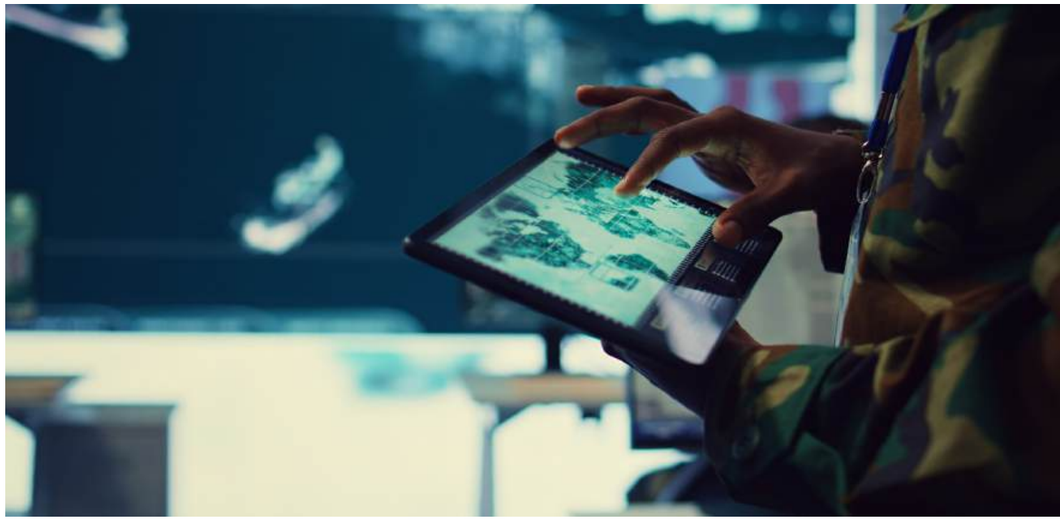
149 same.

150 https://www.incibe.es/incibe/informacion-corporativa/con-quien-trabajamos/proyectos europeos/4nseek/herramienta

CRIME SCENE RECONSTRUCTION AND VIRTUAL REALITY

The combined application of 3D digital technologies and AI can be used to improve the execution of certain phases of forensic visualisation techniques. This combination of technologies can create 3D graphical models of objects and people, based on measurements and images, and animate these models to recreate crime scenes and related events. An example of this technique is the use of visual pattern recognition to analyse the size, shape and distribution of blood stains, all with the aforementioned aim of reconstructing the events that occurred[152].

The VALCRI (Visual Analytics for Sense-Making in Criminal Intelligence Analysis) project allows crime scenes to be analysed by scanning millions of information sources in different formats in seconds (European Commission, 2018; Gallego, 2018): records, victims, images, crime scenes, interrogations, etc. It detects all suspicious patterns and is capable of reconstructing scenes and presenting them on interactive touch screens, to compare with previous data. It also combines artificial intelligence and visual analysis, using facial recognition software to detect and identify specific people from sources. This system seeks to recognise those details that humans can overlook. The project is funded by the European Commission and involves the West Midlands Police (United Kingdom) and Antwerp Police (Belgium) and is coordinated by Middlesex University[153] [154].



151 Faqir, R. S. A. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. *International Journal of Cyber Criminology*, *17*(2), 77-94. https://doi.org/10.5281/zenodo.4766706

152 Singh Sankhla, M., Kumar, R., & Jadhav, E. B. (2020). Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation. *Seybold Report*, *15*(8). https://www.researchgate.net/publication/343826071

153 GALLEGO, Paloma. Artificial intelligence for unsolved crimes? In: Big Data Magazine. 30 May 2018 Available at: https://bigdatamagazine.es/inteligencia-artificial-para-casosde-crimenes-sin-resolver.

154 European Commission. Visual analytics for brighter criminal intelligence analysis. In: Cordis. 7 February 2018.

PROJECTS AND INITIATIVES TO STRENGTHEN SECURITY COOPERATION AND CRIMINAL INVESTIGATIONS

The **TRACE Project funded by the European Union's Horizon**[155] research and innovation programme is made up of a broad consortium of organisations whose ultimate aim is to provide European law enforcement authorities with the tools and resources to identify, track, document and dismantle illicit money flows in a timely and effective manner in six areas: (i) terrorist financing, (ii) web forensics, (iii) cyber extortion, (iv) use of cryptocurrencies in real estate market transactions, (v) money laundering in art and antiques, and (vi) on-line gambling. The project includes developing AI tools for analysing and visualising financial data, identifying patterns of suspicious financial activity and collaborating with other agencies to share information. The project includes eleven components, including one on ethical, legal and social impact aspects[156].

The ***iBorderCtrl*** project is an initiative funded by the European Union to improve border control through the use of advanced technologies, including facial recognition and a risk assessment system. It started in 2016 and ended in 2019, with tests in Greece, Hungary and Latvia. Its main objective is to speed up border crossings for third-country travellers, using a pre-registration system and biometric technologies, such as facial and palm vein scanning, to verify travellers' identities before they reach the border.

Despite the interest it generated, one of the most controversial elements of the project was an AI-powered lie detector, which assesses travellers' facial expressions during a virtual interview to determine whether they are lying about the purpose of their travel or length of stay. If the system detects irregularities, additional checks are carried out by human agents. Despite its innovativeness, the system has been criticised for ethical and reliability issues, such as its potential discrimination against people with disabilities or anxiety, and concerns about the invasion of fundamental rights. And recently, in 2023, the Court of Justice of the European Union ruled in favour of transparency, allowing some documents related to the project to be accessible to the public, while maintaining the protection of certain commercial interests of the consortium that developed it.

The Spanish Civil Guard has adopted a system called **ATLAS**, an AI-based tool that allows for the analysis of large volumes of information obtained from seized electronic devices, such as mobile phones and computers. ATLAS uses data mining and machine learning techniques to identify hidden evidence and link communications between suspects, which is particularly useful in cases of organised crime and drugs trafficking. Furthermore, the Spanish National Police Force has developed Centinela, which applies artificial intelligence algorithms to detect links between different criminal organisations, both nationally and internationally. Centinela is especially effective in the fight against drugs trafficking and human trafficking.

155 The TRACE Project at: https://trace-illicit-money-flows.eu/

156 The 11 components of the project are described at: https://trace-illicit-money-flows.eu/project-outcomes/

4.3. AI TOOLS FOR SPECIFIC TOPICS OR AREAS

ANALYSIS AND EVALUATION OF EVIDENCE

In the field of analysis and evaluation of evidence, the following projects and initiatives can be highlighted from both the judicial and police spheres.

- **AVENUE** (Analysis of Video Evidence with Novel Enhanced Understanding Engine). This project, funded by the European Commission under the Horizon 2020 programme, uses AI for advanced analysis of video evidence, which is increasingly common in criminal investigations. AVENUE applies computer vision and object recognition algorithms to automate the reviewing of large amounts of security camera or mobile phone recordings, helping to identify suspects and behaviours relevant to the case. It is used in investigations of serious crimes, such as terrorism and organised crime, where video evidence is key.

- **TENSOR** (Retrieval and analysis of heterogeneous data for predicting and mitigating violent actions). TENSOR is an AI project also developed within the framework of Horizon 2020, which aims to detect and analyse evidence obtained on-line related to terrorist activities or organised crime. This tool can analyse a mixture of digital evidence, such as social media posts, videos or emails, identifying patterns of radicalisation or potential violent threats. TENSOR AI analyses semi-structured and unstructured data, enabling rapid threat identification in real-time.

- **COPKIT.** Likewise, it is worth mentioning the COPKIT project, which has focused on the problem of analysing, investigating, mitigating and preventing the use of new information and communication technologies by organised crime and terrorist groups. COPKIT proposes an intelligence-based early warning (EW) and early action (EA) system, both at the strategic and operational levels. According to its function, each component developed during the project is described in one of the six phases of the COPKIT early warning/early action ecosystem: data collection, information extraction, information enrichment, knowledge discovery, assessment and forecasting. The project lasted 40 months (from 2018 to 2021). It is coordinated by Isdefe, a public company owned by the Spanish Ministry of Defence. The consortium is made up of 18 partners from 13 countries with different profiles and experience in various fields, including public security agencies, industry, academia, and research and technology organisations. Furthermore, the COPKIT project gives a key role to the "End-Users and Stakeholders Advisory Board" (EUSAB). This external and independent board is led by EUROPOL and includes end-users and experts from different fields who advise the consortium on the practical implementation of the project objectives, as well as on issues related to its direction, progress, results and deliverables.[157]

- **ROXANNE** (Real-time network, text, and speech analytics for combating organised crime and terrorism). This project, which is also part of the Horizon 2020 programme, integrates AI to analyse social media data, texts and audio evidence obtained in criminal investigations. ROXANNE uses voice recognition and natural language processing (NLP) technologies to identify communication networks between suspected organised crime or terrorism suspects. It also provides a collaborative platform for sharing evidence and analysis between police and judicial agencies from different countries of the European Union.

157 https://copkit.eu/

- **iCOP** (Identifying and Catching On-line Predators). Developed to combat on-line child sexual abuse, this AI project analyses large volumes of data obtained from investigations into child sexual exploitation. The iCOP tool uses AI algorithms to identify suspicious behaviour patterns in file-sharing networks and on-line communities. iCOP can scan media files for illegal content and provide key evidence in criminal investigations into such crimes.

- Moreover, in 2018, a tool was developed that was able to detect which reports were false in cases of robbery with violence and intimidation or snatching[158]: **Veripol**. It is based on an algorithm and a mathematical model which, through artificial intelligence and natural language processing, is able to locate the words that alleged victims use most when they lie when reporting crimes. According to the study by its creators, among them Miguel Camacho, police inspector and current coordinator of Technological Innovation and Cybersecurity of the State Council, its success when determining which complaints are false is 91%, a figure much higher than the 75% obtained by an expert police officer.

AI-ASSISTED DECISION-MAKING AND JUDICIAL RESOLUTIONS

In this section it is worth highlighting the **JuLIA (Justice, fundamental rights and Artificial Intelligence Applications)** project, which is an EU-funded initiative that focuses on providing AI training to European judges, specifically in relation to fundamental rights and automated decision-making (ADM). The project aims to improve understanding of the effects of AI on judicial systems and its impact on fundamental rights, such as the right to a fair trial and protection against discrimination.

JuLIA offers on-line and in-person courses, including transnational workshops for judges, with the aim of training them in the use of AI tools within the European legal framework. The project also includes the creation of a "Casebook" on the limits of algorithmic government, focused on the use of AI in the public administration. This training aims to ensure that judges are equipped to face the challenges that AI presents to the protection of fundamental rights and the judicial process.

It involves several institutions, including the Faculty of Law of the University of Groningen, together with six other international partners, and follows the previous work of the **FRICoRe** (Fundamental Rights in Courts and Regulation) project, which ended in 2022. However, this project is currently in the implementation phase and a transnational workshop is planned for 2024.

158 Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M. (2018). Automatically applying misleading language detection to police reports: extracting behavioural patterns from a multi-step classification model to understand how we lie to the police. Knowledge-Based Systems, 149, 155-168.

MONITORING THE EXECUTION OF SENTENCES IMPOSED IN A RULING

AI has begun to play an important role in monitoring and following up on the enforcement of sentences imposed by criminal courts in several countries of the European Union, although its implementation varies depending on the level of technological adoption of each member state and its judicial systems. AI not only improves efficiency in case management, but also provides tools for more accurate and effective enforcement of sentences, particularly in relation to parole, alternative measures to imprisonment, and the monitoring of repeat offenders.

One of the key aspects where it has proven useful is in the supervision and management of alternative measures to imprisonment, such as conditional release, house arrest or permanent localisation with electronic devices and other sanctions that allow the social reintegration of offenders without resorting to their incarceration. This is the case in the Netherlands, where AI algorithms help predict the likelihood of repeat offences or failure to comply with established conditions by analysing previous behaviour patterns. In this way, they improve interoperability between different agencies and allow for more effective control over the behaviour of convicts on parole, based on historical data and socio-demographic or contextual variables that offer a more detailed view of the risk posed by each convict. For its part, its prison system has integrated AI technologies to monitor and analyse inmate behaviour in real time through wearable devices and surveillance systems. These data are analysed using algorithms that detect anomalous behaviour patterns that could indicate a risk of flight or violence. Advances in predictive analytics enable authorities to intervene before incidents occur.

In Spain they have the **VioGén System** (Comprehensive Monitoring System in cases of Gender Violence), which is a tool developed by the Spanish Ministry of the Interior to improve the monitoring and protection of victims of gender violence. Created in 2007, this system integrates information on victims and aggressors, allowing for a constant assessment of risks and better coordination between the authorities responsible for protecting and enforcing the measures and penalties imposed.

The system sends automatic alerts when risk situations are detected or when the aggressor violates precautionary measures or sentences imposed by the court, such as restraining orders or prohibitions on communication with victims. The system allows security forces to receive real-time alerts about possible breaches. This allows security forces to act proactively, protecting the victim before a violent incident occurs. Coordination between local police forces, the National Police, the Civil Guard and other authorities is essential in this regard.

VioGén has been used in more than 800,000 cases since its creation, and according to the Ministry of the Interior, in more than 90% of the cases in which an extreme or high risk alert has been activated, a new violent episode has been avoided. The platform is constantly evolving, incorporating improvements based on user experiences and technological advances, such as the use of big data and machine learning to improve risk assessment accuracy. VioGén has been so successful that other countries have shown interest in developing similar systems, and the European Union has highlighted the Spanish model as an example of good practice in the fight against gender violence and monitoring of compliance with sentences and protective measures. However, it is important to take into account key elements of transparency and applicability when developing applications or systems such as VioGén and RisCanvi.

Eurojust, the EU's judicial cooperation agency, is also developing AI technologies to improve cross-border cooperation in the implementation and monitoring of criminal judgments, facilitating interoperability between different judicial systems. These technologies are helping to ensure that sentences imposed in one member country are duly enforced or recognised in another, reducing response time and improving efficiency in the administration of criminal justice in the region.

4.4. AI TOOLS USED IN LATIN AMERICAN AND CARIBBEAN COUNTRIES

Below are some AI tools that are currently used or have been used in some countries in the region. It is important to mention that the list of tools or systems developed may be incomplete both in the areas of security and justice, as well as in the countries that have them.

ARGENTINA

PROMETEA is an AI system developed with the purpose of improving efficiency and automation in judicial and administrative decision-making. It was created by the Public Prosecutor's Office of the Autonomous City of Buenos Aires and the Innovation and Artificial Intelligence Laboratory of the Faculty of Law of the University of Buenos Aires[159]. Among the main benefits of PROMETEA are:

- Ability to automate the drafting of judicial and administrative documents, such as opinions, resolutions and sentences, with great speed and precision.
- Understanding and processing complex regulatory and judicial texts, extracting relevant information to issue a recommendation or draft a resolution.
- It helps classify, prioritise and manage large volumes of cases, identifying those that require urgent attention or that can be quickly resolved through automated procedures.
- It ensures that each decision or recommendation generated by the system is explainable.

BRAZIL

VICTOR: This is an AI tool used by the Federal Supreme Court of Brazil that analyses and classifies the appeals filed before said court and has the ability to predict whether the requested appeal will have a broad social impact and relevance so that it might deserve to be submitted to the study and analysis by the Magistrates that make up the court. The project was named as a tribute to Victor Nunes Leal, a Brazilian Magistrate responsible for systematising the jurisprudence of the TSF and facilitating the application of judicial precedents applicable to appeal trials in Brazil[160].

159 IDB, "PROMETEA, Transforming the administration of justice with artificial intelligence tools" at: https://publications.iadb.org/es/publications/spanish/viewer/PROMETEA-Transformando-la-administracion-de-justicia-con-herramientas-de-inteligencia-artificial.pdf

160 Habib Lantyer, Victor, "The Era of Artificial Intelligence in Law: Brazil in a Global Context " (1 December 2023), p.10, available at SSRN: https://ssrn.com/abstract=4650117

Apoia MPF: System based on Generative Artificial Intelligence designed to help analyse extrajudicial and judicial procedures. By intelligently extracting information from the files, the system classifies the data into specific typologies according to class and object, suggesting a draft according to the case. The system also provides complementary information catalogued as important to aid decision making (background information published by the Federal Revenue Secretariat in the name of the accused and factual news information deposited at the Federal Public Prosecutor's Office (MPF) in Brazil.

Transcreve AI: Audio and video transcription solution to meet the needs of members of various areas of the MPF. Used to transcribe court hearings, extrajudicial hearings, meetings and other activities requiring recording.

MPFMed: Solution that extracts the full text of court procedural documents (initial petition, MPF opinion and court decision) and extrajudicial procedures (order, recommendation, file promotion, PA/IC/PP ordinance, other documents, electronic protocol, electronic petition) information on diseases, medicines, medical treatments and supplies. The results are presented in statistical panels that assist in research, decision making and evaluation of claims, including the proposal of structural ways to address recurrent problems, through recurrent problems through specific actions.

Automatic alerts on personnel management acts: Emails are sent to members and officials with automatic alerts on personnel management acts, such as appointments and terminations. The service uses artificial intelligence (AI) to identify publications of interest in the Official Journal of the European Union (OJEU), the Electronic Journal of the MPF (DMPF-e) and the Bulletin of the Federal Public Prosecutor's Office (BSMPU).

Automation of requests for STJ court cases: Use of AI to automate the requisitioning of High Court of Justice (STJ) cases of interest to the MPF, due to the mandatory intervention provided for in the Federal Constitution and legal norms. On a daily basis, the Electronic Gazette of Justice (DJe) carries an average of 4.5 thousand STJ publications, the IA identifies cases of interest and indicates them for request. These requests for cases correspond to more than 75% of the manifestations made by the offices of the MPF acting in the STJ.

TRIA Único: Artificial Intelligence solution integrated in the Unico system to reduce the time of habeas corpus received in the offices. The sense of the judicial decision and the opinion of the MPF, inferred from the full text of the Habeas Corpus cases, are categorised into "Favourable" or "Unfavourable" to the MPF, "Decisions on the MPF, 'Decisions on precautionary measures" and "Decisions without opinion of the MPF". This categorisation is obtained by analysing the admissibility and merits of the MPF's opinions and the decisions of the High Court of Justice (STJ). This allows the Deputy Prosecutor to prioritise his or her actions in judicial proceedings.

IPL/TCOs: Application of artificial intelligence to the totality of the Police Proceedings and Terms of Detention in conjunction with metadata extraction to perform classification according to the following types of inference: "Time limit", "Reported", "Quota met"

and “Other”, indicating the IPL/TCO page where the AI found the information. Information. Displays information extracted from the metadata: amount of time (year/month/day) since the case was filed; number of times it has been filed with the MPF; time (year/month/day) elapsed since the last exit; statute of limitations (if it has been registered); and the number of times the case has been filed with the MPF.

Trial outcomes in criminal cases: use of generative Artificial Intelligence in conjunction with classical AI techniques to infer outcome information (Criminal Type, Sentence, Sentencing Regime, Fine, Sentencing Date and Judge) of defendants in criminal cases, with defendants in criminal cases, with easy access to the full sentence. Automated The automated extraction of this information streamlines the work of member offices.

Simba and Sittel: Simba is a system for receiving banking and financial data from financial institutions. The system receives data in a standardised and structured format, as well as files in various formats, enabling descriptive and analytical reports to be issued. It is a system distributed to about a hundred public bodies (used by all police forces and prosecutors’ offices and various courts of auditors and judicial bodies). Sittel has similar characteristics, as it receives telephone data, registration data and ERB (radio base station) information in a structured and standardised way.

Analysis MPF: System integrating several solutions for the management of investigations and the analysis of banking and telephone data and financial intelligence reports. The system consists of a BI solution (Apache Superset) and an integrated link analysis solution (Neo4J and Cytoscape). A web-based digital trace capture solution (E-Capture) has been integrated, with issuance of a certificate to ensure chain of custody. Solutions are being developed for the extraction of entities and other information from financial intelligence reports using natural language (initial testing with Llama 3.1) and a solution for the indexing and analysis of unstructured data derived from confidentiality breaches and electronic device extractions.

Sisconta Eleitoral: Sisconta Eleitoral is a system developed by the Federal Public Prosecutor’s Office to optimise the analysis and cross-referencing of data relevant to the work of members of the Electoral Public Prosecutor’s Office, with access available to electoral prosecutors throughout Brazil. It is composed of a Dirty Dossiers Module, which facilitates the analysis of ineligible candidates, and a Dirty Accounts Module, with information on campaign finances and any indications of irregularities in the electoral campaign, based on a systemic analysis of data from the various databases available.

Georadar: System that aggregates geo-referenced databases, allowing the simultaneous cross-referencing of hundreds of layers, the consultation of literal data associated with them, the construction of maps and the issuance of reports directly by members and officials of the Federal Public Prosecutor’s Office. Data integration is carried out through ETL processes and geo-services.

ID Mask: Personal data anonymisation system, focused on legal texts, using Artificial Intelligence techniques based on Named Entity Recognition (NER). Developed to comply with personal data protection legislation in the Federal Public Prosecutor’s Office, the system performs the automated concealment of personal data in documents, preserving their usefulness and integrity for purposes of sharing with third parties and public disclosure.

CHILE

In the area of crime prediction, the Urban Crime Predictive System stands out, which was developed in 2017 by the University of Chile together with the Criminal Analysis Department of Carabineros de Chile, the objective of which is to predict areas at greater risk of crime occurrence in order to carry out targeted patrols and reinforce the effectiveness of the criminal prosecution system[161].

The Chilean Public Prosecutor’s Office has developed several tools based on artificial intelligence to respond to specific challenges in different work processes. The models available and under development seek to optimise the analysis of large volumes of information, improve the classification and linking of complaints, and strengthen the early detection of risks in cases of domestic violence. Specifically, the existing solutions correspond to Fiscal HeredIA (Prosecutor HeredIA), the Intelligent Preclassifier and the Risk Suggestion Algorithm.

Fiscal HeredIA is an ecosystem of tools for criminal analysis, developed since 2020 in collaboration with actors from the academic world. This ecosystem streamlines the processing of large volumes of data through specialised modules that interact with internal databases and relevant documents from criminal investigations.

The Intelligent Preclassifier is also based on artificial intelligence, a tool that allows the automatic reading of the reports that enter the system, identifying relevant elements in the stories and also summarising the facts and suggesting a preliminary classification of the cases, with the aim of suggesting possible courses of action to the institution’s officials.

Finally, the Risk Suggestion Algorithm was designed to generate alerts to the possibility of victims of domestic violence suffering new episodes of aggression. For this purpose, it integrates sources of information from complaints, background information on victims and aggressors, allowing alerts to be issued to the teams in charge of adopting protection measures for victims and improving their capacity to respond to acts of violence.

Fiscal HeredIA®: Fiscal HeredIA® is a technological tool based on artificial intelligence whose purpose is to contribute to the strengthening of criminal analysis and investigation in the Chilean Public Prosecutor’s Office. To this end, it integrates different models that allow to analyse and exploit information efficiently and effectively, facilitating the identification of criminal structures, especially in the

161 Fair Trials, “Artificial intelligence in public security and the criminal justice system in Latin America. Analysis based on due process”, December 2024, p.17, available at: https://www.fairtrials.org/app/uploads/2024/08/Inteligencia-artificial-en-la-seguridad-publica-y-en-el-sistema-penal-en-America-Latina.pdf

context of complex crimes and organised crime. The tool is conceived as an ecosystem as it integrates multiple modules with specific functionalities, designed to respond to different investigative needs.

Its development began in 2020 as part of an applied research project funded by the National Research and Development Agency's (ANID) Scientific and Technological Development Fund (FONDEF), in collaboration between the Public Prosecutor's Office and the universities of Chile, Biobío and Los Andes.

The tool incorporates different analysis modules, which allow to:

- Identifying criminal gangs
- Analysing documents via a chat interface
- Linking information contained in investigative files
- Process audio files allowing for transcription, translation and analysis

These modules have been developed using mathematical models from the field of optimisation, as well as advanced techniques in Natural Language Processing (NLP).

The Fiscal HeredIA® ecosystem is currently being deployed nationwide, collaborating with investigations into different criminal phenomena.

COLOMBIA

PRETORIA is an AI system that supports and optimises the selection, analysis and structuring process of tutela (constitutional action to protect fundamental rights) rulings of the Constitutional Court of Colombia. It was developed jointly by the Innovation and Artificial Intelligence Laboratory of the University of Buenos Aires, the Universidad del Rosario and other public and private institutions in Colombia in 2020[162].

This system carries out the selection, analysis and structuring of the protection rulings for review by the Constitutional Court through three functions:

- (i) Search. It allows information of interest to be identified for the selection of sentences;
- (ii) Categorisation. It allows to information to be categorised and selected according to criteria relevant to the Constitutional Court; and
- (iii) Statistics. It allows the creation of time lines and graphs that help provide a more complete and comprehensive view of tutela.

162 Constitutional Court of the Republic of Colombia, "PRETORIA, the Constitutional Court's smart system to support the selection of *tutelas*, is awarded as the best tool for modernisation in the field of justice by the CEJ" Bulletin No. 187, Bogota, 15 December 2020, at: https://www.corteconstitucional.gov.co/noticia.php?PRETORIA,-sistema-inteligente-de-la-Corte-Constitucional-para-apoyar-la-selecci%C3%B3n-de-tutelas,-es-premiada-como-mejor-herramienta-de-modernizaci%C3%B3n-en-materia-de-justicia-por-la-CEJ-9031

PRISMA (Recidivism Risk Profile for Requesting Security Measures). It is an AI tool used to predict the risk of recidivism based on the profile of the person under investigation, which aims to support the work of prosecutors and judges to determine a preventive measure, such as the detention of an individual who is being investigated by the Colombian authorities. The tool can show the predicted risk of criminal recidivism that the person under investigation may have during the criminal procedure. This tool seeks to optimise the management of prison quotas and supports criminal judges by displaying information on people with a higher probability of criminal recidivism [163].

The OECD reports on an AI tool related to the prediction of sentences in lawsuits against the State in Colombia developed by the National Agency for Legal Defence of the State (ANDJE) and Quantil, a private company, which consists of a mathematical tool to estimate the probability of an unfavourable sentence in a litigation process against the nation, and to recommend the optimal amount of a settlement based on current case conditions. According to the OECD, the predictive component of the model is based on machine learning techniques, while the optimisation of the settlement arrangement is based on financial and game theory fundamentals[164].

In the area of surveillance and citizen protection, the OECD reports that in the LAC region, greater experimental use is being made of AI to analyse images of faces along with other videos, pictures and audio in order to detect criminal activities and identify offenders, and refers to the cases of the Command, Control, Communications and Computing Centre (C4) in Bogotá, Colombia, and the ECU 911 in Ecuador[165].

TALION was a prototype of a fuzzy logic expert system for determining punishment according to the criteria and parameters established by law and was presented in 2009 in a competition of the Ministry of Information and Communication Technologies of Colombia[166]

COSTA RICA

In March 2024, the Judiciary, through the Data Protection Commission, implemented an AI tool that allows documents to be depersonalised in order to protect the sensitive information contained in the sentences found in the Nexus PJ. system, which is used by the Judicial Branch of Costa Rica to protect the rights of users in accordance with Law No. 8968 on the Protection of Persons

163 For an explanation and examples of the PRISMA System, see: Attorney General's Office. Public Policy and Strategy Directorate. "PRISMA Tool: Recidivism Risk Profile for Requesting Security Measures" at: https://www.fiscalia.gov.co/colombia/wp-content/uploads/Perfil-de-riesgo-de-reincidencia-para-solicitudes-de-medida-de-aseguramiento.pdf

164 OECD/CAF, "Practical Cases of the Use of AI in Governments in Latin America and the Caribbean" in Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean, p.41, at: https://www.oecd-ilibrary.org/docserver/6150ef8b-es.pdf?expires=1728901099&id=id&accname=guest&checksum=0E79838E53C73FBED198E22AC70437A8

165 OECD/CAF, "Practical Cases of AI Use in Governments in Latin America and the Caribbean" *Op. cit.*, note 61, pp. 46-47.

166 https://www.calameo.com/read/000099861d3cfe698d294

against the processing of their data[167].

The Costa Rican Judicial Power has opted for technological innovation as a response to a context of growing social demands, budgetary restrictions and a freeze on vacancies. In this challenging environment, the use of artificial intelligence has been promoted as a strategic tool to modernise processes, increase efficiency and guarantee the continuity of judicial services..

In the institution, AI solutions operate on an on-premises technological infrastructure, based on Google, Microsoft and Cloudera technologies, which guarantees control over the security, processing and traceability of data.

The initiatives have been developed with internal resources and are currently in a productive environment, generating tangible value in administrative, jurisdictional and customer service areas.

The main solutions that have been implemented are as follows:

- **ChatbotPJ** (2018): Automates attention to frequent queries about judicial services. Operates 24/7, generating more than 4,000 monthly interactions and estimated annual savings of $14,000.
- **Budget prediction** (2019): Machine Learning model to anticipate budget execution, used by more than 60 management centres, optimises the use of the institutional budget.
- **Document typifier** (2021-2024): Classifies more than 140,000 documents per month in collection matters. In 2024, it will process 900,000 documents automatically, saving the equivalent of 34 positions.
- **Nymiz** (2023): Commercial tool to anonymise personal data prior to the publication of court decisions, complying with Law 8968.
- **Prediction of criminal statute of limitations** (2024): Identifies files at risk of statute of limitations, optimising resources and prioritising cases.
- **Criminal complaint typifier** (2024): In pilot phase with the Judicial Investigation Agency (OIJ, for its acronym in Spanish), it allows for the automatic classification of complaints for more efficient initial management.

These tools have made it possible to offer a fairer, more accessible and proactive service. Its success has been made possible by three key pillars:

- The committed participation of expert users, who adjust and validate the models.
- The strategic backing of institutional hierarchies.
- An organisational vision that understands innovation as a habit, not an exception.

These experiences position the Costa Rican Judicial Power as a regional benchmark in the application of AI for justice, with a firm commitment to transparency, efficiency and respect for the fundamental rights of all people.

MEXICO

SORJUANA. This is an AI tool built based on programming tools from third-party companies such as Streamlit, Google and Pinecone, which was developed in the presentation of Minister Ana Margarita Ríos Farjat of the Supreme Court of Justice of the Nation (SCJN) and whose main purpose is to facilitate the reviewing, understanding and socialisation of the content of the public versions and sentences of the SCJN. The tool is currently in the testing phase and only considers the cases of Minister Ríos Farjat, but not all of the cases being analysed by the SCJN. The system provides summary answers on the content of the judgments and allows users to request explanations on specific chapters of current laws and regulations related to the rulings[168].

In Mexico, EXPERTIUS was also developed, a prototype expert system based on the symbolic or top-down paradigm. It has been developed at the Institute of Legal Investigations and the Centre for Applied Science and Technological Development (both of the UNAM), under the auspices of the National Council of Science and Technology, in collaboration with the Tabasco State Superior Court of Justice. Its purpose is to assist in decision-making and the homogenisation of collective knowledge of the judicial community, in maintenance trials to determine maintenance quantities. Expertius II is an evolution with a more complex model that aims to simulate the judge's logical reasoning with neural networks in Deep and machine learning type systems[169].

URUGUAY

The World Wide Web Foundation reports on the implementation of the PredPol crime prediction system between 2014 and 2017 in Uruguay, whose licence was acquired by the Ministry of the Interior with the aim of offering information and statistical models on crime prediction in certain geographic areas. Its use is reported to have been discontinued due to failure to reduce crime rates in this country and failure to meet its general objectives170.

167 Judicial Branch of Costa Rica, "Novel Artificial Intelligence tool applied to improve data protection", undated press release, at: https://pj.poder-judicial.go.cr/index.php/prensa/1186-novedosa-herramienta-de-inteligencia-artificial-se-aplica-en-mejora-de-la-proteccion-de-datos

168 The Sor Juana system portal is located at: https://ponenciamamrfgpt.streamlit.app/

169 CACERES NIETO, E. (2023). Artificial intelligence applied to law as a new branch of legal theory. Annals of the Francisco Suárez Chair, 57, 63–89. https://doi.org/10.30827/acfs.v57i.26281

170 World Wide Web Foundation, "Algorithms and Artificial Intelligence in Latin America. A Study of implementations by governments in Argentina and Uruguay", September 2018, pp. 27-30, at: https://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Spanish_Screen_AW.pdf

OECD/CAF, "Practical Cases of the Use of AI in Governments in Latin America and the Caribbean" in Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean, p. 45-46.

BLOCK 5: RECOMMENDATIONS FOR ACTION AND CONCLUSIONS

5.1. RECOMMENDATIONS FOR ACTION

The growing adoption and expansion of artificial intelligence in Latin America and the Caribbean has profoundly changed the landscape of organised crime in the region. Criminal organisations are leveraging advanced AI capabilities to develop new forms of crime that challenge traditional law enforcement strategies. The ability to generate synthetic identities or "fake persons" through technologies such as deepfakes is a significant threat that undermines trust in institutions and social interactions. Just as counterfeit money can destabilise economies and erode trust in financial systems, "counterfeit persons" have the potential to destabilise social and political systems by facilitating fraud, extortion and disinformation campaigns.

Faced with this challenge, it is imperative that Latin American and Caribbean countries adopt a regional and collaborative approach to develop effective strategies to combat the misuse of AI by organised crime. Specific recommendations aimed at addressing these challenges from a regional perspective are presented below.

1. **Defining and understanding AI.** It is recommended to publish a clear definition of what AI entails for each organisation. Promote a learning and research environment on AI and its potential impact on police activity.

2. **Creation of a regional cooperation framework.** Since organised crime operates across national borders, it is essential to establish regional cooperation mechanisms that allow for the exchange of information, good practices and technical resources. The creation of a regional body dedicated to cybersecurity and combating the misuse of AI can facilitate coordination between countries and strengthen collective capacity to confront these threats. To reduce this legal loophole of impunity, an international instrument with new crimes or aggravating circumstances related to artificial intelligence would facilitate the abolition of double criminality controls and might ensure faster mutual trust and much more effective international cooperation between courts. It also helps to prosecute new crimes and reduce impunity for them, and attempts to increase compensation for damages to victims.

3. **Updating data protection regulatory frameworks.** Strengthening personal data protection laws can limit the availability of information that criminal organisations need to generate false identities. Stricter regulation on access to and handling of sensitive data can reduce the risk of this information being exploited by malicious players.

4. **National AI strategies and sub-strategies for security, justice and judiciary authorities.** Design joint AI strategies containing specific objectives and goals that are measurable in the implementation and use of AI systems by justice authorities and the judiciary. These objectives may range from improving public safety, reducing crime rates, increasing the efficiency of investigated case management or improving the impartiality of judicial proceedings. The objectives must be measurable in the short and medium term and the strategies must be reviewed and updated periodically.

5. **Transparency in the processes of integrating AI into procedures for combating Organised Crime.** It is essential that the competent public institutions and criminal investigation agencies generate an environment and atmosphere of transparency, in which, based on not only legal but also ethical responsibility and through cooperation with the community, the most efficient use of AI in criminal investigation might be achieved, while generating confidence among citizens. Engage with the community to explain how AI will be used in policing and gather their feedback. Establish channels for ongoing community input and transparency regarding AI use.

6. **Prohibition and regulation of the creation of synthetic identities.** It is recommended that countries in the region establish legal frameworks that explicitly prohibit the creation and distribution of "fake persons" or synthetic identities for illicit purposes. This regulation should equate the creation of false digital identities with counterfeiting currency, recognising the damaging potential that both practices have on society and the economy. Furthermore, it is essential that these laws provide for appropriate criminal and civil sanctions to deter and punish these activities.

7. **Strengthening legislation on cybercrime.** Both substantive and procedural criminal codes in Latin American countries should be updated to include crimes or aggravating circumstances related to the malicious use of AI, such as the generation and dissemination of deepfakes, algorithmic manipulation, and automated fraud. This will enable authorities to effectively pursue and punish those who use these technologies for criminal activities.

8. **Implementation of ethical standards in AI development.** Promoting the adoption of ethical principles in the development and deployment of AI technologies is essential to prevent their malicious use. This includes incorporating security measures that make it difficult to create synthetic identities for illicit purposes, promoting responsible practices among developers and data scientists and establishing a governance structure to oversee the ethical and responsible use of AI, designating roles and responsibilities, and ensuring accountability.

9. **Establishment of specialised cybercrime units.** Creating and strengthening specialised units within law enforcement dedicated exclusively to cybercrime and AI misuse will allow for a faster and more effective response. These units must have trained personnel and adequate technological resources to confront highly sophisticated threats committed through AI systems and applications.

10. **Promoting research and development in AI security.** Fostering academic and scientific research into AI security will help develop new techniques and tools to counter emerging threats. Supporting regional research centres can foster innovative solutions

tailored to the Latin American context. Likewise, international information security quality certifications and standards such as ISO 27001, the Spanish National Security Scheme or Common Criteria should be encouraged and promoted.

11 **Development of public awareness campaigns.** It is essential to educate the public about the risks associated with "fake persons" and other forms of AI manipulation. Awareness campaigns can help citizens identify signs of fraud or misinformation, promoting a culture of healthy scepticism and caution in digital interactions.

12 **Strengthening monitoring capacities in prisons.** Considering the potential of AI systems to improve management, efficiency and security in prisons and communities, it is recommended that this type of tools be widely disseminated and used to measure and predict potential threats and identify high-risk criminal profiles for the prison population by establishing supervision and audit mechanisms and ensuring compliance with ethical and responsible principles such as transparency, explainability and human supervision.

13 **Conduct a comprehensive risk assessment to understand the potential challenges and threats associated with AI.** Establish a fundamental rights impact assessment and risk analysis and management mechanism with the adoption of technical, organisational and legal measures for continuous risk reduction and mitigation as AI technologies evolve.

14 **Promoting public-private collaboration.** Technology companies and digital service providers play a crucial role in detecting and preventing the misuse of AI. It is recommended to establish alliances between the public and private sectors to develop technological solutions that can identify and block malicious content, and share information on emerging threats and implement agile mechanisms to preserve stored computer data (subscriber data and traffic data) of service providers that may be useful to justice authorities in criminal investigations related to any type of crime.

15 **Plan AI acquisitions.** Understand the problems you are looking to solve with AI and tailor your procurement approach to ensure that the solutions you choose meet your needs and comply with the established policies.

16 **Investment in training and technological resources.** Establish training programmes for police, prosecutors and the judiciary designed for them to understand how AI applications most commonly used for criminal purposes by organised crime work. This includes the acquisition of advanced tools for the detection and analysis of criminal activities using AI, as well as specialised training to effectively interpret and use these resources in investigations and judicial processes.

17 **Implement training programmes to develop the knowledge and skills needed to leverage AI.** Promote cross-departmental training to ensure a unified approach to AI adoption.

18 **Establish rapid evaluation processes for the feasibility of projects to integrate AI solutions into criminal investigation procedures.** For example, in line with what is required by the European Parliament171 and what is suggested by the European Ethical

171 European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by law enforcement authorities and the judiciary in criminal matters (2020/2016(INI))

Charter on the use of artificial intelligence in and around judicial systems172, a check-list could be designed to help make a quick initial assessment of the risks and benefits of each potential project, including relevant aspects for both their legal viability and the procedural value of products that the proposed AI solution may generate. This quick check-list would help prioritise, or even rapidly discard the projects and the efforts devoted to each of them. The points to be checked could be those listed below, and the result of their assessment can only be one of two options: FAVOURABLE/UNFAVOURABLE:

- It is aimed at the protection and benefit of all members of society.
- It improves the Institution's working methods and criminal investigation capabilities.
- It can produce discrimination and contain biases.
- Impact assessment of impact on Fundamental Rights.
  - It affects human rights such as the right to privacy, presumption of innocence, effective judicial protection and an impartial judge.
  - It involves the processing of personal data.
  - It involves mass surveillance.
  - It entails automated analysis or recognition in publicly accessible spaces of human characteristics, such as gait, fingerprints, DNA, voice and other biometric and behavioural signals.
- It offers an acceptable standard of quality and safety.
  - It is reliable.
  - It is consistent.
  - It is auditable.
  - It ensures the attribution of legal responsibilities in the event of harmful effects.
- It is accessible, transparent, intelligible and explainable.
- It respects human autonomy. In other words, it guarantees that the final decision will be made by a human.

172 European Ethical Charter on the use of artificial intelligence in and around justice systems (2018). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021IP0405

5.2. CONCLUSIONS

Addressing the role of artificial intelligence not only as a powerful tool for development and innovation, as well as for streamlining processes in the administration of justice, security and the prison system or criminal investigation, particularly in the analysis of large volumes of data and the identification of complex patterns, but also as a factor that, if not managed properly, can enhance complex and high-impact criminal activities. Activities that we are already seeing in everyday life with phishing techniques, deepfakes and fraud, among others.

It is crucial that both governments and security organisations adapt to this new reality by developing and implementing responsible, ethical and objective technology to counteract AI misuse. This will require the development of robust regulatory frameworks that first of all allow AI technology companies and their use by society as a whole and by business and government ecosystems to flourish, and also criminalise and prosecute their misuse by both criminal organisations and state institutions.

This study, carried out from a holistic and multi-sectoral point of view, concludes with the following key points:

- **Need for a solid and ethical regulatory framework**: The implementation of artificial intelligence in the fight against organised crime raises important questions about ethics, privacy, gender bias and data protection. There is a fine line between surveillance for security and the violation of fundamental rights. It is therefore recommended that countries in the region reform the substantive legal and criminal procedural framework to regulate the use of AI for criminal purposes and objectives. In the absence of legislation, a robust regulatory framework must be created that oversees both the use of AI by authorities and its potential misuse. This framework must balance the protection of citizens' rights with national security and public order. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225) and the European AI Regulation are two examples that could be used both for ratification by countries concerned, in the case of the Council of Europe Framework Convention, and for the drafting of minimum standards on AI in Latin America and the Caribbean. There is also hope and we will have to keep an eye on possible outcomes related to a future Council of Europe instrument on artificial intelligence and criminal law, which the Committee of Ministers of the Council of Europe has entrusted to the CDPC.

- **In the procedural sphere, the inclusion of obligations to collaborate with providers of technology and AI systems in the investigation of serious crimes by justice authorities would be of great relevance.** Such collaborations have been taking place with some fluidity in aspects related to sexual abuse of minors. However, in AI matters, collaboration must be standardised, regulated and forced if necessary, given the impact that AI has on a multitude of crimes. Likewise, an express crime of disobedience must be established for those cases in which judicial requirements are not answered.

- **Regional and national strategies and specific guidelines.** The creation of national strategies and guidelines on AI for the authorities of the justice system in the region must be prioritised. Strategies should be developed jointly by the investigative authorities of the justice system and the judiciary and coordination and collaboration mechanisms established with technology and AI system providers. Strategies should include mechanisms for the participation of AI experts from the scientific and academic community who can help contribute to the work of activities that combat organised crime, and in particular in preventing and protecting victims of crimes committed through AI systems.

- **Tool development, process digitalisation and obtaining quality data.** Provide security, justice and judicial authorities in the region with AI tools and systems that facilitate and optimise their activities and that can help to better combat organised crime and prevent crime in its various forms. AI tools must be previously assessed and tested by the authorities, they must comply with ethical and responsible principles, have undergone impact assessments, provide information on at least the rules, parameters, applied logic, importance and consequences of the known source codes and have measurement indices that help to achieve specific objectives and goals during their implementation within the scope of each organisation. Furthermore, the development of AI tools is recommended because their internal development favours the digitalisation of processes in order to feed the tool with information and data. Without properly obtained and high-quality data, there is a risk of developing tools with unforeseen biases and trends.

- **Training and skills development to combat criminal technology**: The effectiveness of the fight against organised crime using AI depends largely on the adequate training of security forces, justice authorities and all operators in the criminal chain, as well as the development of teams of experts in cybersecurity, cybercrime and artificial intelligence.

- **Increase in the complexity and sophistication of criminal activities. Difficulty in detection and prevention**: The ability of AI algorithms to analyse large volumes of data and learn complex patterns is also exploited by criminal organisations to carry out more precise cyberattacks, identity theft using deepfakes, faster money laundering operations evading detection, all of which increases the sophistication of criminal groups. From another perspective, AI also facilitates the automation of various illicit activities, such as financial fraud and coordinated cyberattacks. Using AI to make communications and transactions anonymous allows criminals to operate with greater security and less risk of detection. This represents a significant barrier to law enforcement, which is surpassed in speed and technological complexity. This means that AI tools must be developed urgently in the field of security to counter these tactics.

- **Development of public-private strategic alliances.** Public-private collaboration in the development of AI tools for the justice, security and prison sectors is a unique opportunity to take advantage of technological potential and turn it into solutions that positively impact the lives of citizens, contributing directly and indirectly to preventing crime and fighting national and transnational organised crime groups. This strategic alliance will allow both sectors to build a safer, more efficient and transparent future, and also promote the development of technological ecosystems that will bring positive returns for national and local economies.

BIBLIOGRAPHY

Abusamadov, K. (2024). Revolutionizing crime prevention: The role of AI and big data in modern law enforcement. *Journal of Law, Market & Innovation, 1(2), 21-25.*

AGUILAR, Alberto R. (2023). The Interior Ministry admits that it has not consulted the AEPD about the facial recognition algorithm it is training the police in. Business Insider. 26 December 2022 Accessed 1 July 2023.

AIplusInfo. (2023). *How will artificial intelligence affect policing and law enforcement? Artificial Intelligence +.*

Amnesty International. (2018). *Toxic Twitter: Violence and abuse against women on-line.*

AMOS, Zac. (2023/08/11) What is FraudGPT? HackerNoon.

ASMANN, P. (15 August 2018). Are armed drones the weapon of the future for Mexico's cartels? *InSight Crime*

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access, 10, 77110–77122.*

IDB (n.d.). *PROMETEA: Transforming the administration of justice with artificial intelligence tools.*

CACERES NIETO, E. (2023). Artificial intelligence applied to law as a new branch of legal theory. Annals of the Francisco Suárez Chair, 57, 63–89

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science, 9(1).*

Centre for AI and Digital Policy (CAIDP). (2023). *Artificial Intelligence and Democratic Values Index 2023, pp. 56–77.*

Centre for Internet Security (CIS). (n.d.). Breaking down the BlackCat ransomware operation.

ECLAC. (24 September 2024). *Latin American Artificial Intelligence Index (ILIA) keeps Chile, Brazil, and Uruguay as regional leaders.*

ECLAC/CENIA. (7 August 2023). *Latin American Artificial Intelligence Index (ILIA). National Library of Congress of Chile, Department of Studies, Extension and Publications.*

Clarín. (14 October 2024). Scandal at a school in San Martín: a student is reported for selling AI-manipulated photos of his classmates naked.

European Commission. (25 April 2018). *Communication from the Commission: Artificial Intelligence for Europe (COM(2018) 237 final).*

European Commission. (7 February 2018). Visual analytics for brighter criminal intelligence analysis. In: Cordis.

European Commission. (14 March 2023). *Global Gateway: EU, Latin American, and Caribbean partners launch the EU-LAC Digital Alliance in Colombia [Press release].*

Constitutional Court of the Republic of Colombia. (15 December 2020). PRETORIA, the Constitutional Court's smart system to support the selection of *tutelas, is awarded as the best tool for modernisation in the field of justice by the CEJ [Bulletin No. 187].*

Constitutional Court of the Republic of Colombia (2024). Ruling T-323 of 2024. Second Review Chamber.

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

Council of Europe. (2018). *Algorithms and human rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications.*

Council of Europe. (8 April 2020). *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member states on the human rights impacts of algorithmic systems.*

Council of Europe. (2020). European Committee on Crime Problems (CPDC), '*Feasibility study on a future Council of Europe instrument on artificial intelligence and criminal law'.*

Council of Europe. (2024). *Framework Convention on Artificial Intelligence, Human Rights and the Rule of Law, CETS No. 225, Vilnius 5.IX.2024.*

Deloitte. (2021). *Surveillance and predictive policing through AI. Deloitte Insights. https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html*

Durán San Juan, Isabela. (2024). How will robots and artificial intelligence transform sexual relations in the future? Infobae

El Comercio. (16 July 2023). People's voices are cloned with AI to scam or fake kidnappings: at least 55 cases in Peru.

ENACT. (2023). *AI and organised crime in Africa. Sigsworth, R. ENACT Observer.*

European Commission. (8 April 2019). *Ethics guidelines for trustworthy AI.*

European Commission. (2022). *AI Watch: National strategies on artificial intelligence - A European perspective (2022 Edition).*

European Parliament. (July 2020). *Artificial intelligence and law enforcement: Impact on fundamental rights [Study requested by the LIBE Committee of the European Parliament]. González Fuster, G.*

European Parliament. (6 October 2021). *European Parliament resolution on artificial intelligence in criminal law and its use by law enforcement authorities and the judiciary in criminal matters (2020/2016(INI)).*

European Union Agency for Fundamental Rights (FRA). (8 December 2022). *Bias in algorithms: Artificial intelligence and discrimination.*

European Union. (2024). *Regulation (EU) 2024/1689 of 13 June 2023 establishing harmonised rules on artificial intelligence (AI).*

EUROPOL (2017). *European Union serious and organised crime threat assessment (SOCTA). European Union Agency for Law Enforcement Cooperation.*

EUROPOL (2020). *Malicious uses and abuses of artificial intelligence. Trend Micro Research, European Union Agency for Law Enforcement Cooperation.*

EUROPOL (2024). *AI and policing: The benefits and challenges of artificial intelligence for law enforcement [Observatory report from the Europol Innovation Lab].*

Faqir, R. S. A. (2023). Digital criminal investigations in the era of artificial intelligence: A comprehensive overview. *International Journal of Cyber Criminology, 17(2), 77-94.*

Office of the Attorney General, Directorate of Public Policies and Strategy. (n.d.). *PRISMA Tool: Risk profile of recidivism for the request for security measures.*

Fortune. (17 May 2024). A deepfake 'CFO' tricked the British design firm behind the Sydney Opera House in $25 million scam.

Habib Lantyer, V. (1 December 2023). *The era of artificial intelligence in law: Brazil in a global context. SSRN.*

HAO, Karen trad. MILUTINOVIC Ana (14 April 2021). Facebook's AI discriminates against women in job ads. *Technology Review.*

Hart, R. (4 May 2024). The conflict between Scarlett Johansson and OpenAI could lead to a war between celebrities and AI companies. Forbes Argentina. Accessed 1 June 2024.

Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture, 17(2), 209–233.*

Infobae. (29 August 2023). Chorrillos: Schoolchildren who altered photos of their classmates with AI and marketed them were not expelled.

InSight Crime. (26 August 2024). 4 ways AI is shaping organised crime in Latin America.

INTERPOL (2023). *Global threat assessment on scams. INTERPOL*

JOSEFINA GARCÍA, JON MARINA. *(2024). Use of artificial intelligence in the stock market (high-frequency trading). Pérez Llorca Techlaw 2024*

Kanwel, S., Imran Khan, M., & Usman, M. (2023). From bytes to bars: The transformative influence of artificial intelligence on criminal justice. *Qlantic Journal of Social Sciences, 4(4), 84-89.*

Keeper. (13 September 2024). How AI makes phishing attacks more dangerous.

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics, 26(1), 89–120.*

KOSINSK M. Y FORREST A. (2024). Prompt injection. IBM Research. 26 March 2024

LAMAS LOPEZ, F., & PERALTA GUTIERREZ, A. (2023). Public International Law Framework and Military Uses of Artificial Intelligence in the EU. Electronic Journal of International Studies, (46), 505–525

LÓPEZ B., Joaquín M. (2019). The artificial intelligence system to anticipate crimes in Bogotá. In: La República. 22 April 2019

MARTIN, Nacho. (2024). El Independiente. (9 November 2024). WormGPT: The unrestricted ChatGPT used by cybercriminals.

National School of Political and Administrative Studies. (n.d.). *Artificial intelligence – a double-edged sword: Organised crime's AI v.. law enforcement's AI.*

United Nations. (7 March 2024). *Artificial intelligence already reproduces gender stereotypes.*

OECD.AI Policy Observatory. *Catalogue of tools & metrics for trustworthy AI.*

OECD.AI Policy Observatory. *OECD AI Incidents Monitor (AIM).*

OECD. (2022). *OECD framework for the classification of AI systems. OECD Digital Economy Papers No. 323. OECD Publishing.*

OECD. (24 April 2024). *Report of the implementation of the OECD recommendation on artificial intelligence (C/MIN(2024)17).*

OECD & CAF Development Bank of Latin America. (2022). *The strategic and responsible use of artificial intelligence in the public sector of Latin America and the Caribbean. OECD Publishing.*

Olowe, O., Kawalek, P., & Odusanya, K. (2023). Artificial intelligence adoption in criminal investigations: Challenges and opportunities for research. In *UKAIS 2023 Conference Proceedings.*

Pereira-Kohatsu JC, Quijano-Sánchez L, Liberatore F, Camacho-Collados M. (2019). Detecting and Monitoring Hate Speech in Twitter. Sensors (Basel, Switzerland). Oct;19(21):E4654. DOI: 10.3390/s19214654. PMID: 31717760; PMCID: PMC6864473

Judiciary of Costa Rica (n.d.). Novel artificial intelligence tool applied to improve data protection. [Press Release].

Práxedes Martínez-Moreno, Andrea Valsecchi, Pablo Mesejo, Óscar Ibañez, Sergio Damas. (2024). Evidence evaluation in craniofacial superimposition using likelihood ratios. *Information Fusion.*

Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M. *(2018). Automatically applying misleading language detection to police reports: extracting behavioural patterns from a multi-step classification model to understand how we lie to the police. Knowledge-Based Systems, 149, 155-168*

RIOS, Juan. Infobae. (29 October 2024). Be careful on WhatsApp: they copy your mother's voice, use AI to create the scam and steal money from the bank.

Simmler, M., Brunner, S., Canova, G., & Schedler, K. (2023). Smart criminal justice: Exploring the use of algorithms in the Swiss criminal justice system. *Artificial Intelligence and Law, 31(2), 213-237.*

Singh Sankhla, M., Kumar, R., & Jadhav, E. B. (2020). Artificial intelligence: Advancing automation in forensic science & criminal investigation. *Seybold Report, 15(8).*

TechInformed. (15 October 2024). Deepfake cybercrime tool threatens crypto exchanges.

TRM. (11 October 2024). Ransomware in 2024: Latest trends, mounting threats, and the government response.

United Nations. (11 March 2024). *General Assembly Resolution 78/L.49: Harnessing opportunities of secure, protected and reliable AI systems for sustainable development.*

UNESCO. (2019). *I'd Blush if I Could.*

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence (SHS/BIO/PI/2021/1).*

UNESCO. (2023). *Global AI toolkit on AI and rule of law for the judiciary.*

UNESCO. (2024). *Artificial intelligence and gender equality: Key findings of UNESCO's Global Dialogue.*

UNESCO. (2024). *Challenging systematic prejudices: An investigation into bias against women and girls in large language models.*

UNICRI. (2024). *Generative AI: A new threat for on-line child sexual exploitation and abuse.*

UNICRI & INTERPOL. (February 2024). *Responsible AI innovation in law enforcement: AI toolkit.*

UNODC. (2024). *Casino underground banking report 2024. UNODC Publications.*

Varma Microsoft, P. (n.d.). *Transforming law enforcement policies and governance procedures: The benefits of AI integration.*

VV.AA., HERRERA TRIGUERO, Francisco; PERALTA GUTIÉRREZ, Alfonso; TORRES LÓPEZ, Leopoldo Salvador. (2022). Chapter "Police use of artificial intelligence systems in the comparative field" p. 453 and following. Law and artificial intelligence. 2022. 24/10/2022. Editorial Universidad de Granada. 978-84-338-7049-0.

West, S. M., Whittaker, M., & Crawford, K. (2019). *Discriminating systems: Gender, race, and power in AI. AI Now Institute.*

WIRED. (15 October 2024). Millions of people are using abusive AI 'Nudify' bots on Telegram.

World Wide Web Foundation. (September 2018). *Algorithms and artificial intelligence in Latin America: A study of implementations by governments in Argentina and Uruguay.*

EL PACCTO 2.0

EU-LAC Partnership on justice and security

Funded by EU