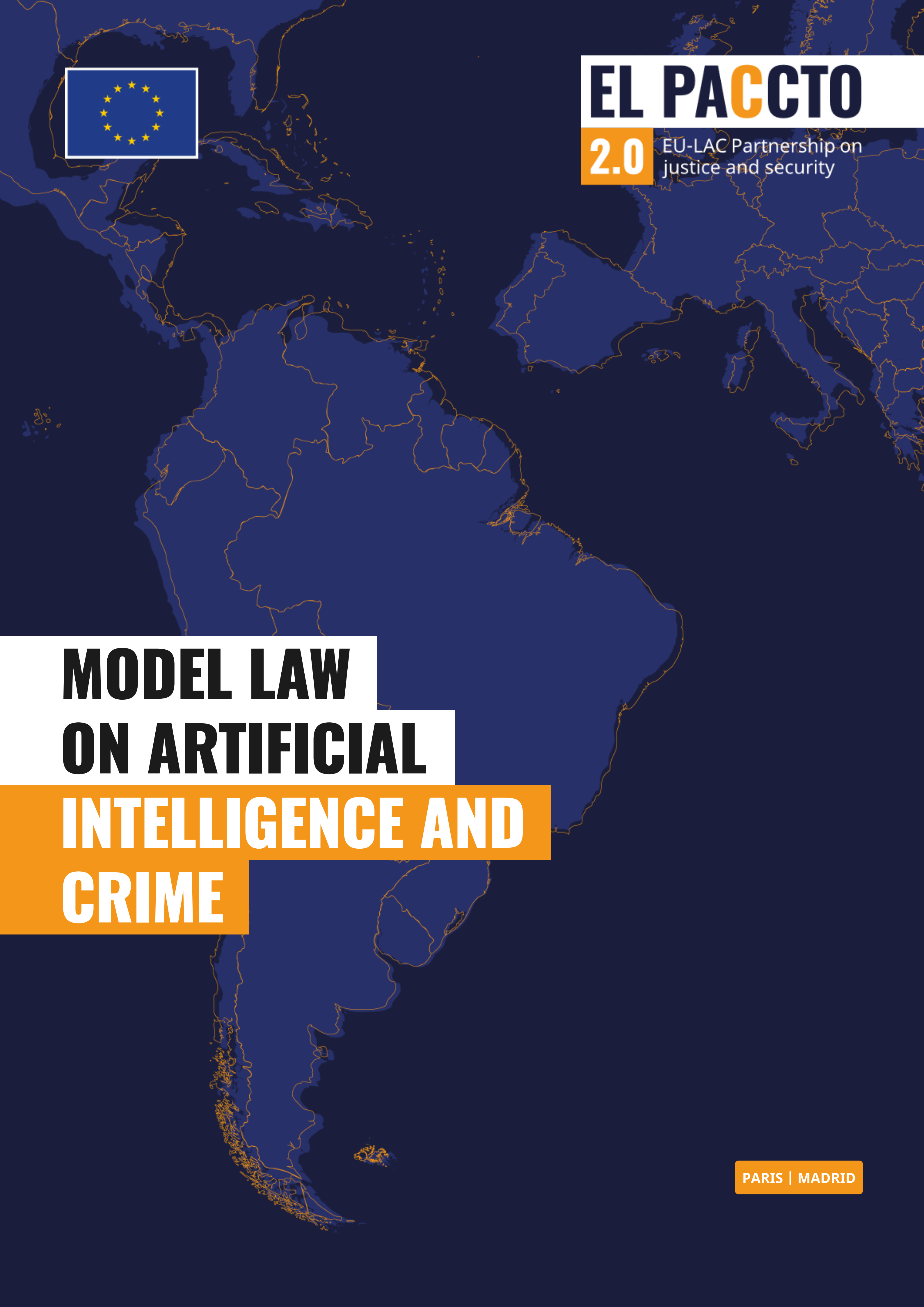


EL PACCTO 2.0

EU-LAC Partnership on justice and security

MODEL LAW ON ARTIFICIAL INTELLIGENCE AND CRIME

PARIS | MADRID

Edited by: EL PACCTO 2.0

Coordinated by:

With the direction and review of:
Marc Reina Tortosa, Executive Manager, EL PACCTO 2.0
Emilie Breyne, Project Officer, EL PACCTO 2.0

Authors

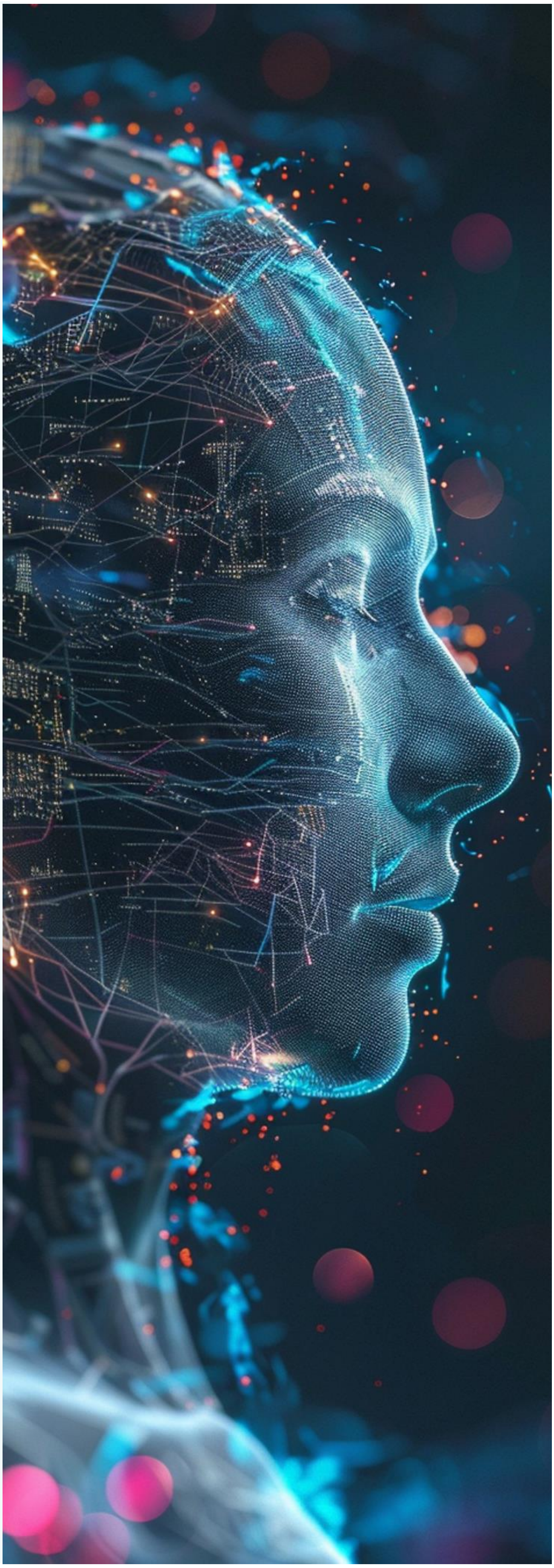
Alfonso Peralta, Cristos Velasco and Thomas Cassuto

Usage Rights: This document has been prepared for the EL PACCTO 2.0 Programme, with financial support from the European Union. However, it reflects only the opinions of the authors and not those of the Programme and/or the European Union. EL PACCTO 2.0 and the European Union are not responsible for any consequences arising from the reuse of this publication.

Non-commercial edition

Madrid, August 2025

info@elpaccto.eu
Avenida del Partenón, 16-18, 3ª planta
28042 – Madrid (Spain)



INDEX

BACKGROUND

Exponential growth in the use of Artificial Intelligence (AI) systems and applications has permeated the way humans interact with this technology in different areas of today's economy and in the administration of justice. The adoption and implementation of AI systems in the work of security and intelligence agencies and criminal justice authorities, including the judiciary, is gradually becoming a reality in some countries. AI has the potential to facilitate, enhance and improve the investigative work of the criminal justice authorities and government agencies that are responsible for countering organized crime. However, organized criminal groups and criminal networks are also exploiting and making use of AI systems to enable and perpetrate many traditional and evolving types of crimes, and to enhance the automation of attacks using AI to perform their illicit activities on a larger scale and support the creation of new crime-as-a-service (CaaS) profit models, while reducing the chances of being identified by law enforcement authorities.

In recent years, technological advancements have accelerated rapidly, bringing remarkable benefits but also a darker side that organized crime has seized upon to evade the efforts of the justice system and law enforcement agencies. Criminals leverage AI to streamline and amplify their attacks, increase their profits in a shorter time frame, exploit more victims, elevate social engineering significantly, and devise more sophisticated criminal enterprises, all while minimizing the risk of detection. The advent of Generative AI and Large Language Models has further revolutionized this landscape.

Evidence shows that AI is driving an acceleration in various crimes, such as financial crime, phishing, DDoS attacks, Chile Sexual Abuse Material (CSAM) distribution, romance scams, and fraud. It is boosting these activities, increasing both revenue for criminals and harm to victims, and has also enabled new types of crimes, such as Deepfakes.

In December 2024, EL PACCTO 2.0 published the *Artificial Intelligence and Organized Crime Study.*[1] Among other things, the report contains an in-depth analysis of the main crimes committed using AI tools, describes current cases and examples of crime typologies, and highlights how AI is currently being used and exploited by organized criminal groups in Europe and Latin America and the Caribbean (LAC). The conclusions and recommendations for action contained in the study include the development of robust regulatory frameworks to counter the use, abuse and exploitation of AI systems by organized criminal groups to perpetrate crimes and illicit conducts. It also sets out key recommendations, some of which emphasize the need to reform substantive and procedural legal frameworks in the criminal field, including strengthening and updating legislation on cybercrime and the malicious use of AI for criminal activities.

[1] E., Velasco, C., Bueno Benedí, M., Gómez Gómez, J. de D., García Periche, J., & Peralta Gutiérrez, A. (2024). Artificial Intelligence and Organised Crime. Expertise France and FIAP. https://doi.org/10.5281/zenodo.16740421

In March 2025, EL PACCTO also published a document on *Mapping and Profiling the Most Threatening Criminal Networks (HRCN) Operating in Latin America and the Caribbean*.[2] It contains mapping and a description of the most prolific and known criminal networks operating in the LAC region, and a brief description of their core activities. The report mentions that the criminal portfolios of these organized crime groups include serious offenses involving cybercrime, sexual exploitation, extortion, human trafficking, and the use of crime-as-a-service (CaaS) models to recruit individuals and exploit victims.

EUROPOL recently released the *Serious and Organized Crime Threat Assessment (SOCTA) 2025 Report,*[3] in which it identified AI as a transformative force that is enhancing various criminal activities and the ability of criminal networks to adapt rapidly to the new technological solutions offered by AI, including tactics for serious organized criminal activities involving the CaaS model, financial crime and money laundering, criminal exploitation of legal business structures, corruption, violence, cyberattacks, online fraud schemes, online child sexual exploitation, trafficking in human beings, currency counterfeiting, and terrorism, among other illicit activities.

EUROPOL's report highlights several key areas where the use of AI is particularly concerning:

- *AI-Driven Fraud and Cybercrime:* Criminal networks are increasingly utilizing AI to conduct sophisticated fraud schemes. Generative AI enables the creation of realistic multilingual impersonations facilitating large-scale, automated scams that are challenging to detect.
- *State-Sponsored Cyber-Attacks:* The report underscores the convergence of state-sponsored actors and criminal networks, with AI-enhanced cyber-attacks targeting critical infrastructure and public institutions. These attacks often serve dual purposes of financial gain and geopolitical destabilization, posing significant security challenges.
- *Emerging Threats from Autonomous AI:* Europol raises alarms about the potential emergence of fully autonomous AI systems that could operate without human oversight. Such developments may lead to AI-controlled criminal networks, marking a new era in organized crime and presenting unprecedented challenges for law enforcement.
- *Online Child Sexual Exploitation* will be further accelerated by AI, expediting the generation of materials and stepping up the scale and the production of Child Sexual Abuse Material (CSAM). The report mentions that Generative AI has emerged as a new way of producing CSAM, leading to growing concerns relating to the manipulation of images, text and video, and to synthetic AI-generated CSAM multiplying the volume of such material online, thereby creating additional challenges in analyzing the images and identifying the victims and offenders. AI tools will enhance offenders' countermeasures and shift CSAM production methods.

[2] EL PACCTO 2.0 and InSight Crime (2025), *Mapping and Profiling the Most Threatening Criminal Networks in Latin America and the Caribbean*. Available at: https://insightcrime.org/wp-content/uploads/2025/02/Mapping-and-profiling-HRCN_LAC.pdf

[3] Europol (2025), *Serious and Organised Crime Threat Assessment (SOCTA).* Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

One of the key aspects highlighted in the *SOCTA 2025 report* is that "policymakers, law enforcement agencies, and the technology sector must collaborate to develop robust safeguards, consistent regulations and advanced detection tools to counter the growing threat of AI enabled crime". Further, it places strong emphasis on the need to improve international cooperation and forward technological solutions to address the evolving threats posed by AI in the realm of organized crime.

Similarly, on 1 September 2025, EL PACCTO 2.0 published a study mapping Latin American and Caribbean criminal networks that use AI to commit serious crimes.[4] The study focuses on identifying some of the major operators, facilitators, and platforms that sell AI services for committing crimes on both the open internet and the dark web. In Mexico, for example, several criminal networks and cartels, such as the Sinaloa Cartel and the Jalisco New Generation Cartel, have been identified as deploying AI systems with drones for territorial control and monitoring, deliveries and transport, but also to intimidate and terrorize the civilian population and rival criminal groups. The study also focuses on analyzing the modus operandi and technology used by these criminal networks. Reference is also made to other networks and platforms operating outside the Latin American and Caribbean region.

The European Commission (EC) published its *European Internal Security Strategy* in April 2025.[5] It highlights AI as a tool for enhancing security capabilities, particularly for law enforcement and judicial authorities. However, it is also noted that cyberattacks and information manipulation are increasingly exploiting new technologies like AI. The strategy highlights EC plans to invest in security research and innovation, and in facilitating training to improve the use of AI systems by law enforcement and judicial authorities. The *European Internal Security Strategy* also describes organized crime as a significant and evolving threat in the EU, and notes that powerful organized crime networks are proliferating, often nurtured online and spilling over into the economy and society. It highlights the objective of the EC to propose stronger rules to tackle organized crime networks, including modernized legislation, enhanced intelligence sharing, and measures to cut off access to criminal tools and assets. The vulnerability of young people to being recruited by organized crime is also highlighted as a major concern, with plans to address the root causes through education and crime prevention policies. Guidelines are also established to ensure that minors – as users of online platforms – enjoy greater protection with higher levels of privacy, security and safety.

The pace of development of substantive and procedural legislation to counter cyber-enabled crimes and crimes committed or assisted through AI has been rather slow and not entirely straightforward and consistent. This is despite the ongoing efforts of international and regional organizations to support countries in the development of legislation based on

[4] Juan Manuel Aguilar Antonio (2025), Use of AI by High Risc Criminal Networks: mapping and profiling. EL PACCTO 2.0. DOI: 10.5281/zenodo.16750778

[5] European Commission (2025), European Internal Security Strategy – Protect EU. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148

international frameworks on organized crime and cybercrime, like the *UN Convention against Transnational Organized Crime*, the *Council of Europe's Budapest Cybercrime Convention* and its two additional protocols, the *Council of Europe's Convention on the Protection of Children against Online Sexual Exploitation and Sexual Abuse*, *The Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 225),* and the recent *UN Convention against Cybercrime*.

In response to these crimes, some countries have recently introduced new legislation or amendments specifically regarding sexual deepfakes. In May 2025, the President of the United States of America signed the *TAKE IT DOWN Act,*[6] which prohibits the nonconsensual online publication of intimate and sexual visual depictions of individuals, both authentic and computer-generated, and requires certain online platforms to promptly remove such depictions upon receiving notice of their existence. Under this law, perpetrators would be subject to mandatory restitution and/or criminal penalties, including a fine. Separately, the platforms covered by the legislation must establish a process through which subjects of intimate visual depictions may notify the platform of their existence and request the removal of any intimate visual depiction of them that was published without their consent. The platforms that are covered must remove such depictions within 48 hours of notification. Under the bill, the platforms that are covered are defined as public websites, online services, or applications that primarily provide a forum for user-generated content.

In September 2024, South Korea introduced three amendments to the *Deepfake Sexual Crime Prevention Act,*[7] which include strengthening the state's responsibility to criminalize deepfake crimes and enhancing victim recovery measures. The law provides for penalties and imprisonment with up to 7 years or a fine of up to 50 million of South Korean won for individuals who edit, summarize, process, publish or compile photographs, videos, or audios using the face, body or voice of a person in a form that may cause sexual desire or shame against their will. The law criminalizes the possession or compilation of images, with prison terms of up to 3 years and fines of up to 30 million. The use of synthetic techniques is also criminalized.

The Australian parliament is debating the *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024.*[8] This creates a new offense where a person uses a carrier service to transmit sexual material which depicts (or appears to depict) another person (who is, or appears to be 18 years of age or over) when: (i) the person knows the other person does not consent to the transmission; or (ii) the person is reckless as to whether the other person consents to the transmission. This Bill also created two aggravated offenses and repealed two existing aggravated offenses.

The United Kingdom has introduced a new criminal offense concerning sexually explicit 'deepfake' images, including creating and sharing intimate image without consent and

[6] Available at: https://www.congress.gov/bill/119th-congress/senate-bill/146
[7] Available at: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=68812&type=part&key=9
[8] Available at: https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r7205

installing equipment to enable these offenses. Perpetrators could face up to two years in prison.[9] In the UK, it is already an offense to share or threaten to share intimate images, including deepfakes, under the Sexual Offenses Act 2003, following amendments that were made by the Online Safety Act 2023.

Mexico has approved the Olimpia Law which criminalizes the non-consensual dissemination of intimate content, including content generated by artificial intelligence, such as deepfakes, as a form of digital violence. It establishes penalties of between three and six years in prison and financial fines, with harsher penalties if the victim is a woman, a minor, or if the content is disseminated on a large scale or for profit. It protects the right to privacy and dignity of the individual, and punishes the use of technology for the purposes of control, humiliation or gender-based violence in digital environments.

Argentina has enacted Law 27,736, which, like in Mexico, establishes a new form of gender-based violence, digital violence, as a specific form of aggression against women encompassing any action in digital environments that violates their dignity, reputation, identity, freedom, or sexual integrity. It considers dissemination of intimate content without consent to be a crime, whether it is authentic or manipulated using technologies such as artificial intelligence. Although the law does not explicitly mention artificial intelligence, it does cover content that has been edited or falsely attributed to women, including deepfakes.

Peru introduced *Law No. 32214* in April 2025,[10] amending the Penal Code and Cybercrime Law to regulate the use of artificial intelligence in the commission of crimes as an aggravating circumstance. It imposes strict penalties for several specific crimes enabled by Artificial Intelligence, such as child pornography, defamation and aggravated fraud, among others. The fines and penalties range from one to ten years’ imprisonment, depending on the gravity of the offense, and it also provides for additional fines. Infringements of copyright by artificial intelligence are also criminalized.

In Spain, the *draft Organic Law for the protection of minors in digital environments*[11] is currently going through a legislative revision process. Article 173 bis punishes individuals that, without the authorization of the persons concerned and with the intention of undermining their moral integrity, disseminate, exhibit or transfer body images or voice audio generated, modified or recreated using automated systems, software, algorithms, artificial intelligence or any other technology, in such a way that it purports to be real, simulating situations of sexual content or seriously degrading situations. Different aggravated offenses are also introduced in this draft bill, addressing the use of fake identities through technology to facilitate or enable the commission of crimes against minors.

[9] GOV.UK, Press release "Government crackdown on explicit deepfakes", 7 January 2025. Available at: https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes
[10] Available at: https://edicioneslegales.com.pe/wp-content/uploads/2025/04/32314.pdf
[11] Available at: https://www.congreso.es/public_oficiales/L15/CONG/BOCG/A/BOCG-15-A-52-1.PDF

JUSTIFICATION FOR A MODEL LAW ON AI AND CRIME

A Model Law is a very useful, effective, and flexible legal instrument for the harmonization (approximation) of law between different jurisdictions, functioning as a soft law mechanism that facilitates the adoption of common minimum standards while respecting the particularities of each national legal system, and without imposing rigid structures. Its non-binding nature is essential, as it respects the sovereignty of each State and its right to establish its own legal framework.

The concept has its origin in the method used by the National Conference of Commissioners on Uniform State Laws, whose purpose is to create harmonized state law by introducing substantive or adjective rules into the domestic legal system of the states, in order to prevent inconveniences arising from legislative diversity through the application of basic precepts establishing the possibility of making the necessary modifications to take into account the peculiarities and special circumstances of nations. [11]

Model laws offer greater flexibility, allowing countries to make adaptations according to their particular needs without distorting the essence of the instrument. They seek international harmony of solutions through the admission of rules that are not binding in the strict legal sense, because they are not coercible, and their compliance is not imposed; but which, however, have an effective validity in practice because they are accepted and obeyed voluntarily by the participants through a general acceptance and consensus of their validity, usefulness, and recognition of their added value.

The nature of model laws allows each state to incorporate them as a separate special law literally into national law, or to integrate them as part (chapter or section) of a larger existing legislation on the subject matter in question as modifications or amendments or to serve as general guides to inspire legislators. In this project, the aim is for the states of Latin America and the Caribbean to be able to use this model law on artificial intelligence and crime either in its entirety or in parts, with the possibility of enrichment, improvement, modifications and adaptations to their respective legal systems and jurisprudence.

Model laws serve as a starting point for states to introduce, discuss, and ultimately pass legislation on certain topics and areas. By building on a pre-existing draft, model laws can significantly speed up the legislative process and make it more effective and consistent so that legislators can focus on those issues that are most controversial or of greatest interest according to their needs.

[11] PARRA ARANGUREN, G. (1998). Studies in International Commercial Law. Caracas: Central University of Venezuela, pp. 71 and 318, cited by BERMÚDEZ ABREU, Yoselyn, & ESIS VILLAROEL, Ivette. (2008). THE UNCITRAL MODEL LAW ON INTERNATIONAL COMMERCIAL ARBITRATION AND ITS IMPACT ON THE VENEZUELAN LEGAL SYSTEM. Law Review, (29), 257-266. Retrieved on 4 August 2025 from: https://www.redalyc.org/pdf/851/85102910.pdf

As mentioned in the previous paragraph, there are several purposes for legislative uniformity and filling existing legal gaps, all in accordance with the protection of fundamental rights and public freedoms. In this case, model laws are particularly useful for addressing contemporary needs and technological advances by modernizing legislation through agile frameworks, and aligning it with international standards and best practices.

Legal uniformity seeks to generate a more predictable and consistent legal environment, thereby decreasing the costs and complexities associated with navigating different legal systems. Better legislative drafting, on the other hand, contributes to clearer and more accessible laws, minimizing ambiguity and the possibility of misinterpretations, as well as increasing legal certainty in order to promote and not harm the innovation and development of artificial intelligence. In the case of a global technology market, this is especially important where multinational companies often operate through multiple legal systems. The use of a Model Law also facilitates judicial cooperation by addressing questions relating to dual criminality, particularly in matters of extradition, international cooperation, and mutual legal assistance.

This specific Model Law on Artificial Intelligence and Crime aims to achieve greater legislative quality by taking advantage of the specialized knowledge and expertise not only of the work of the drafting team, but also of all the intervening countries and their representatives, which makes it almost impossible to reach each of them in each jurisdiction individually. In this way, a single, well-informed, and harmonized initiative can serve as a template or model for various legal systems. The idea of drafting a model law on AI and crime was launched at the "*First bi-regional conference on AI and organized crime*" held in San Jose in Costa Rica from 2 to 4 December 2024, and materialized at the "*Multi-country meeting on AI regulatory development and regional AI strategy*" held in Brussels from 23 to 25 April 2025. Both meetings were organized by the EU flagship programme on Justice and Security in Latin America and the Caribbean called EL PACCTO 2.0.

The main purpose of this Model Law is to support and guide LAC countries to use a framework to generate future legal reforms of substantive and procedural criminal legislation at the national level in order to counter the use of AI systems for criminal and malicious purposes by organized criminal groups operating and targeting victims located in LAC countries. This model law framework, as its name suggests, is only "a model law" and does not substitute the current binding international treaties, conventions and existing legislation in the area of transnational organized crime, cybercrime, online child sexual exploitation and abuse, money laundering, and artificial intelligence developed by international and regional organizations.

To facilitate and reduce the existing regional legal loopholes, the Model Law sets forth a list of conducts and offenses assisted or enabled by AI and currently used by organized criminal groups, as well as procedural provisions for the purpose of specific criminal investigations and procedures involving the use of AI systems and applications.

Finally, the Model Law seeks to provide a flexible legal framework for regional and international cooperation between criminal justice authorities (police investigators, public prosecutors, judges and magistrates), and to facilitate and support the investigation, prosecution and adjudication of conducts and evolving threats raised by the use of AI in order to decrease the level of impunity and optimize enforcement and prosecution in the area of criminal justice in the LAC region, prioritizing the protection of particularly vulnerable populations.

MODEL LAW ON ARTIFICIAL INTELLIGENCE AND CRIME

PREAMBLE

Whereas AI is increasingly being leveraged for tools and platforms that facilitate the commission of crimes and illegal activities conducted by organized criminal groups;

Whereas many countries in Latin America, the Caribbean and the EU do not yet have substantive and procedural legal frameworks to investigate and prosecute crimes committed or assisted through AI Systems.

Whereas persons involved in criminal acts can leverage AI to improve and speed up their attacks by seizing profitable opportunities, targeting new victims, and developing more inventive criminal business models.

Whereas some democracies have introduced new legislation or amendments specifically criminalizing the use and diffusion of deepfakes for fraudulent activities and the diffusion of non-consensual sexual images and content for malicious and criminal purposes.

Delegates have agreed on a Model Law on Artificial Intelligence and Crime (MLAIC) as follows.

PART I. PURPOSE, SCOPE OF APPLICATION, INTERPRETATION AND DEFINITIONS

Article 1. Purpose

The main purpose of the Model Law is:
1. To establish a regional framework for the development of national legislation on criminal law relating to artificial intelligence, including organized crime.
2. To encourage countries of Latin America and the Caribbean to fill the existing gaps and loopholes in the area of criminal law and artificial intelligence by addressing and regulating relevant aspects through substantive and procedural criminal legislation, and using common international normative principles, in particular to:
- Criminalize offenses resulting from the misuse of artificial intelligence systems.
- Punish the use of AI for the commission of an offense as an aggravating circumstance.

- Crack down on the use of AI to create, generate and disseminate deepfakes that infringe on personal rights and personal data for malicious and illegal purposes.
- Protect human rights and personal data; and
- Clarify the conditions of criminal liability in the event of fraudulent use of an artificial intelligence system.

3. To provide for the development of AI systems while protecting the fundamental rights enshrined in and regulated by international and regional instruments on human rights, national legislation, jurisprudence and existing case law at national level.
4. To empower courts to cooperate more effectively with foreign counterparts and representatives on new criminal models related to artificial intelligence, in particular to:

- Define jurisdictional competence in criminal matters in connection with the use of artificial intelligence systems.
- Establish general rules of procedure intended to punish offenses committed in connection with artificial intelligence systems.
- Establish rules to facilitate judicial cooperation in order to punish offenses committed in connection with artificial intelligence systems more effectively.

Article 2. Scope of application

This Model Law:

1. Applies to offenses related to, committed, or enabled through artificial intelligence systems insofar as they affect individual rights and personal data, as an instrument, and as aggravating circumstances in the occurrence of offenses already in force in national laws.
2. Sets forth rules for strengthening liability, aggravating circumstances, and penalties for behaviors related to the wrongful application or misuse of artificial intelligence systems, and enhancing protection for the victims.
3. Provides rules for establishing jurisdiction when addressing offenses related to, committed, or enabled through artificial intelligence systems.
4. Provides rules for reinforcing judicial cooperation in dealing with offenses related to, committed, or enabled through artificial intelligence systems.
5. The provisions of this Model Law do not affect or prevent the development of technical standards and policies, particularly ethical frameworks, in the areas of artificial intelligence system governance, development and implementation, provided that these are consistent with the principles arising from this law.

Article 3. Interpretation

1. In the interpretation of this Model Law, regard is to be had to its regional origin and to the need to promote uniformity in its application and the observance of good faith.
2. Aspects concerning matters governed by this Model Law which are not expressly settled herein are to be settled in conformity with the general principles on which this Model Law is based, as mentioned in the second section of Article 1.

Article 4. Definitions

For the purposes of this Model Law, the key concepts include:

‘AI deployer’ means a natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity. **(*Art 3 (4) EU AI Act)***

‘AI provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system, or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge. **(*Art 3 (3) EU AI Act)***

‘Importer’ means a natural or legal person located or established in the country that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country. **(*Art 3 (6) EU AI Act)***

‘Distributor’ means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market. **(*Art 3 (7) EU AI Act)***

‘Operator’ means a provider, product manufacturer, deployer, authorized representative, importer or distributor. **(*Art 3 (8) EU AI Act)***

‘Artificial intelligence system’ means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Different artificial intelligence systems may vary in their levels of autonomy and adaptiveness after deployment**. *(Art 2. CoE Framework Convention on AI and HRDRL and Art 3. EU AI Act)***

‘Content data’ means any electronic data, other than subscriber information or traffic data, relating to the substance of the data transferred by an information and communications technology system, including, but not limited to, images, text messages, voice messages, audio recordings and video recordings (***Art. 2(d) UN Convention against Cybercrime)***

‘Critical infrastructure’ means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network, or a system, which is necessary for the provision of an essential service. ***(Art. 2(4) EU Directive on the Resilience of Critical Entities of 14.12.2024)***

‘Deepfake’ means AI-generated or manipulated image, audio, video, or any other content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful. **(*Art 3 (60) EU AI Act)***

“Information and communications technology system” means any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data. **(*Art.2 (a) UN Convention against Cybercrime)***

‘Particularly vulnerable population’ shall be understood to mean minors, persons with disabilities, women and others who face a greater risk of exploitation and revictimization.

‘Organized criminal group’ means a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offenses in order to obtain, directly or indirectly, a financial or other material benefit; ***(Art. 2(a) UN Convention against Transnational Organized Crime)***

‘Personal data’ means any information relating to an identified or identifiable natural person **(*Art. 2(g) UN Convention against Cybercrime)***

‘Serious crime’ means conduct constituting an offense punishable by a maximum deprivation of liberty of at least four years or a more serious penalty. ***(Art. 2 (b) UN Convention against Transnational Organized Crime and Art.2 (h) UN Convention against Cybercrime)***

‘Subscriber data’ means any information that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
(i) The type of communications service used, the technical provisions related thereto and the period of service;
(ii) The subscriber’s identity, postal or geographical address, telephone or other access number, billing or payment information, available based on the service agreement or arrangement. **(*Art. 2(f) UN Convention against Cybercrime)***

‘Traffic data’ means any electronic data relating to a communication by means of an information and communications technology system, generated by an information and communications technology system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration or type of underlying service. **(*Art. 2(c) UN Convention against Cybercrime)***

‘Malicious purposes’: the intentional use of an AI system to cause unlawful harm or benefit without right.

PART II. OFFENSES

Title I. Aggravating circumstances

Article 5

1. The following constitute an aggravating circumstance:

(i) The use of an artificial intelligence system to commit the crime of terrorism and financing of terrorist activities.

(ii) The use of an artificial intelligence system to cause or attempt to cause the death of a person.
(iii) The use of an artificial intelligence system to control or manipulate robots, autonomous weapons, or drones to cause the death of a person or a group of persons.
(iv) The use of an artificial intelligence system to commit crimes related to fraud, extortion, impersonation and identity theft, forgery and money laundering, including laundering of the proceeds of crime.
(v) The use of an artificial intelligence system to harass, intimidate, extort, threaten or harm the physical or psychological integrity of a person, particularly when the harassment is committed by the dissemination and publication of messages, images, videos or any other violent content accessible to the public by any electronic means.
(vi) The use of an artificial intelligence system to commit any other serious offenses.

2. In the previous paragraph, the use of an AI system shall be deemed to mean to help to evade the efforts of the justice system and law enforcement agencies, amplify attacks, increase profits in a shorter time frame, exploit more victims, or increase social engineering, all while minimizing the risk of detection.
3. The maximum penalty incurred shall be increased proportionally when an aggravating circumstance as provided for in this article has been sufficiently demonstrated.

Title II. Fraud, swindling and breach of trust

Article 6.

The use of an artificial intelligence system to abuse the trust of another intentionally and without right, or to commit or perpetuate fraud to the detriment of another person, including causing loss of property or an intangible financial asset, digital assets, stablecoins or electronic assets recorded on a distributed ledger or wallet, and to procure an economic benefit for oneself or for another person, shall be punished.

Title III. Artificial intelligence system as an instrument of crime

Article 7.

(i) The use of an artificial intelligence system for the purpose of targeting a victim, to identify, manipulate, exploit any vulnerabilities, or distort the behavior of a person or a group of persons and lure victims through social media with the intention of committing a criminal offense, regardless of the result, shall be punished.

(ii) The use of an artificial intelligence system for the purpose of concealing the consequences of the commission or attempted commission of a criminal offense shall be punished.

(iii) The use of an artificial intelligence system for the purpose of committing an attack against a critical infrastructure facility or a critical infrastructure provider shall be punished.

(iv) The use of an artificial intelligence system for the purpose of concealing, altering or modifying physical or electronic evidence of the commission or attempted commission of an offense shall be punished.

Title IV. Offenses resulting from the alteration or modification of an artificial intelligence system

Article 8.

(i) Whoever promotes, manufactures, distributes, exhibits, offers, markets, advertises, publishes, imports, exports or handles technologies with the sole purpose of committing or attempting to commit an offense regulated by this law shall be punished. The design, provision, making accessible or available, facilitation or marketing of an artificial intelligence system for the purpose of committing or attempting to commit an offense targeting a victim, or of concealing the consequences of committing or attempting to commit an offense, shall be punished.

(ii) The fraudulent introduction, modification or destruction of an artificial intelligence system or any voluntary intervention intended to alter the foreseeable functioning of an artificial intelligence system with the sole purpose of committing or attempting to commit an offense regulated by this law, shall be punished.

(iii) The fraudulent introduction, modification or destruction of an artificial intelligence system or any voluntary intervention intended to alter the foreseeable functioning of an artificial intelligence system used for decision-making processes affecting third parties, in conditions likely to affect the decision-making process or the decision, shall be punished.

Title V. Offenses related to child sexual exploitation and abuse, dissemination of intimate images and misuse of devices and platforms

Article 9. Offenses related to Child Sexual Exploitation and Abuse through artificial intelligence systems

(i) Whoever intentionally creates, generates or edits pornographic content or material involving any real or fictitious person who clearly has the appearance of a child, made by or with the use of an artificial intelligence system, an edited, synthesized, or processed photograph, video, or audio targeting the face, body or voice of a person or any other personal data, engaged in sexually explicit conduct, or appearing to be a minor engaged in sexually explicit conduct, in particular a child under the national age of sexual consent, shall be punished.

(ii) Whoever intentionally produces, offers, sells, distributes, transmits, broadcasts, displays, publishes or otherwise makes available through any platform child sexual abuse or child sexual exploitation material made by or with the use of an artificial intelligence system, shall be punished.

(iii) Whoever possesses or shares, intentionally and without right, child sexual abuse or child sexual exploitation material through any platform, stored in an information and communications technology system or another storage medium, commits a serious offense and shall be punished.

(iv) Whoever uses an artificial intelligence system to create a false, fictitious, or imaginary identity for themselves, or to appear as someone else, or to misrepresent their age, sex, legal gender identity, or other personal characteristics, with the intent of committing a crime or deceiving someone into providing pornographic or sexual abuse material or showing them pornographic images, commits a serious offense and shall be punished. It constitutes a more serious offense when the person or victim is a minor, as they are a particularly vulnerable population.

(v) Whoever promotes, manufactures, distributes, exhibits, offers, markets, advertises, publishes, imports, exports, sells or handles technologies to make a fake character (troll farm) intended to commit any of the offenses established in this Model Law commits a serious offense and shall be punished. It constitutes a more serious offense when the person or victim is a minor, as they are a particularly vulnerable population.

Article 10. Offenses related to the use and dissemination of unlawful content through artificial intelligence systems

(i) Whoever uses a deepfake or synthetic image, video or content generated through an artificial intelligence system used intentionally and without right, including anyone who promotes, manufactures, distributes, exhibits, offers, markets, advertises, publishes, imports, exports, sells, handles or otherwise makes available an intimate image of a person by means of an information and communications technology system without the explicit consent of the person depicted in the image, intending to cause harm, including psychological, financial, or reputational harm, or to make profits, shall be punished. It constitutes a more serious offense when the person or victim is a minor, as they are a particularly vulnerable population.

(ii) Whoever uses a deepfake or a synthetic image, video or content generated through an artificial intelligence system used intentionally and without right, including anyone who promotes, manufactures, distributes, exhibits, offers, markets, advertises, publishes, imports, exports, sells, handles or otherwise makes available an intimate image of a person by means of an information and communications technology system without the explicit consent of the person depicted in the image, intending to cause reputational harm to a candidate for an official position, or to use manipulative techniques to persuade persons to engage in unwanted behavior, or to try to influence an electoral process or electoral campaign, shall be punished.

(iii) Whoever uses a deepfake or a synthetic image, video or content generated through an artificial intelligence system used intentionally and without right, including anyone who promotes, manufactures, distributes, exhibits, offers, markets, advertises, publishes, imports, exports, sells, handles or otherwise makes available an intimate image of a person by means of an information and communications technology system without the explicit consent of the person depicted in the image, intending to induce, provoke or give reason to a State to declare war, shall be punished.

(iv) Whoever uses a deepfake or a synthetic image, video or content generated through an artificial intelligence system used intentionally and without right, including anyone who promotes, manufactures, distributes, exhibits, offers, markets, advertises, publishes, imports, exports, sells, handles or otherwise makes available an intimate image of a person by means of an information and communications technology system without the explicit consent of the person depicted in the image, intending specifically to engage in public glorification or justification of those who have participated in offenses related to terrorism, or of those who have participated in their execution, or in the commission of acts discrediting, belittling or humiliating the victims of terrorist offenses or their relatives or families, shall be punished.

(v) It constitutes a serious offense when the crime is committed on the basis of gender.

(vi) It constitutes a serious offense when the person or victim is a minor, as they are a particularly vulnerable population.

(vii) Whoever uses a deepfake or a synthetic image, video or content generated through an artificial intelligence system used intentionally and without right, including anyone who promotes, manufactures, distributes, exhibits, offers, markets, advertises, publishes, imports, exports, sells, handles or otherwise makes available an intimate image of a person by means of an information and communications technology system without the explicit consent of the person depicted in the image intended for deepfake manipulative or deceptive purposes, with the objective or effect of materially distorting the behavior of a person or a group of persons by appreciably impairing their ability to make an informed decision, in order to alter or preserve the listed price of a financial security or instrument; obtain financial profit; alter the prices that would arise from free competition of products, merchandise, securities or financial instruments, services or any other moveable assets or real estate; assure themselves a dominant position on the market for such securities or instruments; set their prices at abnormal or artificial levels; endanger public health with medicines, health products or therapies and thus endanger the life or health of persons in such a way that it appears real, shall be punished.

(viii) Whoever designs, programs, implements, distributes, produces, sells, displays, offers or facilitates technologies for the sole purpose of the offences described in the previous paragraphs, commits a serious offense and shall be punished. This shall not include those dual-use technologies that can be used for good or lawful purposes, but only those technologies whose sole purpose is to engage in punishable conduct.

Article 11. Misuse of devices and platforms for criminal purposes

1. Whoever designs, programs, implements, distributes, produces, sells, displays, offers, or facilitates technologies for the purpose of committing any of the offenses established in

accordance with Articles 5 through 10 of this Model Law, with the purpose set forth in subsection (vi) of Article 10, commits a serious offense and shall be punished.
(a) The punishment may be extended to anyone who facilitates, enables or displays a device, including a program, application or platform designed or adapted primarily for the purpose of committing any of the offenses established in accordance with Articles 5 through 10 of this Model Law, including a password, access credentials, electronic signature or similar data by which the whole or any part of an information and communications technology system is capable of being accessed; with the intent that the device, including a program, application, password, access credentials, electronic signature, or similar data be used for the purpose of committing any of the offenses established in accordance with Articles 5 through 10 of this Model Law; and
(b) The possession of an item referred to in this article, with the intent that it be used for the purpose of committing any of the offenses established in accordance with Articles 5 through 10 of this Model Law shall be a criminal offense when committed intentionally and without right.
(c) Deliberately hosting a website, application or artificial intelligence system explicitly designed to commit one or more offenses established in this Model law shall also be punished.

2. This article shall not be interpreted as imposing criminal liability where the obtaining, production, sale, procurement for use, import, distribution or otherwise making available, or possession referred to in paragraph 1 of this article is not for the purpose of committing an offense established in accordance with Articles 5 through 10 of this Model Law, such as for the authorized testing or protection of an information and communications technology system. This shall not include those dual-use technologies that can be used for good or lawful purposes, but only those technologies whose sole purpose is to engage in punishable conduct.

Title VI. Organized crime

Article 12. Conspiracy and organized crime

1. Participation by any means whatsoever in an ‘organized criminal group’ whose purpose is to commit an offense using an artificial intelligence system or to make available an artificial intelligence system designed to commit an offense established in accordance with Articles 5 through 11 of this Model Law, shall be punished.
2. Participation in an ‘organized criminal group’ which uses or leverages artificial intelligence with a view to or with the purpose of amplifying their attacks, increasing their profits in a shorter time frame, or exploiting victims on a larger scale and committing a serious offense established in accordance with Articles 5 through 11 of this Model Law, shall be punished.

Title VII. Criminal liability

Article 13.

The following parties may be considered ‘the perpetrators’ of any of the offenses defined in the present Model Law:

(i) an individual or natural person who uses an artificial intelligence system for criminal and malicious purposes.

(ii) the supplier of an artificial intelligence system explicitly presented as intended for the commission of criminal offenses.

(iii) the importer of an artificial intelligence system designed for criminal and malicious purposes.

(iv) the distributor of an artificial intelligence system designed for criminal and malicious purposes.

(v) the integrator of an artificial intelligence system designed for criminal and malicious purposes.

(vi) the operator of an artificial intelligence system designed for criminal and malicious purposes.

(vii) legal entities on whose behalf or for the benefit of which any of the offenses contained in Articles 5 through 11 of the present Model Law were committed shall be held criminally liable.

(viii) legal entities on whose behalf or for the benefit of which an artificial intelligence system has been intentionally used, designed, promoted, integrated, or provided for the purpose of committing any of the offenses contained in Articles 5 through 11 of the present Model Law shall be held criminally liable.

(ix) the criminal liability of legal persons is not exclusive of the liability of natural persons, provided that the latter have intentionally participated in any way whatsoever in the commission of the offense.

(x) The complexity or autonomy of an artificial intelligence system cannot be an exemption from liability.

For the purposes of criminal liability, the generally recognized state of the art in the field of AI at the time of the facts shall be taken into due account, according to technical specifications, international standards, and common knowledge.

Title VIII. Incitement, aiding, abetting and attempt

Article 14.

(i) Any person who incites the commission of one of the offenses established in accordance with Articles 5 through 11 of the present Model Law shall be punished as the main perpetrator or as an author of the said offense.

(ii) Any person who has facilitated help or support to commit one of the offenses established in accordance with Articles 5 through 11 of the present Model Law shall be punished as the main perpetrator or as an author of the said offense.

(iii) Any person who becomes an accomplice in committing one of the offenses established in accordance with Articles 5 through 11 of the present Model Law shall be punished as the main perpetrator or as an author of the said offense.

(iv) Any person who attempts to commit one of the offenses established in accordance with Articles 5 through 11 of the present Model Law, and even any ‘attempt’ resulting from circumstances beyond their control, shall be punished as the main perpetrator or as an author of the said offense.

Title IX. Sanctions and measures

Article 15.

1. Each party shall introduce and adopt such legislative and other measures as may be necessary to ensure that the criminal offenses established in accordance with Articles 5 through 11 of the present Model Law are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
2. Each party shall ensure that legal persons held liable in accordance with Title VII Article 13 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions, fines or confiscation.

PART III. JURISDICTION

Article 16. International jurisdiction

1. This Model Law applies to any offense established in accordance with Articles 5 through 14 of this Model Law, when the offense is committed:
a. in its territory; or
b. on a ship or aircraft registered in [enacting country]; or
c. by one of its nationals if the offense is punishable under criminal law or, when the national resides or is located outside the territory where the crime was committed, if the person's conduct would also constitute an offense under a law of the country where the offense was committed.
d. against a victim or a number of victims who, at the time of the commission of the acts, had nationality or habitual residence in the [enacting country], and the offender has not been acquitted, exempted or sentenced abroad or at a competent international tribunal.

2. Each Party shall adopt such measures as may be necessary to establish jurisdiction over extraditable offenses pursuant to multilateral and bilateral extradition treaties and agreements they are party to.
3. This Model Law does not exclude any criminal jurisdiction exercised by a Party in accordance with its national law.
4. When more than one country claims jurisdiction over an alleged offense in accordance with Articles 5 through 14 of this Model Law, the Parties involved shall facilitate consultations with a view to determining the most appropriate jurisdiction for prosecution.

Article 17. Court jurisdiction

1. This Model Law applies to any criminal activity committed or assisted through an artificial intelligence system in the context of crime and organized crime. The following courts shall have jurisdiction:
a. in the courts where the victim is domiciled or has his or her habitual residence or at his or her choice, regardless of the domicile of the victim.

b. in the courts for the place where the perpetrator is domiciled or arrested. The perpetrator shall not be required to have an official headquarters, it is sufficient that there be a delegation or authorized representative to carry out commercial transactions on its behalf to be deemed to be the state of the domicile.
c. in the courts of the place where the harmful event occurred or may occur.
d. in the courts of the place where the police investigation may have some success, such as a place where elements of the crime took place, where computers can be operated and accessed, where the artificial intelligence system is stored, or where the data was used or produced by the artificial intelligence system, or where the content is published or where the illegal content is publicly accessible and where the investigation can be effective.

2. In the event of a conflict of jurisdiction between two or more courts [public prosecutors, investigative judge], a mechanism shall be established for resolving the conflict. Each court or representative of each court shall be invited to submit their opinion.
The Supreme Court shall have jurisdiction to resolve any conflict of jurisdiction that has not been resolved by mutual agreement between the courts [the public prosecutor] concerned.

3. In order to strengthen the capacities of the specialized jurisdiction [public prosecutor, investigative judge], under this Model Law, provisions shall be made (by decree) to provide training and expertise capacity development for judges and prosecutors in this field.

PART IV. PROCEDURAL LAW, VICTIMS AND MEASURES

Article 18. Procedural Law

Parties shall establish sufficient powers and procedures for the purpose of conducting specific criminal investigations or proceedings related to criminal offenses committed and assisted through the use of an artificial intelligence system in the context of organized criminal activities, including the collection and preservation of evidence arising from any criminal offense in electronic form, including the possibility for law enforcement authorities to freeze and neutralize artificial intelligence systems pursuant to Part V of this Model Law.

Article 19. Victims

The fundamental rights of victims of crimes involving the use of artificial intelligence, including their right to privacy, adequate information, support, free assistance, measures to prevent revictimization and effective protection, together with compensation following the conviction of the perpetrator or perpetrators of the crimes covered by this law, shall be guaranteed at all stages of the criminal proceedings. The competent authority shall be responsible for ensuring full respect for these rights.

Particularly vulnerable members of the population who are victims of crimes involving the use of artificial intelligence shall be subject to special protection, in particular children and adolescents.

For those purposes, victims shall receive online assistance to file a complaint and guidance in preserving or identifying clues or evidence, and submitting them to the competent authorities. Subsequently, victims shall be kept informed of the details of their complaint and the outcome, and are invited to participate in the rest of the procedure until the final decision, including by facilitating gathering of evidence, enabling prosecution, claiming compensation, and avoiding revictimization.

Evidence collected cannot be declared inadmissible because it was submitted online by the victim to the competent authorities.

Article 20. Liability of the providers, suppliers and distributors of the AI system, those responsible for deployment, the authorized representative, and the importers of the AI system

Regarding the liability of the providers, suppliers and distributors of the AI system, those responsible for the deployment, the authorized representative and the importers of the AI system shall not be responsible for the mere transmission, access, hosting, or storage of the information. Nor can providers be required to monitor information or actively search for facts or circumstances that indicate the existence of illegal activities.
Providers, suppliers and distributors of the AI system, those responsible for the deployment, the authorized representative and the importers of the AI system shall not be liable for the commission of crimes established in accordance with Articles 5 through 11 of the present Model Law, by using or assisting their systems when:
(a) They do not have effective knowledge that the activity or information stored is unlawful or that it infringes the property or rights of a third party that may be subject to compensation; or
(b) They do have effective knowledge but act diligently and promptly to remove the data or the AI system or make it impossible to access it by blocking it.
For effective knowledge, it will be sufficient for the borrower and other operators to acquire knowledge, in one way or another, as a result of an investigation carried out on their own initiative or notified to them by administrative, police and/or judicial authorities, without the need for judicial authorization. All this shall be without prejudice to the procedures for detecting and removing content that providers and other operators apply by virtue of voluntary agreements and other means of effective knowledge that may be established, including other means of effective knowledge, even if it is mediated or by logical inferences.

In order to effectively report allegedly illicit artificial intelligence-generated content, judicial, police or administrative authorities shall indicate:
(i) a reference to the legal basis in international or national law.
(ii) a statement of reasons explaining why the information is illegal content, referring to one or more legal provisions.
(iii) identification to the issuing authority.
(iv) clear information that allows the illegal content in question to be identified and located.
(v) information on redress mechanisms.
(vi) information about which authority should receive the information.

For risk mitigation or reparation of damage, it may help when providers initiate investigations in good faith and diligently on their own initiative without prior effective knowledge and voluntarily, or take measures to detect, identify, remove, or block access to illegal content.

Article 21. Expedited preservation of data

(i) The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute and adjudicate the offenses established in accordance with Articles 5 through 11 of the present Model Law are competent to obtain the expedited preservation of data, including the artificial intelligence system, the processing of data, the results of the processing of data by an artificial intelligence system compromised or involved in the commission of one of the aforementioned offenses.

(ii) The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute, and adjudicate the offenses established in this Model law are competent to access and seize any server, storage medium, database likely to support or process all or part of the data and software involved in the compromise of an artificial intelligence system or involved in the commission of one of the aforementioned offenses by such artificial intelligence system.

(iii) The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute, and adjudicate the offenses established in this Model Law are competent to issue a production order to access and seize any server, storage medium or database likely to support or process all or part of the data and software involved in the compromise of an artificial intelligence system or involved in the commission of one of the aforementioned offenses by such artificial intelligence system.

(iv) The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute and adjudicate the offenses established in this Model Law are competent to issue a request to a supplier, host, developer, promoter or any entity or person likely to be able to access the data, storage medium or source codes allowing the seizure of data useful for the investigation, prosecution or adjudication of the offenses provided in this Model Law.

(v) The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute and adjudicate the offenses established in this Model Law are competent to issue a request for the purpose of intercepting a data flow emanating from an artificial intelligence system involved in the commission of offenses provided for in this law.

Article 22. Expedited preservation and partial disclosure of traffic data

The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute and adjudicate the offenses established by this Model Law may order the expedited preservation and disclosure of traffic data when one or more service providers were involved in the transmission of the communication, and ensure the expeditious disclosure to a competent authority of a sufficient amount of traffic data to enable the competent judicial authority to identify the service providers and the path through which the communication or indicated information was transmitted.

Article 23. Production order

The competent judicial authorities [public prosecutor, investigative judge] may order:
(a) A person or an entity in their territory to submit specified electronic data in that person's possession or control that is stored in an information and communications technology system or an electronic data storage medium; and
(b) A service provider offering its services in the territory of the judicial authority to submit subscriber information relating to such services in that service provider's possession or control.

Article 24. Search and seizure

(1) If a [judge] [magistrate] is satisfied based on [affidavit] that there are reasonable grounds to believe, supported by circumstances sufficiently strong to justify, that there may be in a place a computer system, an artificial intelligence system or relevant data contained therein:
a. that may be material as evidence in proving an offense; or
b. that has been acquired by a person as a result of an offense.
The magistrate shall issue a warrant authorizing a [public prosecutor] [law enforcement] officer, with such assistance as may be necessary, to enter the place to search and seize the computer system, artificial intelligence system or relevant data contained therein, including to search or similarly access:
i. a computer system, an artificial intelligence system or part of it and computer data stored therein; and
ii. a computer data storage medium in which computer data may be stored in an artificial intelligence system in the territory of the country.

(2) If a [law enforcement] [police] officer that is undertaking a search based on procedural law has grounds to believe that the data sought is stored in another computer system or an artificial intelligence system or part of it in its territory, and that such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search request or similarly gain access to the other system.

(3) A [law enforcement] [police] officer who is undertaking a search is empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2.

Article 25. Lack of cooperation of AI providers and platforms

In all cases where the recipient, without legitimate reason, refuses to provide, or does not provide the requested data, does not provide it in full, or does not provide it within the specified time-frame, the recipient shall inform the issuing authority of these reasons, without undue delay and as soon as possible [within 48 hours], and, where notification has been given to the implementing authority, the implementing authority referred to in the injunction. The issuing authority shall review the injunction in light of the information provided by the recipient and, if necessary, set a new deadline for the recipient to produce the data.

In the event of failure to provide the data or refusal to provide it, the court [public prosecutor, investigative judge] may impose a fine or administrative sanctions.

Article 26. Assistance and cooperation

(i) The offenses established in this Model Law constitute a legal basis for requesting the extradition of any person who has participated directly as an author, co-author, or accomplice in one of the offenses established in this Model Law, subject to prosecution seeking a sentence of at least 2 years and to the principle of dual criminality. The authorities shall afford other countries mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to this Model Law.

(ii) The offenses established in this Model Law constitute a legal basis for requesting mutual legal assistance for investigation or prosecution, subject to the principle of dual criminality.

Article 27. Joint investigation teams

The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute, and adjudicate the offenses established in this Model law are competent to conclude, implement and direct joint teams to combat 'organized criminal groups' using AIS.

Where appropriate, the members of the joint investigation team are competent to exchange, share and make available to other members clues and evidence collected within the framework of the joint investigation team by one of the members of this team, without it being necessary to resort to international mutual assistance in criminal matters.

Article 28. Procedural safeguards

The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute and adjudicate the offenses established in this Model Law shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Model Law are subject to conditions and procedural safeguards provided for under its domestic law, which shall include the adequate protection of human rights and liberties pursuant to international and regional conventions on human rights, and shall incorporate the principles of necessity and proportionality, including the limitation of the scope and duration of such power or procedure.

Article 29. Freezing and confiscation

1. The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute, and adjudicate the offenses established in this Model law shall be empowered to take the necessary measures to enable the freezing [or seizure] of any property of any

description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title or interest in such property, which shall be considered to be the proceeds of a criminal offense, or its equivalent, whether the full amount of the value or only part of the value of such proceeds or the instrumentalities of a criminal offense, or the value of such instrumentalities, in order to prevent the destruction, transformation, removal, transfer or disposal of property with a view to the confiscation thereof.

2. The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute, and adjudicate the offenses established in this Model law shall be empowered to take the necessary measures to enable the confiscation of all or part of the instrumentalities and proceeds, or of property whose value corresponds to that of those instrumentalities or proceeds, subject to a final conviction for a criminal offense, which may also have been handed down in absentia.

3. Where confiscation is not possible based on paragraph 2, the judicial authorities [public prosecutor, investigative judge] shall be empowered to take the necessary measures to enable the confiscation of instrumentalities or proceeds in cases where criminal proceedings have been initiated concerning a criminal offense that is likely to give rise, directly or indirectly, to an economic advantage and where those proceedings would have been likely to result in a criminal conviction if the suspect or accused person had been able to appear in court.

4. The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute, and adjudicate the offenses established in this Model law shall be empowered to take the necessary measures to allow for the confiscation of all or part of the property belonging to a person convicted of a criminal offense from which an economic advantage may be derived, directly or indirectly, where a court, based on the circumstances of the case, including concrete factual elements and available evidence, such as the fact that the value of the property is disproportionate to the lawful income of the convicted person, is satisfied that the property in question is derived from criminal activities.

PART V. INTERNATIONAL PUBLIC-PRIVATE COOPERATION

Article 30. Cooperation with criminal justice authorities

(i) The judicial authorities [public prosecutor, investigative judge] competent to investigate, prosecute and adjudicate the offenses established in this Model Law, and artificial intelligence providers, deployers, importers, distributors, operators or any other relevant entity or party involved in the creation, deployment, functioning or management of an artificial intelligence system, shall facilitate immediate cooperation in good faith when a crime has been committed or assisted through an artificial intelligence system, including when a deepfake has been used to commit or perpetrate any of the offenses established in accordance with Articles 5 through 11 of this Model Law.

(ii) Each party shall introduce and adopt such legislative and other measures as may be necessary to ensure that artificial intelligence providers, deployers, importers, distributors, operators or any other relevant entity or party involved in the creation, deployment, functioning and management of an artificial intelligence system, cooperates under a legal mandate establishing fines in case of non-compliance or lack of cooperation with the competent judicial authorities [public prosecutor, investigative judge] responsible for the investigation, prosecution and adjudication of any of the offenses established in this Model Law.

(iii) Each party shall ensure that legal persons held liable in accordance with Article 13 shall be subject to effective, proportionate, and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions and fines.

Article 31. Technical and material assistance and artificial intelligence literacy

1. Each party is strongly encouraged to make concrete efforts, to the extent possible and in coordination with each other and with international and regional organizations:

(i) To enhance their cooperation at various levels with other countries, with a view to strengthening their capacity to prevent and combat criminal offenses established in accordance with Articles 5 through 11 of the present Model Law.

(ii) To provide technical and material assistance to other countries in effectively preventing and combating the offenses covered by this Model Law, by providing continuous training, capacity building programs and skills to assist them in achieving the purpose and objectives of this Model Law.

(iii) To exchange best practices and information with regard to activities undertaken, with a view to avoiding duplication of efforts and making best use of capacity building and training programs in the area of AI and crime, and to stimulate discussion on problems of mutual concern, including particular challenges and needs of countries of LAC.

2. Providers and deployers of artificial intelligence systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, in particular regarding crimes committed or assisted through AI, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

EL PACCTO

2.0 EU-LAC Partnership on justice and security