The MEDICRIME Convention
La Convention MÉDICRIME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 20 March 2025

T-MED (2025) 03

# Preliminary draft report

# The MEDICRIME Convention in the Age of AI: Challenges and Opportunities

**prepared by**

**Prof. Fernando MIRÓ LLINARES**

**CRIMINA Center, University Miguel Hernández of Elche (Spain)**

Directorate General I – Human Rights and Rule of Law

## TABLE OF CONTENTS

# THE MEDICRIME CONVENTION IN THE AGE OF AI: CHALLENGES AND OPPORTUNITIES

## 1. Introduction

### 1.1. Objectives and methodology of the preliminary draft paper

The advent of artificial intelligence (AI) in contemporary society is profoundly and rapidly transforming multiple sectors, generating impacts of a magnitude that is difficult to compare with any other recent technological innovation. In the field of health, particularly concerning the manufacturing, distribution, and commercialization of medicines and other medical products, AI -combined with the widespread use of social networks and other digital technologies- is introducing new dynamics in both production and commercialization in digital environments. These transformations create opportunities in terms of efficiency, quality control, and access to healthcare, but they also pose unprecedented regulatory challenges, particularly regarding the proliferation of illegal activities linked to the counterfeiting of medical products, the illegal trade in medicines, and other behaviors that endanger public health.

The MEDICRIME Convention of the Council of Europe constitutes the primary international regulatory framework aimed at combating the counterfeiting of medical products and other related crimes that compromise public health. Its objective is to establish a common legal framework for the criminalization of such behaviors, ensuring regulatory harmonization and international cooperation mechanisms that enable an effective response to the threats they pose to global health security. However, the emergence and consolidation of AI as a disruptive technology require a rigorous analysis of its implications for the effectiveness of the treaty, as it may significantly alter both the commission methods of the crimes covered by MEDICRIME and the tools available for their prevention, detection, and prosecution.

This paper aims to evaluate the impact that AI, in its interaction with the growing digitalization of the medical and pharmaceutical product trade, may have on the applicability and relevance of the MEDICRIME Convention. This analysis is structured around two fundamental and sequential objectives. The first is to explore to what extent AI is transforming the behaviors that the treaty seeks to sanction, recognizing that these criminal practices do not emerge in isolation but within a digitalization process that has evolved over decades and was accelerated after the COVID-19 pandemic. The advent of the internet facilitated the transnational commercialization of medical products without adequate control. Social networks exponentially expanded access to illicit markets through platforms that became even more popular during lockdowns, allowing direct interaction between suppliers and consumers without regulatory intermediaries. Finally, AI has introduced automation and sophistication mechanisms in the generation, distribution, and commercialization of counterfeit products, challenging traditional control strategies. At the same time, AI also offers interesting opportunities for detecting counterfeit products and monitoring their sale, although doing so will require addressing new key players, such as digital service providers. Understanding this context is essential for tackling the second objective of this paper: examining the potential repercussions of these changes on the structure and effectiveness of the MEDICRIME

Convention, analyzing to what extent the treaty's current provisions remain adequate to address these new threats and whether modifications may be necessary to reinforce its applicability in an AI-dominated environment.

The methodology adopted in this analysis combines a legal-normative approach, focusing on the study of the MEDICRIME regulatory framework and its interaction with technological evolution, with a criminological and criminal policy perspective that assesses how changes in criminal dynamics impact the instrument's effectiveness. To achieve this, recent studies on the impact of AI on illicit markets, reports from international organizations, and other bibliographic sources are considered to offer a well-founded diagnosis of the challenges and opportunities posed by artificial intelligence in this field. For the legal analysis, specialized literature is reviewed, and documents such as the "Criminalization of AI-related Offences" report, which examines in general the challenges posed by artificial intelligence in the field of criminal law, are taken into account. This report addresses the need to adapt current legislation to tackle AI-related crimes and identifies the most suitable legislative techniques to achieve this goal.

This paper provides a foundation for reflecting on the need to update, reinterpret, or strengthen the provisions of MEDICRIME considering emerging challenges associated with AI, thereby contributing to the development of a more robust regulatory framework adapted to the complexities of the digital age that can effectively protect public health against new forms of transnational crime that already employ and will increasingly employ this technology.

### 1.2. Definition of AI and scope of the technology considered for this document

For the purposes of this document, Artificial Intelligence (hereinafter AI) is understood as "*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 may influence physical or virtual environments*." We use the definition adopted by the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (hereinafter, CAI) of the Council of Europe, specifically the one contained in Article 2 of that instrument, which further states that "*Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment.*"

From this definition, some fundamental features of AI systems can be identified that are particularly relevant in analyzing the impact of this technology on the MEDICRIME Convention. The definition recognizes the existence of different levels of autonomy and adaptability in AI systems, which, in turn, requires that this idea of "autonomy" be considered. This implies acknowledging a fundamental distinction between computer systems or machines that operate strictly according to predefined rules and those that can modify their behavior based on context and the information they receive after deployment.

Only the latter -those that possess processing capabilities allowing their behavior to adapt based on the data they process, rather than purely reactive or preprogrammed systems- will be considered AI. This is because the ability to operate with some degree

of independence and modify performance based on processed data is what makes AI both an opportunity and a challenge from a regulatory and legal perspective. This, in turn, necessitates a specific analysis of its impact on the crimes that the MEDICRIME Convention seeks to prevent and punish.

Within these concerns, this document will focus particularly on generative AI systems, Large Language Models (LLMs), and other advanced architectures, which have demonstrated a growing ability to produce new content, imitate patterns of human language and imagery, and generate outputs that can be used for both lawful and unlawful purposes. LLMs, such as ChatGPT, Gemini, Claude, or DeepSeek, are deep learning models trained on massive volumes of textual data, capable of generating coherent and contextually appropriate responses based on the input provided. Their application in various fields has led to significant advancements in multiple tasks, but it has also opened the door to risks such as the automated generation of fraud or the creation of false information that is difficult to distinguish from real content (Deep Fakes).

Analyzing their impact on the MEDICRIME Convention will be key to assessing the extent to which this technology can facilitate the counterfeiting of medical products, the spread of health-related misinformation, or the automated production of fraudulent documentation. This evaluation will also determine what regulatory adjustments may be necessary to address these challenges.

Finally, it is important to note that, at present, the most advanced AI applications correspond to what is known as Narrow AI—highly specialized systems that allow the automation of specific tasks within a defined domain but lack general reasoning abilities or contextual understanding beyond the data they were trained on. In the near future, it is possible that Strong AI systems or even forms of artificial superintelligence may be developed, which could pose completely new challenges both from the perspective of the behaviors that MEDICRIME seeks to prevent and from the standpoint of criminal law itself. However, the focus of this document will remain on AI technologies that are already present in the market and that pose immediate risks and opportunities for the application of the treaty, while also considering foreseeable developments within the scope of the CAI definition.

## 2. The new challenge that AI will pose for the counterfeiting and trafficking of medical products

### 2.1. Digitalization and counterfeiting of medical products in the age of AI: state of the art

#### 2.1.1. The current digital ecosystem and the counterfeiting of medical products

In recent decades, the trade in medical products has experienced unprecedented growth and transformation, driven by digitalization on one hand and the globalization of markets on the other. The combination of these two phenomena has facilitated access to medicines and medical devices from anywhere in the world, which, at the same time, has created new opportunities for the proliferation of counterfeit products.

The digital ecosystem has become a key environment for the illicit distribution of counterfeit medicines, as it offers multiple tools and platforms that allow criminal actors to operate with a high degree of anonymity and an unprecedented capacity for expansion. This blurs the traditional boundaries of illegal trade in these products and hinders the effective application of control and oversight mechanisms. This trend appears to have increased following the COVID-19 pandemic, due to the acceleration of digitalization that followed because of lockdown measures. Many social processes have become digitalized, and citizens have begun to trust online commerce much more than before. Social networks seem to play a crucial role in the marketing and distribution of these counterfeit medical products, allowing illicit sellers to use advanced segmentation strategies to target specific consumers with advertisements, without the need to resort to traditional markets or physical distribution channels. Platforms such as Facebook, Instagram, TikTok, and Telegram have been used by criminal networks to promote fraudulent products through personalized ads, fake comments, and manipulated testimonials, which generate trust among consumers. Even though these digital spaces should be moderated and have advertisement supervision mechanisms using AI algorithms, many of these illegal offers manage to bypass the platforms' internal controls and reach thousands of users in a matter of minutes.

Another key element in this ecosystem is the growing use of cryptocurrencies and digital payment platforms, which has facilitated illicit transactions by offering decentralized payment methods that do not require users to reveal personal or financial information. This significantly reduces the risk of detection and allows criminals to operate without leaving traces in traditional banking systems. By using Bitcoin, Monero, and other cryptocurrencies, sellers can receive money from buyers in different parts of the world without relying on financial intermediaries. This not only makes it more difficult to identify counterfeit drug trafficking networks but also prevents the traceability of transactions and the application of control measures over these financial flows.

The emergence of AI in this context has introduced an additional layer of complexity, as this technology allows for the automation of multiple processes related to counterfeiting, distribution, and commercialization of fraudulent medical products. AI can optimize market strategies and maximize the reach of criminal networks. As AI continues to improve and become more widely available at a low cost—which is already happening—and as it integrates further into social networks, advertising algorithms, and digital commerce platforms, its use by criminal groups to facilitate these offenses will become increasingly relevant. This will pose new challenges for regulatory frameworks and international cooperation instruments in the fight against the trafficking of counterfeit medical products.

### 2.1.2. AI as an enabling technology for counterfeiting medical products

One of the most concerning aspects of AI's emergence in the field of medical product counterfeiting is its potential to facilitate the production of fraudulent medicines and healthcare devices with an unprecedented level of sophistication. Traditionally, counterfeiting medicines that appeared authentic required manual or low-tech industrial processes, which limited the quality of the copies and made them easier to identify for

health authorities. However, with advances in AI and automation techniques, counterfeiters now have access to tools that allow them to precisely replicate both the appearance and the chemical composition of original medical products, reducing detection possibilities and increasing public health risks.

Firstly, generative AI models can be used to design fake labels, packaging, and certifications with a level of detail that makes them virtually indistinguishable from legitimate products. Image processing algorithms allow the scanning and replication of official documents with such precision that traditional verification techniques become ineffective, facilitating the introduction of counterfeit medicines into the market without raising suspicion. Moreover, these models are also capable of generating fake QR codes, security holograms, and other authentication mechanisms that mimic legitimate manufacturers' verification systems.

Secondly, AI can be used to optimize chemical synthesis and pharmaceutical production processes, allowing counterfeiters to develop compounds with an appearance and consistency like authentic medications, even though they fail to meet quality and safety standards. Machine learning models can analyze pharmaceutical databases to identify combinations of active ingredients that mimic the effects of a legitimate drug without using the original components. This would not only reduce production costs but also make fraud detection more difficult in standard quality control tests.

Another worrying application of AI in this field is its ability to automate marketing and distribution strategies using bots and ad optimization systems on social media and digital commerce platforms. Segmentation algorithms can identify vulnerable populations who are more likely to purchase medicines online without verifying their authenticity, facilitating the highly targeted promotion of counterfeit products. Additionally, AI systems can automatically generate hundreds or thousands of fake profiles on social networks to post positive reviews, answer potential customer inquiries, and reinforce the perception of legitimacy of illicit sellers.

### 2.1.3. AI as a potential tool for detecting counterfeit medical products

While artificial intelligence has proven to be a technology that facilitates the counterfeiting of medical products, it also offers enormous potential as a detection and control tool, allowing health authorities, regulatory bodies, and digital platforms to improve their ability to identify and remove fraudulent products before they reach consumers. This is the dual-use nature of such technologies.

Through the use of algorithms, big data analysis techniques, and machine learning models, AI can play a key role in the fight against counterfeit medicines and healthcare devices. In fact, the European Medicines Agency (EMA) recently published a Reflection Paper on the Use of Artificial Intelligence (AI) in the Medicinal Product Lifecycle, which, although it does not directly address the impact of AI on counterfeit drug trafficking or the application of MEDICRIME, raises relevant issues regarding the potential use of this technology for traceability and pharmacovigilance. In particular, the document states that AI can play a role in identifying counterfeit medical products by monitoring supply chain patterns and detecting anomalies in distribution. There are key sections in this document

that could be relevant to this area (Section 2.2.7). Furthermore, in Section 2.2.6, it points out that the use of AI in the manufacturing and distribution of medicines could contribute to improving the traceability and security of pharmaceutical products. The EMA has acknowledged some of the main potential applications of AI in this field, for example:

- Automated detection of suspicious patterns on digital commerce platforms and social media. Deep learning algorithms can analyze large volumes of data in real-time to identify listings of medical products with atypical characteristics, such as prices that are too low, inconsistent locations, or altered images.

- Analysis of metadata and interaction networks on social media, which allows tracking the activity of illicit sellers and mapping connections between different actors in the black market for medicines.

- Combining blockchain and AI algorithms to improve supply chain traceability, enabling authorities to verify product authenticity at every stage of the distribution process. By integrating neural networks and decentralized ledger technology, it becomes possible to track the origin and history of each medicine, ensuring that only legitimate products enter the market and facilitating the detection of vulnerabilities in the distribution chain. Blockchain also ensures data integrity and protects patient-sensitive information, reducing the risk of manipulation and ensuring that only authorized parties have access to critical data.

Lastly, AI can also be used in medicine authentication at the consumer level, through the development of mobile applications that allow users to scan security codes and verify in real-time whether a product is legitimate or has been reported as counterfeit. These applications can leverage computer vision and natural language processing techniques to interpret labels, detect irregularities, and alert consumers to potential risks.

## 2.2. Generative AI and the emergence of new medical devices

So far, AI has been analyzed as a tool for the counterfeiting of medical products, but the current practical development of this technology also forces us to consider the possibility that AI itself may become a medical product and an object of fraud. As already described in the literature, the emergence of AI-based chatbots is transforming the healthcare sector, with applications in medical diagnosis, patient assistance, and health education. Currently, tools such as ChatGPT and other medical chatbots are being used to answer patient questions, provide medical information, and assist in the management of chronic diseases such as diabetes. AI-based chatbots are already being used in the healthcare sector for multiple purposes, ranging from patient care to diagnosis and medical record management.

As highlighted by Loh (2023), existing medical chatbots are classified into three main categories:

- Informational chatbots, used to improve health literacy by providing information about diseases, symptoms, and treatments.

- Diagnostic chatbots, which assist doctors in preliminary diagnoses and medication management, rather than replacing clinical judgment.

- Administrative chatbots, which support appointment scheduling, medical record creation, and optimization of healthcare professionals' time.

The evolution of technology suggests that current medical chatbots may develop into regulated medical products focused primarily on diagnosis and treatment of chronic diseases. Although these systems currently act mainly as assistants, in the future, they could be considered medical devices if they autonomously integrate into clinical decision-making. For this to happen, they would need to meet strict regulatory requirements in terms of safety, reliability, diagnostic accuracy, and other medical ethics considerations. In fact, in the United States, the FDA (Food and Drug Administration) has begun to classify certain AI systems as Software as a Medical Device (SaMD), which means that, depending on their function, some chatbots could be regulated as medical devices.

To be considered a regulated medical device, an AI system must: demonstrate precision and reliability in its responses, especially if it offers diagnoses or treatment recommendations; pass clinical trials that validate its effectiveness in medical practice; ensure the privacy and security of patient data. It is, therefore, not unreasonable to expect that AI-powered products will seek regulatory certification from agencies such as the FDA in the U.S. or the EMA in the European Union. These certifications could soon be obtained, leading to an even deeper integration of AI-based systems into healthcare services.

## 3. MEDICRIME in the new scenario shaped by AI

### 3.1. A preliminary issue: AI, criminal liability, and criminalization techniques

The MEDICRIME Convention of the Council of Europe aims to combat the counterfeiting of medical products and other activities that threaten public health by promoting the harmonization of criminal laws and international cooperation. It is, therefore, an international legal instrument focused on criminal law, which, among other provisions, requires the criminalization of certain behaviors and their proportional and dissuasive punishment.

For this reason, before analyzing whether the MEDICRIME Convention needs to be adapted to address AI-related challenges, it is important to understand how AI may affect not only specific counterfeiting-related offenses but also the criminal justice system.

Beyond the potential transformations that criminal law could experience with the emergence of truly autonomous and intelligent entities (in a moral sense) when Strong AI develops, the current Weak AI and the new criminal dynamics derived from its use and development already present significant challenges for criminal liability. Traditional categories and models of criminal responsibility need to be reassessed and adapted to these new technological realities. Therefore, before delving into the specific subject of study, it is essential to understand the broader changes that AI could bring about, making this an important preliminary consideration.

To determine whether the current systems of criminal liability attribution, such as those adopted by the MEDICRIME Convention, are adequate to address these situations or if they require modifications to ensure proper attribution of responsibility, it is necessary to identify the uniqueness of the technology that may strain the foundations of the criminal justice system. AI systems promise an optimization of decision-making processes by reducing human bias and improving efficiency in information management through automation and the partial or total delegation of certain functions to machines.

This entails two things:

1. AI could be shifting the key moment in which criminal liability is determined: Instead of being placed at the moment when harm or risk occurs, liability attribution may need to be analyzed at earlier stages in the AI lifecycle, such as its design and the training of algorithms.

2. The progressive automation of processes through AI poses the risk of gaps in criminal liability in cases where systems act autonomously and unpredictably.

Although these systems do not possess moral autonomy, they can operate with a certain degree of functional independence, which means that, in certain scenarios, the effects of their actions may be unpredictable both for users and developers. The difficulty of assigning criminal liability to human beings when AI systems have played a significant role in the causal process of harm demands, according to some authors, a comprehensive review of the liability attribution system, while others argue that current regulations are sufficient and that the obligation of control and oversight by designers and users must be reinforced to avoid regulatory loopholes.

It is evident, in any case, that the shift of human agency to earlier phases of the AI lifecycle implies that criminal liability must be evaluated at the design and production stages of these technologies, as it is in these moments where the most significant risks can be prevented. The possible criminalization of preparatory acts or violations of administrative duties related to the development and deployment of high-risk AI systems is presented as a viable alternative to prevent situations in which those responsible cannot be sanctioned once harm has occurred. Thus, the omission of supervision over systems that operate with a high degree of autonomy or the lack of adequate controls over AI could be subject to criminal penalties when they generate a concrete risk to legally protected interests, which would require clearly defining the supervision duties imposed on those who design, train, and deploy these systems.

However, the adoption of such criminal provisions must ensure that the prohibition of certain technologies does not violate the principle of legality or hinder the legitimate development of artificial intelligence for lawful purposes. Therefore, it will be necessary to precisely define which uses of AI are considered unacceptable and justify their criminalization in terms of proportionality and necessity.

Another major change that criminal law must address is the expansion of criminal liability for negligence in relation to AI use, given that in many cases, harm will not be caused

intentionally, but rather because of failures in the design, implementation, or oversight of these systems. This will require a reformulation of the types of negligence in criminal law to contemplate situations where the individual has not directly caused harm but has acted negligently in managing the risks inherent in AI use. It will be essential to define with precision the diligence standards that should be required of the various actors involved in the development and application of this technology. The imposition of specific duties of diligence in relation to AI will ensure that criminal liability for negligence is not restricted only to situations where the individual had direct control over the action, but can extend to those who, due to their role in designing and managing the system, have incurred failures that make the production of a harmful outcome foreseeable.

However, it is evident that when an AI system is maliciously designed for the commission of a criminal act, just as when AI is used knowingly and willingly to commit an offense, the use of this technology does not require any modification to the criminal liability system.

Another issue to analyze is whether AI, due to its ability to automate decision-making processes, act autonomously, and replicate actions at high speed, amplifies the scale of harm caused by its use, increasing the magnitude of the damages that may result from its application. The use of AI can lead to a single harmful action affecting a much greater number of victims, generating more severe consequences in terms of protected legal interests. Criminal law can adopt various techniques to respond appropriately to this:

- The creation of new criminal offenses specifically aimed at sanctioning high-risk behaviors associated with AI use, which would allow for early intervention to prevent the materialization of large-scale harm.

- Adapting the penalties of existing offenses to reflect the greater severity that AI use may entail.

However, these options must be approached with caution. It is not about assuming that all AI applications inherently pose greater risks, but rather about evaluating in which contexts and under what circumstances its use generates a sufficient threat to justify an increase in criminal response. This evaluation must be carried out based on factors such as: the nature of the protected legal interest, the foreseeability of harm, the degree of control that human operators have over the system, and the level of autonomy of the system in decision-making. In areas where the impact of AI on particularly sensitive legal interests, such as public health, is significant, stricter sanctioning mechanisms could be established, as long as they remain necessary and proportionate.

Finally, AI will also lead to an increased importance of corporate criminal liability, since many of the unlawful activities associated with this technology will not be attributable to a specific individual, but rather to organizations that implement it without the necessary security and transparency guarantees. Criminal law regulations must include due diligence standards that impose specific obligations on companies that develop, market, or use AI in their processes, establishing self-regulation mechanisms under penalty of criminal sanctions when internal controls are insufficient to prevent offenses. In this context, corporate criminal liability must be adjusted to cover situations in which AI is

fraudulently used within an organization without a clearly identifiable individual perpetrator. This will require redefining the criteria for attributing corporate criminal liability in relation to AI risk management.

In conclusion, the emergence of artificial intelligence in criminal law not only demands adaptations to existing regulations, but also raises fundamental challenges in terms of proportionality, precision, and responsibility attribution. The criminalization of AI-related offenses will require the creation of new offenses, the reformulation of existing criminal provisions, and the imposition of specific supervisory and diligence obligations regarding AI use. Legislators will need to strike a balance between risk prevention and the protection of fundamental rights. To face these challenges, criminal law must apply the best legislative techniques, ensuring that deterrent effectiveness is maintained while also preserving the fundamental guarantees of criminal law.

Now is the time to analyze how this can be done in relation to MEDICRIME.

### 3.2. An opportunity for MEDICRIME: its renewed relevance in the wake of AI

The emergence of artificial intelligence in the counterfeiting of medical products poses an additional challenge for the MEDICRIME Convention, as it requires a review of its validity and relevance within the new context shaped by AI. However, to some extent, it also reinforces the convention, making even more evident its role as a key instrument in the fight against these crimes. As we have seen, AI will enhance the sophistication of counterfeiting, facilitating the production of copies that are practically indistinguishable from original medicines, the creation of fraudulent documentation, and the automated distribution of these products on a global scale.

This scalability and automation capacity would allow criminal groups to operate with greater impunity and make law enforcement efforts more difficult. In this regard, the MEDICRIME Convention, which requires States to criminalize these acts and promotes international cooperation in their prosecution, becomes even more relevant. National regulatory mechanisms increasingly appear insufficient in the face of this global threat, making it essential to establish a joint and coordinated framework among States to address these risks. A similar argument can be made regarding the potential use of AI to detect illicit distribution patterns, analyze large volumes of data in digital markets, and track suspicious cryptocurrency transactions. Undoubtedly, this technology could be used to improve the States' prevention and response capacity, but this would be even more effective if these tools were integrated into the cooperation mechanisms provided by the Convention in such a way that signatory countries could anticipate new forms of criminality and develop more effective strategies against the counterfeiting of medical products.

What is clear, in any case, is that for MEDICRIME to be successful in a digitized technological context such as the one described, a significant increase in the number of signatory countries would be necessary, especially among those where the need to prevent these behaviors is most evident. For example, as will be discussed later, the possibility of requiring service providers to integrate AI-based tools into their algorithms

to detect and remove advertisements for counterfeit medicines will become more feasible as more countries sign the Convention and exert pressure on these companies.

### 3.3. On potential reforms and changes in MEDICRIME

After analyzing the digital technological landscape in which the counterfeiting of medicines and other medical products currently takes place and having examined the key aspects of AI's impact on criminal law in general, it is now time to consider whether MEDICRIME may require some adaptation, either through a modification of its text or by changing the interpretation of certain provisions.

Thus, this section will examine four key areas:

1. Whether the mere use of AI should give rise to specific criminalization or aggravation.

2. The issue of intentional liability in MEDICRIME and its relationship with AI.

3. The potential consideration of medical software as a medical product.

4. International cooperation and additional measures in the MEDICRIME Convention and their possible expansion.

#### 3.3.1. On the possible explicit criminalization of the "Use of AI" to commit the offenses covered by MEDICRIME

It has been stated that AI is significantly changing the way in which certain behaviors are carried out, such as the production of counterfeit medicines, their ingredients, or fraudulent medical devices; the distribution, offering, and intentional trafficking of counterfeit medical products; the forgery of documents to make counterfeit medical products appear legitimate; or the manufacture and commercialization of medical products without proper certification or in violation of regulatory requirements. However, I do not believe that the use of AI systems inherently adds any wrongful content per se to the commission of these offenses. Ultimately, what is criminalized in these cases are behaviors in which the relevant elements are the existence of fraudulent intent and a resulting risk, without requiring any specific means to commit them. In other words, the wrongdoing associated with the criminalized behaviors does not change simply because AI is used.

The only uncertainty is whether the same can be said about harm—the damage or risk to the legally protected interest in this provision, namely public health. It has been observed that AI not only optimizes counterfeiting processes, reducing costs and increasing the sophistication of fraudulent products, but it could also facilitate the expansion of the distribution of these medicines, thereby increasing the risk to public health. Article 13 of the MEDICRIME Convention already requires States to consider it an aggravating circumstance when: "the offenses of supplying and offering to supply were committed having resort to means of large-scale distribution, such as information systems, including the Internet." In this regard, two options can be considered: A possible

reform of MEDICRIME to establish specific aggravating factors related to AI; or interpreting that when paragraph (d) of Article 13 refers to "Information Systems," this already includes AI. In my opinion, this second option is perfectly viable. After all, as previously stated, the CAI definition (Council of Europe's Framework Convention on AI) only adds additional requirements for certain computer systems to be considered AI, but it ultimately recognizes AI as part of "information systems."

With that said and given that a reform of MEDICRIME is not strictly necessary to cover certain aggravated offenses related to the use of AI, we could still consider the explicit inclusion of some of these offenses. Many lawmakers use explicit criminalization techniques as a symbolic way of demonstrating that the criminal justice system is adapting to new realities, even when, without such explicit classification, there are already existing offenses that would allow for the sanction of the same or very similar behaviors. Thus, for example, an increase in penalties could be considered in cases where generative AI models are used for:

- The creation of fraudulent quality certificates, marketing authorizations, and other falsified documents that facilitate the distribution of counterfeit medical products.

- The use of AI-driven algorithms to identify vulnerable populations with specific medical needs and the creation of misleading advertising campaigns targeting these groups, thereby increasing health risks.

- The use of AI-based tools to circumvent traceability, authentication, and verification systems for medical products.

Some of these particularly serious behaviors could already be covered by the aggravating factor mentioned above, but it is worth considering whether its scope should be expanded so that, in the age of AI, the MEDICRIME Convention continues to provide proportionate responses to the severity of these new criminal dynamics.

#### 3.3.2. The issue of intentional liability in MEDICRIME and its relationship with AI

The MEDICRIME Convention is based on the criminalization of intentional offenses. As previously stated, the automation of processes through AI may require shifting criminal liability to earlier stages, where the risk is not yet fully apparent but where negligent actions could still create a potential harmful outcome that materializes later. In these cases, the direct attribution of intent becomes difficult, which is why, in general, the emergence of AI could lead to many offenses—previously punished only when committed intentionally—now also being sanctioned in their negligent form. However, I do not believe this should apply to the offenses that MEDICRIME requires to be criminalized. Expanding criminal liability to cases where negligence in the design, implementation, or oversight of AI facilitates the counterfeiting of medical products would entail a fundamental paradigm shift in the convention. Currently, its sole and specific focus is on clearly intentional offenses, which follow the prototypical structure of fraud: Deception leading to an error, which in turn results in harm.

Including other negligent behaviors related to medicines and medical products would result in a significant expansion of the Convention's scope, which would only be justified after a much deeper analysis and reflection on the medical and pharmaceutical industry. The use of AI can, as we have seen, serve as a tool for deception and inducing errors. Therefore, if the objective of MEDICRIME remains the criminalization of intentional offenses, then nothing about AI's emergence requires any change regarding the subjective elements of criminalization.

### 3.3.3. The potential consideration of AI chatbots as a medical device for the purposes of MEDICRIME

As discussed in this document, technological advancements have led to the emergence of AI systems used in disease diagnosis and treatment, such as medical chatbots. The FDA and EMA have already begun regulating certain AI systems under the category of "Software as a Medical Device" (SaMD), meaning that some AI-based products could be classified as medical devices. This raises the need to clarify whether the MEDICRIME Convention should extend its scope to cover the counterfeiting and fraudulent distribution of these new technological products or whether it already does so through its provisions.

MEDICRIME broadly defines medical devices, including software designed for diagnostic or therapeutic purposes. Therefore, AI applied to healthcare could already be subject to the Convention's provisions if its counterfeiting or unauthorized distribution is demonstrated. Article 8 of the MEDICRIME Convention states: "Each Party shall take the necessary legislative and other measures to establish as offences under its domestic law, when committed intentionally, in so far as such an activity is not covered by Articles 5, 6 and 7," and it includes: "The manufacturing, the keeping in stock for supply, importing, exporting, supplying, offering to supply or placing on the market of medical devices without being in compliance with the conformity requirements, where such conformity is required under the domestic law of the Party."

In my opinion, behaviors such as the commercialization and distribution of uncertified medical software, or the falsification of interfaces and software to imitate legitimate medical tools, could already fall under the criminal offenses required by MEDICRIME. For instance, the creation of fraudulent platforms offering AI systems for diagnosis without the necessary validation from health authorities—exposing users to inaccurate information or dangerous treatments—could fall within the scope of the Convention's protection. The same applies to the development of applications that imitate regulated products to deceive consumers and healthcare professionals. A remaining uncertainty is whether the same applies to the manipulation of algorithms to alter diagnoses and treatments. Intentionally modifying a medical chatbot or an AI-based diagnostic system to mislead patients or healthcare professionals can have devastating consequences for public health, and it is worth considering whether this should be explicitly listed as a criminal offense under MEDICRIME. Perhaps the reference in Article 5 of MEDICRIME to: "Each Party shall take the necessary legislative and other measures to establish as offences under its domestic law, the intentional manufacturing of counterfeit medical products, active substances, excipients, parts, materials and accessories". And the fact that paragraph 2 includes medical devices among the objects covered, may already address this issue.

After all, the intentional manipulation of certified medical software to generate errors in diagnosis or treatment using AI would be equivalent to the adulteration of a physical drug, as it compromises patient safety in a similar manner. However, it would be advisable to clarify this point if mechanisms exist to do so.

#### 3.3.4. Cooperation between authorities, information exchange, and other complementary measures

One of the most important aspects of MEDICRIME is its incorporation of various mechanisms for cooperation between authorities and information exchange. This is regulated, among other provisions, in Article 17 of the Convention, and it is worth considering whether this article should be adapted to the emergence of artificial intelligence (AI). The same applies to Chapter VII of the Convention, particularly Articles 21 and 22. Clearly, the automation and sophistication of counterfeiting through AI, along with its ability to optimize the distribution and promotion of fraudulent medicines in digital environments, necessitate that international cooperation incorporate advanced technological tools and consider new actors soon.

A different question, once again, is whether this should be done through an amendment to MEDICRIME or simply through an updated interpretation of the existing provisions. For effective information exchange between health, customs, and law enforcement authorities, in the future, interoperable databases should be developed, along with the integration of AI-based systems for monitoring counterfeit medical products. If States adopted real-time data analysis mechanisms, integrating machine learning models to detect fraud patterns in digital markets and social media, and shared this information among themselves, the effectiveness of interventions against these frauds would increase. For this reason, promoting the creation of a standardized AI-based early warning system within the Single Points of Contact (SPOC) established by MEDICRIME is an ambitious and perhaps unrealistic goal, but one that would certainly facilitate cooperation between countries in identifying criminal networks that use AI for counterfeiting and illicit trade in medical products.

Even more important, based on the criminological analysis previously conducted, is that MEDICRIME, when addressing cooperation between the public and private sectors, explicitly refers to digital service providers and e-commerce platforms. Currently, many counterfeit products are marketed through AI-optimized automated ads, making their detection more difficult using traditional methods. The question is whether MEDICRIME could encourage States to require digital platforms to implement AI tools for identifying and removing fraudulent advertisements, as well as mandatory cooperation protocols with national authorities to share information on fraud patterns. Taking this further, it is worth considering whether MEDICRIME should explicitly reference the liability of digital service providers in the commercialization of counterfeit products. Although MEDICRIME criminalizes the distribution of counterfeit medicines, it does not impose specific obligations on digital platforms and online services where these products are sold. However, since AI facilitates the large-scale, segmented sale of fraudulent medicines, a recommendation could be made for signatory countries to require online marketplaces and platforms to establish active monitoring mechanisms against counterfeit medical

products and define responsibilities in cases of non-compliance. Similarly, States could commit to enacting laws requiring transparency and traceability in the online sale of medical products, ensuring that platforms operating within their territory cooperate in identifying fraudulent networks.

Finally, regarding the training of units responsible for cooperation and information exchange, Article 17 should include training in AI use for fraud detection in counterfeit medical products. This would ensure that authorities have the knowledge and resources needed to address new criminal dynamics facilitated by AI. In this regard, MEDICRIME could recommend that States include, in their training programs for judges, prosecutors, and law enforcement agencies, specific modules on the impact of AI on counterfeit medical products and technological strategies for detection and prosecution.

Regarding international cooperation in criminal matters, an updated interpretation of Articles 21 and 22 of the Convention could also be considered in light of this new technological reality. For instance, States could incorporate AI-based digital forensic tools in cooperation treaties to analyze online evidence and track automated counterfeiting and sales operations. Additionally, international cooperation should be strengthened to identify and freeze digital assets obtained through AI-driven illicit trade in counterfeit medical products, ensuring that States have compatible legal frameworks for intervening in these funds, which may exist in the form of cryptocurrencies. Furthermore, concerning Article 22, AI's increased capacity for dissemination necessitates that States implement accessible, digitalized reporting channels for victims of counterfeit medical product fraud. Moreover, they should cooperate through transnational reporting platforms where affected individuals can report AI-related health frauds, which would then be redirected to the appropriate national authorities. This would also help strengthen regulation in vulnerable regions, preventing markets for counterfeit medical products from thriving in countries with fewer technological and regulatory resources.

It is true that we are anticipating AI use scenarios that are still relatively uncommon. However, it has already been demonstrated that AI's development speed is astonishing, and that authorities and the public are always lagging behind. In this sense, and to conclude, MEDICRIME could also recommend that States implement national awareness campaigns on AI-related risks in counterfeit medical products, targeting both consumers and healthcare professionals.

**Bibliography**


- Alarcón-Jiménez, O. (2015). The MEDICRIME Convention – Fighting Against Counterfeit Medicine. Eurohealth, 21(4), 24-27.
- Almeman, Ahmad. "The digital transformation in pharmacy: embracing online platforms and the cosmeceutical paradigm shift." *Journal of Health, Population and Nutrition* 43.1 (2024): 60.
- Chakraborty, Chiranjib, et al. "Overview of Chatbots with special emphasis on artificial intelligence-enabled ChatGPT in medical science." *Frontiers in artificial intelligence* 6 (2023): 1237704. “El trabajo describe cómo los
- EMA. Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle…9 September 2024 EMA/CHMP/CVMP/83833/2023 Committee for Medicinal Products for Human Use (CHMP) Committee for Medicinal Products for Veterinary Use (CVMP)
- EUIPO.: Trade in counterfeit pharmaceltical products, EUIPO
- Gomasta, Sarmistha Sarna, et al. "PharmaChain: Blockchain-based drug supply chain provenance verification system." *Heliyon* 9.7 (2023).
- Islam, Iyolita, and Muhammad Nazrul Islam. "Digital intervention to reduce counterfeit and falsified medicines: A systematic review and future research agenda." *Journal of King Saud University-Computer and Information Sciences* 34.9 (2022): 6699-6718.
- Loh, Erwin. "ChatGPT and generative AI chatbots: challenges and opportunities for science, medicine and medical leaders." *BMJ Leader* (2023): leader-2023.
- Mackey, Tim K., and Gaurvika Nayyar. "A review of existing and emerging digital technologies to combat the global trade in fake medicines." *Expert opinion on drug safety* 16.5 (2017): 587-602.
- Mladinić, Nina, Šime Jozipović, and Marko Perkušić. "The Danger of Organized Crime in the Area of Falsification of Medicines and Medical Products (Profit vs. Right to Health)." *EU and comparative law issues and challenges series (ECLIC)* 8 (2024): 113-139.
- Miró-Llinares, F., Association International de Droit Pénal – International Association of Penal Law XXI International Congres of Penal Law: “Artificial Intelligence and Criminal Justice”, International Colloquium of Section II (Criminal Law-specific offences in the Criminal code), 2023.
- Nayyar, Gaurvika ML, et al. "Falsified and substandard drugs: stopping the pandemic." *The American journal of tropical medicine and hygiene* 100.5 (2019): 1058.
- Pascu, G. A., Hancu, G., & Rusu, A. (2020). Pharmaceutical serialization, a global effort to combat counterfeit medicines. *Acta Marisiensis-Seria Medica*, *66*(4), 132-139.
- Singh, Kumkum, et al. "Integrating the AI-Driven Technologies Into Pharmaceutical Service Marketing." *Integrating AI-Driven Technologies Into Service Marketing*. IGI Global, 2024. 395-418.
- Tiwari, Rajesh, et al. "Role of Technology for Pharmaceutical Marketing in the Era of Artificial Intelligence: A Bibliometric Study." *Advances in Digital Marketing in the Era of Artificial Intelligence*. CRC Press 267-278.

- Venhuis, B. J., Oostlander, A. E., Di Giorgio, D., Mosimann, R., & du Plessis, I. (2018). Oncology drugs in the crosshairs of pharmaceutical crime. *The Lancet Oncology*, *19*(4), e209-e217.