

Strasbourg, 24 Avril 2026

T-MED (2025) 03

La Convention MEDICRIME à l'ère de l'IA : défis et opportunités

préparé par

Pr. Fernando MIRÓ LLINARES

Centre CRIMINA, Université Miguel Hernández d'Elche (Espagne)

Direction générale I - Droits humains et État de droit



TABLE DES MATIÈRES

1. Introduction	3
1.1. Objectifs et méthodologie du projet préliminaire	3
1.2. Définition de l'IA et champ d'application de la technologie considérée dans le cadre du présent document	4
2. Le nouveau défi que représente l'IA pour la contrefaçon et le trafic de produits médicaux.....	6
2.1. Numérisation et contrefaçon de produits médicaux à l'ère de l'IA : état des lieux.....	6
2.1.1. L'écosystème numérique actuel et la contrefaçon de produits médicaux	6
2.1.2. L'IA comme technologie habilitante pour la contrefaçon de produits médicaux	7
2.1.3. L'IA comme outil potentiel de détection des produits médicaux contrefaits.....	8
2.2. L'IA générative et l'émergence de nouveaux dispositifs médicaux	9
3. MEDICRIME dans le nouveau scénario façonné par l'IA.....	10
3.1. Une question préliminaire : IA, responsabilité pénale et techniques de criminalisation	10
3.2. Une opportunité pour MEDICRIME : sa pertinence renouvelée dans le sillage de l'IA.....	13
3.3. Sur les réformes et changements potentiels dans MEDICRIME	14
3.3.1. Sur l'éventuelle criminalisation explicite de l' « utilisation de l'IA » pour commettre les infractions couvertes par MEDICRIME	15
3.3.2. La question de la responsabilité intentionnelle dans MEDICRIME et sa relation avec l'IA	16
3.3.3. La considération potentielle des chatbots d'IA en tant que dispositif médical aux fins de MEDICRIME.....	17
3.3.4. Coopération entre les autorités, échange d'informations et autres mesures complémentaires.....	18
Bibliographie.....	20

LA CONVENTION MEDICRIME À L'ÈRE DE L'INTELLIGENCE ARTIFICIELLE : DÉFIS ET OPPORTUNITÉS

1. Introduction

1.1. Objectifs et méthodologie du projet préliminaire

L'avènement de l'intelligence artificielle (IA) dans la société contemporaine transforme profondément et rapidement de multiples secteurs, générant des impacts d'une ampleur difficilement comparable à toute autre innovation technologique récente. Dans le domaine de la santé, en particulier en ce qui concerne la fabrication, la distribution et la commercialisation de médicaments et d'autres produits médicaux, l'IA - combinée à l'utilisation généralisée des réseaux sociaux et d'autres technologies numériques - introduit de nouvelles dynamiques à la fois dans la production et la commercialisation dans des environnements numériques. Ces transformations créent des opportunités en termes d'efficacité, de contrôle de la qualité et d'accès aux soins de santé, mais elles posent également des défis réglementaires sans précédent, notamment en ce qui concerne la prolifération d'activités illégales liées à la contrefaçon de produits médicaux, au commerce illégal de médicaments et à d'autres comportements qui mettent en danger la santé publique.

La Convention MEDICRIME du Conseil de l'Europe constitue le principal cadre réglementaire international visant à lutter contre la contrefaçon des produits médicaux et des infractions similaires qui compromettent la santé publique. Son objectif est d'établir un cadre juridique commun pour la criminalisation de ces comportements, en garantissant l'harmonisation des réglementations et des mécanismes de coopération internationale qui permettent de répondre efficacement aux menaces qu'ils font peser sur la sécurité sanitaire mondiale. Cependant, l'émergence et la consolidation de l'IA en tant que technologie perturbatrice nécessitent une analyse rigoureuse de ses implications pour l'efficacité du traité, car elle peut modifier de manière significative à la fois les modes opératoires des crimes couverts par MEDICRIME et les outils disponibles pour leur prévention, leur détection et leur poursuite.

Ce document vise à évaluer l'impact que l'IA, dans son interaction avec la numérisation croissante du commerce des produits médicaux et pharmaceutiques, peut avoir sur l'applicabilité et la pertinence de la Convention MEDICRIME. Cette analyse s'articule autour de deux objectifs fondamentaux et séquentiels. Le premier est d'explorer dans quelle mesure l'IA transforme les comportements que le traité cherche à sanctionner, en reconnaissant que ces pratiques criminelles n'apparaissent pas isolément mais dans le cadre d'un processus de numérisation qui évolue depuis des décennies et qui s'est accéléré après la pandémie de COVID-19. L'avènement d'Internet a facilité la commercialisation transnationale de produits médicaux sans contrôle adéquat. Les réseaux sociaux ont élargi de manière exponentielle l'accès aux marchés illicites par le biais de plateformes qui sont devenues encore plus populaires pendant les périodes de confinement, permettant une interaction directe entre les fournisseurs et les consommateurs sans intermédiaires réglementaires. Enfin, l'IA a introduit des mécanismes d'automatisation et de sophistication dans la production, la distribution et la commercialisation de produits contrefaits, remettant en cause les stratégies de

contrôle traditionnelles. Dans le même temps, l'IA offre également des possibilités intéressantes de détection des produits contrefaits et de contrôle de leur vente, même s'il faudra pour cela s'adresser à de nouveaux acteurs clés, tels que les fournisseurs de services numériques. Il est essentiel de comprendre ce contexte pour aborder le deuxième objectif du présent document : examiner les répercussions potentielles de ces changements sur la structure et l'efficacité de la Convention MEDICRIME, analyser dans quelle mesure les dispositions actuelles du traité restent adéquates pour faire face à ces nouvelles menaces et si des modifications peuvent être nécessaires pour renforcer son applicabilité dans un environnement dominé par l'IA.

La méthodologie adoptée dans cette analyse combine une approche juridico-normative, axée sur l'étude du cadre réglementaire de MEDICRIME et son interaction avec l'évolution technologique, avec une perspective criminologique et de politique criminelle qui évalue comment les changements dans la dynamique criminelle ont un impact sur l'efficacité de l'instrument. Pour ce faire, des études récentes sur l'impact de l'IA sur les marchés illicites, des rapports d'organisations internationales et d'autres sources bibliographiques sont pris en compte pour offrir un diagnostic bien fondé des défis et des opportunités posés par l'intelligence artificielle dans ce domaine. Pour l'analyse juridique, la littérature spécialisée est examinée et des documents tels que le rapport « Criminalization of AI-related Offences », qui examine de manière générale les défis posés par l'intelligence artificielle dans le domaine du droit pénal, sont pris en compte. Ce rapport traite de la nécessité d'adapter la législation actuelle pour lutter contre les infractions liées à l'IA et identifie les techniques législatives les plus appropriées pour atteindre cet objectif.

Ce document jette les bases d'une réflexion sur la nécessité d'actualiser, de réinterpréter ou de renforcer les dispositions de MEDICRIME en tenant compte des nouveaux défis liés à l'IA, contribuant ainsi à l'élaboration d'un cadre réglementaire plus solide, adapté aux complexités de l'ère numérique et capable de protéger efficacement la santé publique contre les nouvelles formes de criminalité transnationale qui utilisent déjà cette technologie et l'utiliseront de plus en plus.

1.2. Définition de l'IA et champ d'application de la technologie considérée dans le cadre du présent document

Aux fins du présent document, l'intelligence artificielle est définie comme « *un système basé sur une machine qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, des contenus, des recommandations ou des décisions susceptibles d'influencer des environnements physiques ou virtuels* ». Nous utilisons la définition adoptée par la Convention-cadre sur l'intelligence artificielle, les droits humains, la démocratie et l'État de droit (ci-après, CAI) du Conseil de l'Europe, en particulier celle contenue dans l'article 2 de cet instrument, qui dispose en outre que « *les différents systèmes d'intelligence artificielle varient dans leurs niveaux d'autonomie et d'adaptabilité après le déploiement* ».

Cette définition permet d'identifier certaines caractéristiques fondamentales des systèmes d'IA qui sont particulièrement pertinentes pour analyser l'impact de cette

technologie sur la Convention MEDICRIME. La définition reconnaît l'existence de différents niveaux d'autonomie et d'adaptabilité dans les systèmes d'IA, ce qui, à son tour, exige que cette idée d' « autonomie » soit prise en compte. Cela implique de reconnaître une distinction fondamentale entre les systèmes informatiques où les machines qui fonctionnent strictement selon des règles prédéfinies et ceux qui peuvent modifier leur comportement en fonction du contexte et des informations qu'ils reçoivent après leur déploiement.

Seuls ces derniers - ceux qui possèdent des capacités de traitement leur permettant d'adapter leur comportement en fonction des données qu'ils traitent, plutôt que des systèmes purement réactifs ou préprogrammés - seront considérés comme de l'IA. En effet, la capacité de fonctionner avec un certain degré d'indépendance et de modifier les performances en fonction des données traitées est ce qui fait de l'IA à la fois une opportunité et un défi d'un point de vue réglementaire et juridique. Cela nécessite une analyse spécifique de son impact sur les crimes que la Convention MEDICRIME cherche à prévenir et à punir.

Dans le cadre de ces préoccupations, le présent document se concentrera en particulier sur les systèmes d'IA générative, les grands modèles de langage (LLM) et d'autres architectures avancées, qui ont démontré une capacité croissante à produire de nouveaux contenus, à imiter des modèles de langage et d'imagerie humains et à générer des résultats qui peuvent être utilisés à des fins légales et illégales. Les LLM, tels que ChatGPT, Gemini, Claude ou DeepSeek, sont des modèles d'apprentissage profond formés sur des volumes massifs de données textuelles, capables de générer des réponses cohérentes et adaptées au contexte en fonction des données fournies. Leur application dans différents domaines a permis des avancées significatives dans de multiples tâches, mais elle a également ouvert la porte à des risques tels que la génération automatisée de fraudes ou la création de fausses informations difficiles à distinguer du contenu réel (Deep Fakes).

L'analyse de leur impact sur la Convention MEDICRIME sera essentielle pour évaluer dans quelle mesure cette technologie peut faciliter la contrefaçon de produits médicaux, la diffusion d'informations erronées sur la santé ou la production automatisée de documents frauduleux. Cette évaluation permettra également de déterminer quels ajustements réglementaires pourraient être nécessaires pour relever ces défis.

Enfin, il est important de noter qu'à l'heure actuelle, les applications d'IA les plus avancées correspondent à ce que l'on appelle l'IA faible (Narrow AI) - des systèmes hautement spécialisés qui permettent l'automatisation de tâches spécifiques dans un domaine défini, mais qui manquent de capacités de raisonnement général ou de compréhension contextuelle au-delà des données sur lesquelles ils ont été formés. Dans un avenir proche, il est possible que des systèmes d'IA forte, voire des formes de super-intelligence artificielle, soient mis au point, ce qui pourrait poser de tout nouveaux défis, tant du point de vue des comportements que MEDICRIME cherche à prévenir que du point de vue du droit pénal lui-même. Toutefois, le présent document se concentrera sur les technologies d'IA qui sont déjà présentes sur le marché et qui présentent des risques et des opportunités immédiats pour l'application du traité, tout en envisageant également les développements prévisibles dans le cadre de la définition de la Convention-cadre.

2. Le nouveau défi que représente l'IA pour la contrefaçon et le trafic de produits médicaux

2.1. Numérisation et contrefaçon de produits médicaux à l'ère de l'IA : état des lieux

2.1.1. L'écosystème numérique actuel et la contrefaçon de produits médicaux

Au cours des dernières décennies, le commerce des produits médicaux a connu une croissance et une transformation sans précédent, sous l'effet de la numérisation d'une part et de la mondialisation des marchés d'autre part. La combinaison de ces deux phénomènes a facilité l'accès aux médicaments et aux dispositifs médicaux partout dans le monde, ce qui, dans le même temps, a créé de nouvelles opportunités pour la prolifération des produits contrefaits.

L'écosystème numérique est devenu un environnement clef pour la distribution illicite de médicaments contrefaits, car il offre de multiples outils et plateformes qui permettent aux acteurs criminels d'opérer avec un haut degré d'anonymat et une capacité d'expansion sans précédent. Cela brouille les frontières traditionnelles du commerce illégal de ces produits et entrave l'application efficace des mécanismes de contrôle et de surveillance. Cette tendance semble s'être accentuée après la pandémie de COVID-19, en raison de l'accélération de la numérisation qui a suivi les mesures de confinement. De nombreux processus sociaux se sont numérisés et les citoyens ont commencé à faire confiance au commerce en ligne beaucoup plus qu'auparavant. Les réseaux sociaux semblent jouer un rôle crucial dans la commercialisation et la distribution de ces produits médicaux contrefaits, en permettant aux vendeurs illicites d'utiliser des stratégies de segmentation avancées pour cibler des consommateurs spécifiques avec des publicités, sans avoir besoin de recourir aux marchés traditionnels ou aux canaux de distribution physiques. Des plateformes telles que Facebook, Instagram, TikTok et Telegram ont été utilisées par des réseaux criminels pour promouvoir des produits frauduleux par le biais de publicités personnalisées, de faux commentaires et de témoignages manipulés, qui suscitent la confiance des consommateurs. Même si ces espaces numériques devraient être modérés et disposer de mécanismes de supervision des publicités utilisant des algorithmes d'IA, nombre de ces offres illégales parviennent à contourner les contrôles internes des plateformes et à atteindre des milliers d'utilisateurs en quelques minutes.

Un autre élément clef de cet écosystème est l'utilisation croissante des crypto-monnaies et des plateformes de paiement numérique, qui a facilité les transactions illicites en offrant des méthodes de paiement décentralisées qui n'obligent pas les utilisateurs à révéler des informations personnelles ou financières. Cela réduit considérablement le risque de détection et permet aux criminels d'opérer sans laisser de traces dans les systèmes bancaires traditionnels. En utilisant Bitcoin, Monero et d'autres crypto-monnaies, les vendeurs peuvent recevoir de l'argent d'acheteurs situés dans différentes parties du monde sans dépendre d'intermédiaires financiers. Cela rend non seulement plus difficile l'identification des réseaux de trafic de faux médicaments, mais empêche également la traçabilité des transactions et l'application de mesures de contrôle sur ces flux financiers.

L'émergence de l'IA dans ce contexte a introduit une couche supplémentaire de complexité, car cette technologie permet l'automatisation de multiples processus liés à la contrefaçon, à la distribution et à la commercialisation de produits médicaux frauduleux. L'IA peut optimiser les stratégies de marché et maximiser la portée des réseaux criminels. À mesure que l'IA s'améliore et devient plus largement disponible à faible coût - ce qui est déjà le cas - et qu'elle s'intègre davantage dans les réseaux sociaux, les algorithmes publicitaires et les plateformes de commerce numérique, son utilisation par les groupes criminels pour faciliter ces délits deviendra de plus en plus pertinente. Cela posera de nouveaux défis aux cadres réglementaires et aux instruments de coopération internationale dans la lutte contre le trafic de produits médicaux contrefaits.

2.1.2. L'IA comme technologie habilitante pour la contrefaçon de produits médicaux

L'un des aspects les plus préoccupants de l'émergence de l'IA dans le domaine de la contrefaçon de produits médicaux est son potentiel à faciliter la production de médicaments et de dispositifs de santé frauduleux avec un niveau de sophistication sans précédent. Traditionnellement, la contrefaçon de médicaments d'apparence authentique nécessitait des processus industriels manuels ou de faible technicité, ce qui limitait la qualité des copies et les rendait plus faciles à identifier pour les autorités sanitaires. Cependant, grâce aux progrès de l'IA et des techniques d'automatisation, les contrefacteurs ont désormais accès à des outils qui leur permettent de reproduire avec précision l'apparence et la composition chimique des produits médicaux originaux, ce qui réduit les possibilités de détection et accroît les risques pour la santé publique.

Tout d'abord, les modèles génératifs d'IA peuvent être utilisés pour concevoir de fausses étiquettes, de faux emballages et de fausses certifications avec un niveau de détail tel qu'il est pratiquement impossible de les distinguer des produits légitimes. Les algorithmes de traitement d'images permettent de scanner et de reproduire des documents officiels avec une telle précision que les techniques de vérification traditionnelles deviennent inefficaces, ce qui facilite l'introduction de médicaments contrefaits sur le marché sans éveiller les soupçons. En outre, ces modèles sont également capables de générer de faux codes QR, des hologrammes de sécurité et d'autres mécanismes d'authentification qui imitent les systèmes de vérification des fabricants légitimes.

Deuxièmement, l'IA peut être utilisée pour optimiser la synthèse chimique et les processus de production pharmaceutique, ce qui permet aux contrefacteurs de mettre au point des composés ayant l'apparence et la consistance de médicaments authentiques, même s'ils ne respectent pas les normes de qualité et de sécurité. Les modèles d'apprentissage automatique peuvent analyser les bases de données pharmaceutiques pour identifier les combinaisons d'ingrédients actifs qui imitent les effets d'un médicament légitime sans utiliser les composants originaux. Cela permettrait non seulement de réduire les coûts de production, mais aussi de rendre plus difficile la détection des fraudes lors des tests de contrôle de qualité standard.

Une autre application inquiétante de l'IA dans ce domaine est sa capacité à automatiser les stratégies de marketing et de distribution à l'aide de bots et de systèmes d'optimisation des publicités sur les médias sociaux et les plateformes de commerce numérique. Les algorithmes de segmentation peuvent identifier les populations vulnérables qui sont plus susceptibles d'acheter des médicaments en ligne sans vérifier leur authenticité, ce qui facilite la promotion très ciblée de produits contrefaits. En outre, les systèmes d'IA peuvent générer automatiquement des centaines ou des milliers de faux profils sur les réseaux sociaux pour afficher des avis positifs, répondre aux questions des clients potentiels et renforcer la perception de légitimité des vendeurs illicites.

2.1.3. L'IA comme outil potentiel de détection des produits médicaux contrefaits

Si l'intelligence artificielle s'est révélée être une technologie facilitant la contrefaçon de produits médicaux, elle offre également un énorme potentiel en tant qu'outil de détection et de contrôle, permettant aux autorités sanitaires, aux organismes de réglementation et aux plateformes numériques d'améliorer leur capacité à identifier et à retirer les produits frauduleux avant qu'ils n'atteignent les consommateurs. Cela illustre le caractère dual de ces technologies.

Grâce à l'utilisation d'algorithmes, de techniques d'analyse du big data et de modèles d'apprentissage automatique, l'IA peut jouer un rôle clé dans la lutte contre la contrefaçon de médicaments et de dispositifs de santé. En effet, l'Agence européenne des médicaments (EMA) a récemment publié un document de réflexion sur l'utilisation de l'intelligence artificielle dans le cycle de vie des médicaments qui, bien qu'il n'aborde pas directement l'impact de l'IA sur le trafic de médicaments contrefaits ou l'application de MEDICRIME, soulève des questions pertinentes concernant l'utilisation potentielle de cette technologie pour la traçabilité et la pharmacovigilance. En particulier, le document indique que l'IA peut jouer un rôle dans l'identification des produits médicaux contrefaits en surveillant les schémas de la chaîne d'approvisionnement et en détectant les anomalies dans la distribution. Certaines sections clés de ce document pourraient être pertinentes dans ce domaine (section 2.2.7). En outre, la section 2.2.6 souligne que l'utilisation de l'IA dans la fabrication et la distribution des médicaments pourrait contribuer à améliorer la traçabilité et la sécurité des produits pharmaceutiques. L'EMA a reconnu certaines des principales applications potentielles de l'IA dans ce domaine, par exemple :

- Détection automatisée de schémas suspects sur les plateformes de commerce numérique et les médias sociaux. Les algorithmes d'apprentissage profond peuvent analyser de grands volumes de données en temps réel pour identifier les listes de produits médicaux présentant des caractéristiques atypiques, telles que des prix trop bas, des emplacements incohérents ou des images modifiées.
- Analyse des métadonnées et des réseaux d'interaction sur les médias sociaux, qui permet de suivre l'activité des vendeurs illicites et de cartographier les connexions entre les différents acteurs du marché noir des médicaments.

- Combiner la blockchain et les algorithmes d'IA pour améliorer la traçabilité de la chaîne d'approvisionnement, permettant aux autorités de vérifier l'authenticité des produits à chaque étape du processus de distribution. En intégrant les réseaux neuronaux et la technologie des registres décentralisés, il devient possible de suivre l'origine et l'historique de chaque médicament, ce qui garantit que seuls les produits légitimes entrent sur le marché et facilite la détection des vulnérabilités dans la chaîne de distribution. La blockchain garantit également l'intégrité des données et protège les informations sensibles pour les patients, réduisant ainsi le risque de manipulation et garantissant que seules les parties autorisées ont accès aux données sensibles.

Enfin, l'IA peut également être utilisée dans l'authentification des médicaments au niveau du consommateur, grâce au développement d'applications mobiles qui permettent aux utilisateurs de scanner les codes de sécurité et de vérifier en temps réel si un produit est légitime ou s'il a été signalé comme contrefait. Ces applications peuvent s'appuyer sur des techniques de vision artificielle et de traitement du langage naturel pour interpréter les étiquettes, détecter les irrégularités et alerter les consommateurs sur les risques potentiels.

2.2. L'IA générative et l'émergence de nouveaux dispositifs médicaux

Jusqu'à présent, l'IA a été analysée comme un outil de contrefaçon de produits médicaux, mais le développement pratique actuel de cette technologie nous oblige également à envisager la possibilité que l'IA elle-même devienne un produit médical et un objet de fraude. Comme cela a déjà été décrit dans la littérature, l'émergence de chatbots basés sur l'IA transforme le secteur des soins de santé, avec des applications dans le diagnostic médical, l'assistance aux patients et l'éducation à la santé. Actuellement, des outils tels que ChatGPT et d'autres chatbots médicaux sont utilisés pour répondre aux questions des patients, fournir des informations médicales et aider à la gestion des maladies chroniques telles que le diabète. Les chatbots basés sur l'IA sont déjà utilisés dans le secteur des soins de santé à des fins multiples, allant des soins aux patients au diagnostic et à la gestion des dossiers médicaux.

Comme le souligne Loh (2023), les chatbots médicaux existants sont classés en trois catégories principales :

- Les chatbots informatifs, utilisés pour améliorer les connaissances en matière de santé en fournissant des informations sur les maladies, les symptômes et les traitements.
- Les chatbots de diagnostic, qui aident les médecins à établir des diagnostics préliminaires et à gérer les médicaments, plutôt que de remplacer le jugement clinique.
- Les chatbots administratifs, qui favorisent la prise de rendez-vous, la création de dossiers médicaux et l'optimisation du temps des professionnels de santé.

L'évolution de la technologie suggère que les chatbots médicaux actuels pourraient devenir des produits médicaux réglementés axés principalement sur le diagnostic et le traitement des maladies chroniques. Bien que ces systèmes agissent actuellement principalement comme des assistants, ils pourraient à l'avenir être considérés comme des dispositifs médicaux s'ils s'intègrent de manière autonome dans la prise de décision clinique. Pour cela, ils devront répondre à des exigences réglementaires strictes en termes de sécurité, de fiabilité, de précision du diagnostic et d'autres considérations d'éthique médicale. En fait, aux États-Unis, la FDA (Food and Drug Administration) a commencé à classer certains systèmes d'IA dans la catégorie « Software as a Medical Device » (SaMD), ce qui signifie que, selon leur fonction, certains chatbots pourraient être réglementés en tant que dispositifs médicaux.

Pour être considéré comme un dispositif médical réglementé, un système d'IA doit : faire preuve de précision et de fiabilité dans ses réponses, en particulier s'il propose des diagnostics ou des recommandations de traitement ; passer des essais cliniques qui valident son efficacité dans la pratique médicale ; garantir la confidentialité et la sécurité des données des patients. Il n'est donc pas déraisonnable de s'attendre à ce que les produits alimentés par l'IA cherchent à obtenir une certification réglementaire auprès d'agences telles que la FDA aux États-Unis ou l'EMA dans l'Union européenne. Ces certifications pourraient bientôt être obtenues, ce qui conduirait à une intégration encore plus poussée des systèmes basés sur l'IA dans les services de santé.

3. MEDICRIME dans le nouveau scénario façonné par l'IA

3.1. Une question préliminaire : IA, responsabilité pénale et techniques de criminalisation

La Convention MEDICRIME du Conseil de l'Europe vise à lutter contre la contrefaçon de produits médicaux et d'autres activités qui menacent la santé publique en promouvant l'harmonisation des lois pénales et la coopération internationale. Il s'agit donc d'un instrument juridique international axé sur le droit pénal qui, entre autres dispositions, exige la criminalisation de certains comportements et leur sanction proportionnelle et dissuasive.

C'est pourquoi, avant d'analyser si la Convention MEDICRIME doit être adaptée pour répondre aux défis liés à l'IA, il est important de comprendre comment l'IA peut affecter non seulement les infractions spécifiques liées à la contrefaçon, mais aussi le système de justice pénale.

Au-delà des transformations potentielles que le droit pénal pourrait connaître avec l'émergence d'entités véritablement autonomes et intelligentes (au sens moral) lorsque l'IA forte se développera, l'IA faible actuelle et les nouvelles dynamiques criminelles découlant de son utilisation et de son développement posent déjà des défis importants en matière de responsabilité pénale. Les catégories et modèles traditionnels de responsabilité pénale doivent être réévalués et adaptés à ces nouvelles réalités technologiques. Par conséquent, avant d'aborder le sujet spécifique de l'étude, il est essentiel de comprendre les changements plus généraux que l'IA pourrait apporter, ce qui en fait une considération préliminaire importante.

Pour déterminer si les systèmes actuels d'attribution de la responsabilité pénale, tels que ceux adoptés par la Convention MEDICRIME, sont adaptés à ces situations ou s'ils doivent être modifiés pour garantir une attribution correcte de la responsabilité, il est nécessaire d'identifier le caractère unique de la technologie qui peut mettre à l'épreuve les fondements du système de justice pénale. Les systèmes d'IA promettent une optimisation des processus de prise de décision en réduisant les biais humains et en améliorant l'efficacité de la gestion de l'information grâce à l'automatisation et à la délégation partielle ou totale de certaines fonctions aux machines.

Cela implique deux choses :

1. L'IA pourrait déplacer le moment clef de la détermination de la responsabilité pénale : au lieu d'être placée au moment où le dommage ou le risque se produit, l'attribution de la responsabilité pourrait devoir être analysée à des stades plus précoces du cycle de vie de l'IA, tels que sa conception et la formation des algorithmes.
2. L'automatisation progressive des processus grâce à l'IA pose le risque de lacunes en matière de responsabilité pénale dans les cas où les systèmes agissent de manière autonome et imprévisible.

Bien que ces systèmes ne possèdent pas d'autonomie morale, ils peuvent fonctionner avec un certain degré d'indépendance fonctionnelle, ce qui signifie que, dans certains scénarios, les effets de leurs actions peuvent être imprévisibles tant pour les utilisateurs que pour les développeurs. La difficulté d'attribuer une responsabilité pénale aux êtres humains lorsque les systèmes d'IA ont joué un rôle important dans le processus de causalité du préjudice exige, selon certains auteurs, une révision complète du système d'attribution de la responsabilité, tandis que d'autres soutiennent que les réglementations actuelles sont suffisantes et que l'obligation de contrôle et de surveillance par les concepteurs et les utilisateurs doit être renforcée afin d'éviter les lacunes de la réglementation.

Quoi qu'il en soit, il est évident que le déplacement de l'action humaine vers des phases plus précoces du cycle de vie de l'IA implique que la responsabilité pénale doit être évaluée aux stades de la conception et de la production de ces technologies, car c'est à ces moments-là que les risques les plus importants peuvent être évités. La criminalisation éventuelle des actes préparatoires ou des violations des obligations administratives liées au développement et au déploiement de systèmes d'IA à haut risque est présentée comme une alternative viable pour éviter les situations dans lesquelles les responsables ne peuvent pas être sanctionnés une fois que le dommage s'est produit. Ainsi, l'absence de supervision des systèmes qui fonctionnent avec un degré élevé d'autonomie ou l'absence de contrôles adéquats de l'IA pourraient faire l'objet de sanctions pénales lorsqu'elles génèrent un risque concret pour des intérêts légalement protégés, ce qui nécessiterait de définir clairement les obligations de supervision imposées à ceux qui conçoivent, forment et déploient ces systèmes.

Toutefois, l'adoption de telles dispositions pénales doit garantir que l'interdiction de certaines technologies ne viole pas le principe de légalité et n'entrave pas le développement légitime de l'intelligence artificielle à des fins légales. Il sera donc nécessaire de définir précisément les utilisations de l'IA considérées comme inacceptables et de justifier leur incrimination en termes de proportionnalité et de nécessité.

Un autre changement majeur auquel le droit pénal doit faire face est l'extension de la responsabilité pénale pour négligence en relation avec l'utilisation de l'IA, étant donné que dans de nombreux cas, le préjudice ne sera pas causé intentionnellement, mais plutôt en raison de défaillances dans la conception, la mise en œuvre ou la surveillance de ces systèmes. Cela nécessitera une reformulation des types de négligence en droit pénal afin d'envisager des situations où l'individu n'a pas directement causé de préjudice, mais a agi par négligence dans la gestion des risques inhérents à l'utilisation de l'IA. Il sera essentiel de définir avec précision les normes de diligence qui devraient être exigées des différents acteurs impliqués dans le développement et l'application de cette technologie. L'imposition de devoirs de diligence spécifiques en relation avec l'IA garantira que la responsabilité pénale pour négligence ne se limite pas aux situations où l'individu avait un contrôle direct sur l'action, mais peut s'étendre à ceux qui, en raison de leur rôle dans la conception et la gestion du système, ont subi des défaillances qui rendent prévisible la production d'un résultat préjudiciable.

Cependant, il est évident que lorsqu'un système d'IA est malicieusement conçu pour commettre un acte criminel, tout comme lorsque l'IA est utilisée sciemment et volontairement pour commettre une infraction, l'utilisation de cette technologie ne nécessite aucune modification du système de responsabilité pénale.

Une autre question à analyser est celle de savoir si l'IA, en raison de sa capacité à automatiser les processus décisionnels, à agir de manière autonome et à reproduire des actions à grande vitesse, amplifie l'ampleur des dommages causés par son utilisation, augmentant ainsi l'ampleur des dommages qui peuvent résulter de son application. L'utilisation de l'IA peut conduire à ce qu'une seule action dommageable affecte un nombre beaucoup plus important de victimes, générant des conséquences plus graves en termes d'intérêts juridiques protégés. Le droit pénal peut adopter diverses techniques pour répondre de manière appropriée à cette situation :

- La création de nouvelles infractions pénales visant spécifiquement à sanctionner les comportements à haut risque associés à l'utilisation de l'IA, ce qui permettrait une intervention précoce pour empêcher la matérialisation d'un préjudice à grande échelle.
- Adapter les sanctions des infractions existantes pour tenir compte de la gravité accrue que l'utilisation de l'IA peut entraîner.

Toutefois, ces options doivent être abordées avec prudence. Il ne s'agit pas de supposer que toutes les applications de l'IA présentent intrinsèquement des risques plus élevés, mais plutôt d'évaluer dans quels contextes et dans quelles circonstances son utilisation génère une menace suffisante pour justifier un renforcement de la réponse pénale. Cette

évaluation doit être effectuée sur la base de facteurs tels que : la nature de l'intérêt juridique protégé, la prévisibilité du préjudice, le degré de contrôle que les opérateurs humains exercent sur le système et le niveau d'autonomie du système dans la prise de décision. Dans les domaines où l'impact de l'IA sur des intérêts juridiques particulièrement sensibles, tels que la santé publique, est significatif, des mécanismes de sanction plus stricts pourraient être mis en place, pour autant qu'ils restent nécessaires et proportionnés.

Enfin, l'IA conduira également à une importance accrue de la responsabilité pénale des entreprises, étant donné que de nombreuses activités illicites associées à cette technologie ne seront pas imputables à une personne en particulier, mais plutôt aux organisations qui la mettent en œuvre sans les garanties nécessaires en matière de sécurité et de transparence. Les réglementations pénales doivent inclure des normes de diligence raisonnable imposant des obligations spécifiques aux entreprises qui développent, commercialisent ou utilisent l'IA dans leurs processus, en établissant des mécanismes d'autorégulation sous peine de sanctions pénales lorsque les contrôles internes sont insuffisants pour prévenir les infractions. Dans ce contexte, la responsabilité pénale des entreprises doit être adaptée pour couvrir les situations dans lesquelles l'IA est utilisée frauduleusement au sein d'une organisation sans qu'un auteur individuel soit clairement identifiable. Il faudra pour cela redéfinir les critères d'attribution de la responsabilité pénale des entreprises en matière de gestion des risques liés à l'IA.

En conclusion, l'émergence de l'intelligence artificielle en droit pénal exige non seulement des adaptations des réglementations existantes, mais soulève également des défis fondamentaux en termes de proportionnalité, de précision et d'attribution des responsabilités. La criminalisation des infractions liées à l'IA nécessitera la création de nouvelles infractions, la reformulation des dispositions pénales existantes et l'imposition d'obligations spécifiques de contrôle et de diligence concernant l'utilisation de l'IA. Les législateurs devront trouver un équilibre entre la prévention des risques et la protection des droits fondamentaux. Pour relever ces défis, le droit pénal doit appliquer les meilleures techniques législatives, en veillant à maintenir l'efficacité de la dissuasion tout en préservant les garanties fondamentales du droit pénal.

Le moment est venu d'analyser comment cela peut se faire dans le cadre de la Convention MEDICRIME.

3.2. Une opportunité pour MEDICRIME : sa pertinence renouvelée dans le sillage de l'IA

L'émergence de l'intelligence artificielle dans la contrefaçon de produits médicaux pose un défi supplémentaire à la Convention MEDICRIME, car elle nécessite un réexamen de sa validité et de sa pertinence dans le nouveau contexte façonné par l'IA. Toutefois, dans une certaine mesure, cela renforce également la convention, rendant encore plus évident son rôle d'instrument clé dans la lutte contre ces crimes. Comme nous l'avons vu, l'IA va accroître la sophistication de la contrefaçon, en facilitant la production de copies pratiquement impossibles à distinguer des médicaments originaux, la création de documents frauduleux et la distribution automatisée de ces produits à l'échelle mondiale.

Cette évolutivité et cette capacité d'automatisation permettraient aux groupes criminels d'opérer dans une plus grande impunité et rendraient les efforts de répression plus difficiles. À cet égard, la Convention MEDICRIME, qui exige des États qu'ils érigent ces actes en infractions pénales et encourage la coopération internationale en matière de poursuites, devient encore plus pertinente. Les mécanismes réglementaires nationaux apparaissent de plus en plus insuffisants face à cette menace mondiale, d'où la nécessité d'établir un cadre commun et coordonné entre les États pour faire face à ces risques. Un argument similaire peut être avancé concernant l'utilisation potentielle de l'IA pour détecter les schémas de distribution illicite, analyser de grands volumes de données sur les marchés numériques et suivre les transactions suspectes en crypto-monnaies. Sans aucun doute, cette technologie pourrait être utilisée pour améliorer la capacité de prévention et de réponse des États, mais cela serait encore plus efficace si ces outils étaient intégrés dans les mécanismes de coopération prévus par la Convention de manière que les pays signataires puissent anticiper les nouvelles formes de criminalité et développer des stratégies plus efficaces contre la contrefaçon de produits médicaux.

Ce qui est clair, en tout cas, c'est que pour que MEDICRIME réussisse dans un contexte technologique numérisé tel que celui décrit, une augmentation significative du nombre de pays signataires serait nécessaire, en particulier parmi ceux où la nécessité de prévenir ces comportements est la plus évidente. Par exemple, comme nous le verrons plus loin, la possibilité d'exiger des fournisseurs de services qu'ils intègrent dans leurs algorithmes des outils basés sur l'IA pour détecter et supprimer les publicités pour des médicaments contrefaits deviendra plus réalisable à mesure qu'un plus grand nombre de pays signeront la convention et exerceront une pression sur ces entreprises.

3.3. Sur les réformes et changements potentiels dans MEDICRIME

Après avoir analysé le paysage technologique numérique dans lequel s'inscrit actuellement la contrefaçon de médicaments et d'autres produits médicaux et avoir examiné les principaux aspects de l'impact de l'IA sur le droit pénal en général, il convient maintenant de se demander si MEDICRIME peut nécessiter une adaptation, soit par une modification de son texte, soit par un changement de l'interprétation de certaines dispositions.

Cette section examinera donc quatre domaines clefs :

1. La question de savoir si le simple recours à l'IA doit donner lieu à une incrimination spécifique ou à une aggravation.
2. La question de la responsabilité intentionnelle dans MEDICRIME et sa relation avec l'IA.
3. La prise en compte potentielle des logiciels médicaux en tant que produits médicaux.
4. Coopération internationale et mesures additionnelles dans le cadre de la convention MEDICRIME et leur extension éventuelle.

3.3.1. Sur l'éventuelle criminalisation explicite de l' « utilisation de l'IA » pour commettre les infractions couvertes par MEDICRIME

Il a été dit que l'IA modifiait considérablement la manière dont certains comportements sont adoptés, comme la production de médicaments contrefaits, de leurs ingrédients ou de dispositifs médicaux frauduleux ; la distribution, l'offre et le trafic intentionnel de produits médicaux contrefaits ; la falsification de documents pour faire passer des produits médicaux contrefaits pour des produits légitimes ; ou la fabrication et la commercialisation de produits médicaux sans certification appropriée ou en violation des exigences réglementaires. Toutefois, je ne pense pas que l'utilisation de systèmes d'intelligence artificielle ajoute en soi un contenu illicite à la commission de ces infractions. En fin de compte, ce qui est criminalisé dans ces cas, ce sont des comportements dans lesquels les éléments pertinents sont l'existence d'une intention frauduleuse et d'un risque qui en résulte, sans qu'il soit nécessaire de disposer de moyens spécifiques pour les commettre. En d'autres termes, les actes répréhensibles associés aux comportements incriminés ne changent pas du seul fait de l'utilisation de l'IA.

La seule incertitude est de savoir s'il en va de même pour le préjudice, c'est-à-dire l'atteinte ou le risque pour l'intérêt juridiquement protégé dans cette disposition, à savoir la santé publique. Il a été observé que l'IA non seulement optimise les processus de contrefaçon, en réduisant les coûts et en augmentant la sophistication des produits frauduleux, mais qu'elle pourrait également faciliter l'expansion de la distribution de ces médicaments, augmentant ainsi le risque pour la santé publique. L'article 13 de la Convention MEDICRIME demande déjà aux Etats de considérer comme circonstance aggravante lorsque : « les infractions de fourniture et d'offre de fourniture ont été commises en ayant recours à des moyens de distribution à grande échelle, tels que les systèmes d'information, y compris l'Internet ». A cet égard, deux options peuvent être envisagées : une éventuelle réforme de MEDICRIME pour établir des circonstances aggravantes spécifiques liées à l'IA ; ou interpréter que lorsque le paragraphe (d) de l'article 13 fait référence aux « systèmes d'information », cela inclut déjà l'IA. A mon avis, cette deuxième option est parfaitement viable. En effet, comme indiqué précédemment, la définition de la CAI (Convention-cadre du Conseil de l'Europe sur l'IA) ne fait qu'ajouter des exigences supplémentaires pour que certains systèmes informatiques soient considérés comme de l'IA, mais elle reconnaît en fin de compte l'IA comme faisant partie des « systèmes d'information ».

Cela étant dit et étant donné qu'une réforme de MEDICRIME n'est pas strictement nécessaire pour couvrir certains délits aggravés liés à l'utilisation de l'IA, nous pourrions tout de même envisager l'inclusion explicite de certains de ces délits. De nombreux législateurs utilisent des techniques d'incrimination explicite comme moyen symbolique de démontrer que le système pénal s'adapte aux nouvelles réalités, même lorsque, sans cette classification explicite, il existe déjà des infractions qui permettraient de sanctionner les mêmes comportements ou des comportements très similaires. Ainsi, par exemple, une augmentation des peines pourrait être envisagée dans les cas où des modèles génératifs d'IA sont utilisés pour :

- La création de certificats de qualité frauduleux, d'autorisations de mise sur le marché et d'autres documents falsifiés qui facilitent la distribution de produits médicaux contrefaits.
- L'utilisation d'algorithmes pilotés par l'IA pour identifier les populations vulnérables ayant des besoins médicaux spécifiques et la création de campagnes publicitaires trompeuses ciblant ces groupes, augmentant ainsi les risques pour la santé.
- L'utilisation d'outils basés sur l'IA pour contourner les systèmes de traçabilité, d'authentification et de vérification des produits médicaux.

Certains de ces comportements particulièrement graves pourraient déjà être couverts par la circonstance aggravante mentionnée ci-dessus, mais il convient de s'interroger sur l'opportunité d'en élargir le champ d'application afin que, à l'ère de l'IA, la convention MEDICRIME continue d'apporter des réponses proportionnées à la gravité de ces nouvelles dynamiques criminelles.

3.3.2. La question de la responsabilité intentionnelle dans MEDICRIME et sa relation avec l'IA

La Convention MEDICRIME est fondée sur la criminalisation des infractions intentionnelles. Comme indiqué précédemment, l'automatisation des processus par l'IA peut nécessiter le déplacement de la responsabilité pénale à des stades plus précoces, où le risque n'est pas encore totalement apparent, mais où des actions négligentes peuvent encore créer un résultat dommageable potentiel qui se matérialise plus tard. Dans ces cas, l'attribution directe de l'intention devient difficile, et c'est pourquoi, en général, l'émergence de l'IA pourrait conduire à ce que de nombreuses infractions - auparavant punies uniquement lorsqu'elles étaient commises intentionnellement - soient désormais également sanctionnées sous leur forme négligente. Toutefois, je ne pense pas que cela devrait s'appliquer aux infractions que MEDICRIME exige de criminaliser. L'extension de la responsabilité pénale aux cas où la négligence dans la conception, la mise en œuvre ou la surveillance de l'IA facilite la contrefaçon de produits médicaux impliquerait un changement de paradigme fondamental dans la convention. À l'heure actuelle, celle-ci se concentre uniquement et spécifiquement sur les infractions clairement intentionnelles, qui suivent la structure prototypique de la fraude : la tromperie conduit à une erreur qui, à son tour, entraîne un préjudice.

L'inclusion d'autres comportements négligents liés aux médicaments et aux produits médicaux entraînerait une extension significative du champ d'application de la convention, qui ne se justifierait qu'après une analyse et une réflexion beaucoup plus approfondies sur l'industrie médicale et pharmaceutique. L'utilisation de l'IA peut, comme nous l'avons vu, servir d'outil de tromperie et induire des erreurs. Par conséquent, si l'objectif de MEDICRIME reste l'incrimination des infractions intentionnelles, rien dans l'émergence de l'IA n'exige de modifier les éléments subjectifs de l'incrimination.

3.3.3. La considération potentielle des chatbots d'IA en tant que dispositif médical aux fins de MEDICRIME

Comme indiqué dans le présent document, les progrès technologiques ont conduit à l'émergence de systèmes d'IA utilisés dans le diagnostic et le traitement des maladies, tels que les chatbots médicaux. La FDA et l'EMA ont déjà commencé à réglementer certains systèmes d'IA dans la catégorie « Software as a Medical Device » (SaMD), ce qui signifie que certains produits basés sur l'IA pourraient être classés comme dispositifs médicaux. Il est donc nécessaire de clarifier si la Convention MEDICRIME devrait étendre son champ d'application pour couvrir la contrefaçon et la distribution frauduleuse de ces nouveaux produits technologiques ou si elle le fait déjà par le biais de ses dispositions.

MEDICRIME définit au sens large les dispositifs médicaux, y compris les logiciels conçus à des fins diagnostiques ou thérapeutiques. Par conséquent, l'IA appliquée aux soins de santé pourrait déjà être soumise aux dispositions de la Convention si sa contrefaçon ou sa distribution non autorisée est démontrée. L'article 8 de la convention MEDICRIME dispose ce qui suit : « Chaque Partie prend les mesures législatives et autres nécessaires pour ériger en infraction, conformément à son droit interne, les actes commis intentionnellement, dans la mesure où elles ne tombent pas sous le coup des articles 5, 6 et 7 : La fabrication, le stockage pour fourniture, l'importation, l'exportation, la fourniture, l'offre de fourniture ou la mise sur le marché de dispositifs médicaux sans respecter les exigences de conformité, lorsque cette conformité est requise en vertu du droit interne de la Partie ».

À mon avis, des comportements tels que la commercialisation et la distribution de logiciels médicaux non certifiés, ou la falsification d'interfaces et de logiciels pour imiter des outils médicaux légitimes, pourraient déjà relever des infractions pénales requises par MEDICRIME. Par exemple, la création de plateformes frauduleuses proposant des systèmes d'IA pour le diagnostic sans la validation nécessaire des autorités de santé - exposant les utilisateurs à des informations inexacts ou à des traitements dangereux - pourrait entrer dans le champ de protection de la Convention. Il en va de même pour le développement d'applications imitant des produits réglementés afin de tromper les consommateurs et les professionnels de la santé. Une incertitude subsiste quant à la question de savoir s'il en va de même pour la manipulation d'algorithmes visant à modifier les diagnostics et les traitements. La modification intentionnelle d'un chatbot médical ou d'un système de diagnostic basé sur l'IA pour tromper les patients ou les professionnels de la santé peut entraîner des conséquences dévastatrices pour la santé publique et il convient de se demander si cela devrait être explicitement répertorié comme une infraction pénale dans le cadre de MEDICRIME. Peut-être la référence à l'article 5 de MEDICRIME à : "Chaque partie prend les mesures législatives et autres nécessaires pour ériger en infraction, conformément à son droit interne, la fabrication intentionnelle de produits médicaux, substances actives, excipients, éléments, matériaux et accessoires contrefaits ». Le fait que le paragraphe 2 inclue les dispositifs médicaux parmi les objets couverts peut déjà résoudre ce problème.

Après tout, la manipulation intentionnelle d'un logiciel médical certifié pour générer des erreurs de diagnostic ou de traitement à l'aide de l'IA équivaldrait à la falsification d'un

médicament physique, car elle compromet la sécurité des patients de la même manière. Il serait toutefois souhaitable de clarifier ce point s'il existe des mécanismes pour le faire.

3.3.4. Coopération entre les autorités, échange d'informations et autres mesures complémentaires

L'un des aspects les plus importants de MEDICRIME est l'incorporation de divers mécanismes de coopération entre les autorités et d'échange d'informations. Cet aspect est régi, entre autres, par l'article 17 de la convention, et il convient de s'interroger sur l'opportunité d'adapter cet article à l'émergence de l'intelligence artificielle. Il en va de même pour le chapitre VII de la convention, en particulier les articles 21 et 22. Il est clair que l'automatisation et la sophistication de la contrefaçon par l'IA, ainsi que sa capacité à optimiser la distribution et la promotion des médicaments frauduleux dans les environnements numériques, nécessitent que la coopération internationale intègre des outils technologiques avancés et prenne rapidement en compte de nouveaux acteurs.

Une autre question, une fois de plus, est de savoir si cela doit se faire par le biais d'un amendement à MEDICRIME ou simplement par le biais d'une interprétation actualisée des dispositions existantes. Pour un échange d'informations efficace entre les autorités sanitaires, douanières et répressives, il conviendrait à l'avenir de développer des bases de données interopérables et d'intégrer des systèmes basés sur l'IA pour surveiller les produits médicaux contrefaits. Si les États adoptaient des mécanismes d'analyse des données en temps réel, intégrant des modèles d'apprentissage automatique pour détecter les schémas de fraude sur les marchés numériques et dans les médias sociaux, et partageaient ces informations entre eux, l'efficacité des interventions contre ces fraudes augmenterait. Pour cette raison, promouvoir la création d'un système d'alerte précoce normalisé basé sur l'IA au sein des points de contact uniques établis par MEDICRIME est un objectif ambitieux et peut-être irréaliste, mais qui faciliterait certainement la coopération entre les pays dans l'identification des réseaux criminels qui utilisent l'IA pour la contrefaçon et le commerce illicite de produits médicaux.

Plus important encore, sur la base de l'analyse criminologique menée précédemment, MEDICRIME, lorsqu'il aborde la question de la coopération entre les secteurs public et privé, fait explicitement référence aux fournisseurs de services numériques et aux plateformes de commerce électronique. Actuellement, de nombreux produits contrefaits sont commercialisés par le biais de publicités automatisées optimisées par l'IA, ce qui rend leur détection plus difficile à l'aide des méthodes traditionnelles. La question est de savoir si MEDICRIME pourrait encourager les États à exiger des plateformes numériques qu'elles mettent en œuvre des outils d'IA pour identifier et supprimer les publicités frauduleuses, ainsi que des protocoles de coopération obligatoires avec les autorités nationales pour partager des informations sur les schémas de fraude. Pour aller plus loin, il convient de se demander si MEDICRIME devrait explicitement faire référence à la responsabilité des fournisseurs de services numériques dans la commercialisation de produits contrefaits. Bien que MEDICRIME criminalise la distribution de médicaments contrefaits, il n'impose pas d'obligations spécifiques aux plateformes numériques et aux services en ligne où ces produits sont vendus. Cependant, l'IA facilitant la vente segmentée et à grande échelle de médicaments frauduleux, il pourrait être recommandé aux pays signataires d'exiger des places de marché en ligne et des plateformes qu'elles

mettent en place des mécanismes de surveillance active contre les produits médicaux contrefaits et qu'elles définissent les responsabilités en cas de non-respect de ces règles. De même, les États pourraient s'engager à promulguer des lois exigeant la transparence et la traçabilité dans la vente en ligne de produits médicaux, en veillant à ce que les plateformes opérant sur leur territoire coopèrent à l'identification des réseaux frauduleux.

Enfin, en ce qui concerne la formation des unités chargées de la coopération et de l'échange d'informations, l'article 17 devrait inclure une formation à l'utilisation de l'IA pour la détection des fraudes sur les produits médicaux contrefaits. Cela permettrait aux autorités de disposer des connaissances et des ressources nécessaires pour faire face aux nouvelles dynamiques criminelles facilitées par l'IA. A cet égard, MEDICRIME pourrait recommander aux Etats d'inclure, dans leurs programmes de formation des juges, des procureurs et des forces de l'ordre, des modules spécifiques sur l'impact de l'IA sur la contrefaçon de produits médicaux et les stratégies technologiques de détection et de poursuite.

En ce qui concerne la coopération internationale en matière pénale, une interprétation actualisée des articles 21 et 22 de la convention pourrait également être envisagée à la lumière de cette nouvelle réalité technologique. Par exemple, les États pourraient intégrer dans les traités de coopération des outils de criminalistique numérique basés sur l'IA afin d'analyser les preuves en ligne et de suivre les opérations de contrefaçon et de vente automatisées. En outre, la coopération internationale devrait être renforcée pour identifier et geler les actifs numériques obtenus par le commerce illicite de produits médicaux contrefaits piloté par l'IA, en veillant à ce que les États disposent de cadres juridiques compatibles pour intervenir sur ces fonds, qui peuvent exister sous la forme de crypto-monnaies. En outre, concernant l'article 22, la capacité accrue de diffusion de l'IA nécessite que les États mettent en place des canaux de signalement accessibles et numérisés pour les victimes de la fraude de produits médicaux contrefaits. En outre, ils devraient coopérer par le biais de plateformes de signalement transnationales où les personnes touchées peuvent signaler les fraudes sanitaires liées à l'IA, qui seraient ensuite redirigées vers les autorités nationales compétentes. Cela contribuerait également à renforcer la réglementation dans les régions vulnérables, en empêchant les marchés de produits médicaux contrefaits de prospérer dans les pays disposant de moins de ressources technologiques et réglementaires.

Il est vrai que nous anticipons des scénarios d'utilisation de l'IA encore peu répandus. Cependant, il a déjà été démontré que la vitesse de développement de l'IA est stupéfiante et que les autorités et le public sont toujours à la traîne. En ce sens, et pour conclure, MEDICRIME pourrait également recommander aux Etats de mettre en place des campagnes nationales de sensibilisation aux risques liés à l'IA dans la contrefaçon de produits médicaux, ciblant à la fois les consommateurs et les professionnels de santé.

Bibliographie

- Alarcón-Jiménez, O. (2015). La convention MEDICRIME - Lutte contre la contrefaçon de médicaments. *Eurohealth*, 21(4), 24-27.
- Almeman, Ahmad. "La transformation numérique en pharmacie : adoption des plateformes en ligne et changement de paradigme cosméceutique". *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. Document de réflexion sur l'utilisation de l'intelligence artificielle (IA) dans le cycle de vie des médicaments...9 septembre 2024 EMA/CHMP/CVMP/83833/2023 Comité des médicaments à usage humain (CHMP) Comité des médicaments à usage vétérinaire (CVMP)
- EUIPO : Commerce de produits pharmaceutiques contrefaits, EUIPO
- Gomasta, Sarmistha Sarna, et al. "PharmaChain : Système de vérification de la provenance de la chaîne d'approvisionnement en médicaments basé sur la blockchain". *Heliyon* 9.7 (2023).
- Islam, lyolita, et 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 et chatbots d'IA générative : défis et opportunités pour la science, la médecine et les leaders médicaux". *BMJ Leader* (2023) : leader-2023.
- Mackey, Tim K., et Gaurvika Nayyar. "Un examen des technologies numériques existantes et émergentes pour lutter contre le commerce mondial de faux médicaments." *Avis d'experts sur la sécurité des médicaments* 16.5 (2017) : 587-602.
- Mladinić, Nina, Šime Jozipović, et Marko Perkušić. "Le danger du crime organisé dans le domaine de la falsification des médicaments et des produits médicaux (profit vs. droit à la santé)." *Série de questions et défis en matière de droit européen et comparé (ECLIC)* 8 (2024) : 113-139.
- Miró-Llinares, F., Association International de Droit Pénal - International Association of Penal Law XXI International Congress of Penal Law : "Intelligence artificielle et justice pénale", Colloque international de la section II (infractions spécifiques au droit pénal dans le code pénal), 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. et Rusu, A. (2020). La sérialisation pharmaceutique, un effort mondial pour lutter contre les médicaments contrefaits. *Acta Marisiensis-Seria Medica*, 66(4), 132-139.
- Singh, Kumkum, et al. "Integrating the AI-Driven Technologies Into Pharmaceutical Service Marketing". *Intégrer les technologies pilotées par l'IA dans le marketing des services*. 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 (Avancées dans le marketing numérique à l'ère de l'intelligence artificielle)*. CRC Press 267-278.
- Venhuis, B. J., Oostlander, A. E., Di Giorgio, D., Mosimann, R., & du Plessis, I. (2018). Les médicaments oncologiques dans le collimateur de la criminalité pharmaceutique. *The Lancet Oncology*, 19(4), e209-e217.