COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 19 September 2025 CDPC-AICL(2025)01

EUROPEAN COMMITTEE

ON CRIME PROBLEMS

(CDPC)

Working Group on Artificial Intelligence and Criminal Law

(CDPC-AICL)

COMPILATION OF NATIONAL RESPONSES TO THE CDPC-AICL QUESTIONNAIRE ON ARTIFICIAL INTELLIGENCE AND CRIMINAL LIABILITY – 2025

Document prepared by the CDPC Secretariat

Directorate General I – Human Rights and Rule of Law

www.coe.int/cdpc | dgi-cdpc@coe.int

Contents

BELGIUM

A: Cadres existants

1. **Votre législation nationale et/ou votre jurisprudence abordent-elles spécifiquement la responsabilité pénale ou les infractions liées à l'intelligence artificielle ?**
   Le cas échéant, pourriez-vous s'il vous plaît :
   (1) fournir, si disponible, les textes pertinents (en anglais ou en français) ;
   (2) indiquer si la responsabilité pénale est attribuée à une personne spécifique (physique ou morale, par exemple : conducteur, producteur, programmeur, superviseur de flotte, téléopérateur, etc.) et sur quel fondement elle repose (à savoir : responsabilité objective, négligence, intention).
   Dans le cas contraire, les règles générales s'appliqueront-elles dans les situations où des infractions sont commises, facilitées, renforcées ou assistées par l'intelligence artificielle ?

Pour l'instant, ce sont les règles générales qui s'appliquent.

2. **Quelles règles générales sont appliquées dans votre droit lorsque des systèmes d'intelligence artificielle (tels que définis à l'article 2 de la CAI, STCE n° 225) sont utilisés comme outils pour la commission intentionnelle d'infractions pénales (telles que le meurtre, l'homicide involontaire ou le vol) ?**

La doctrine fait observer qu'il existe des incertitudes en la matière. Il y a tout d'abord la question de l'existence d'une personnalité juridique pour un système d'intelligence artificielle et, quand bien même cet obstacle serait levé, cela ne ferait pas disparaître les réserves légitimes quant à l'application à l'IA du concept éminemment moral de culpabilité. Ainsi, il semble actuellement impossible de rendre un système d'IA pénalement responsable en tant que tel sur la base du droit pénal. D'ailleurs, même si c'était le cas, la question se poserait encore de savoir s'il est judicieux d'imposer les sanctions actuelles à des systèmes d'IA. Pour l'instant, la règle *machina delinquere non potest*[1] s'applique.

En ce qui concerne l'imputation objective du comportement d'un système d'IA à un sujet de droit, on peut constater qu'en pratique, il y aura des incertitudes quant à la responsabilité pénale de l'utilisateur en dehors des cas où celui-ci a un contrôle total ou n'a aucun contrôle sur le système d'IA. Au niveau du créateur, l'incertitude découle en outre de la complexité des systèmes d'IA lorsque plusieurs personnes interviennent dans leur création. Plus il y a de personnes impliquées dans ce processus, plus il est difficile d'identifier la personne pénalement responsable en cas de problème. Par ailleurs, il existe des formes évolutives d'IA dont il résulte une distance croissante entre le comportement du système d'IA et son créateur qui est directement proportionnelle à l'évolution de ce système[2].

En ce qui concerne l'imputation subjective, à savoir la détermination de la composante morale dans le chef de l'utilisateur ou du créateur d'un système d'IA, on peut constater qu'en dehors des cas où le système est utilisé ou programmé expressément à cette fin, on peut s'attendre à ce que

[1] Julie PETERSEN, *AI criminaliteit. Nieuwe uitdagingen in het (ondernemings)strafrecht*, Louvain, éditions LeA, 2024, n° 57-58, p. 49-50.
[2] Vincente KERKHOFS, "Artificiële intelligentie en strafrechtelijke verantwoordelijkheid", *Nullum Crimen* 2022, p. 26.

la plupart des infractions intentionnelles restent impunies. En ce qui concerne les infractions commises par négligence, il convient de conclure qu'ici aussi, il y aura des incertitudes dans la pratique quant à la responsabilité pénale de l'utilisateur en dehors des cas de contrôle total ou d'absence de contrôle sur le système d'IA, en particulier en ce qui concerne la question de savoir si la responsabilité d'empêcher les comportements punissables lui incombait. En outre, le caractère évolutif d'un système d'IA influe également sur la détermination de la composante morale, en ce sens qu'il peut constituer un obstacle à la détermination de la prévisibilité des conséquences, condition nécessaire pour pouvoir établir la négligence[3].

3. **Selon votre droit interne et/ou votre jurisprudence, l'utilisation de systèmes d'intelligence artificielle peut-elle être considérée comme une circonstance aggravante ?**

Il n'est pas prévu que l'utilisation de systèmes d'IA puisse être considérée comme une circonstance aggravante.

4. **Votre législation traite-t-elle de l'utilisation de technologies spécifiques d'intelligence artificielle pour commettre des infractions, par exemple l'utilisation de deepfakes dans certains contextes (tels que les deepfakes à caractère sexuel, le harcèlement sexuel en ligne, ou lors des processus électoraux), l'utilisation de drones autonomes pour tuer quelqu'un, ou des formes spécifiques de fraude ?**

Cela repose sur un certain nombre de dispositions du droit européen et sur les incriminations de droit commun[4].

Ainsi, l'art. 50 de la loi sur l'IA prévoit un certain nombre d'obligations de transparence pour les systèmes d'IA qui génèrent ou manipulent des images ou des contenus audio ou vidéo constituant un hypertrucage (deepfake). En vertu de la loi sur l'IA, ces sorties doivent être explicitement identifiables comme telles (« ayant été générées ou manipulées par une IA »). Il est important de noter que cette obligation ne s'applique qu'aux fournisseurs et aux déployeurs de systèmes d'IA qui produisent des deepfakes. Compte tenu des définitions restrictives de ces notions à l'article 3 de la loi sur l'IA, les utilisateurs qui emploient un système d'IA « dans le cadre d'une activité personnelle à caractère non professionnel » sont exclus du champ d'application du règlement, ce qui limite la portée de celui-ci.

Un deuxième outil législatif pertinent dans ce cadre est le règlement sur les services numériques, lequel a été assorti, mi-2022, d'un code de conduite plus strict sur la désinformation[5]. Les signataires de ce code, qui comprennent d'importantes plateformes en ligne telles que Google et Meta, se sont ainsi engagés, entre autres, à rendre la diffusion de deepfakes moins attrayante financièrement et à fournir aux utilisateurs de meilleurs outils pour reconnaître, comprendre et repérer les « fausses » informations. Bien que le code repose sur une base volontaire (par exemple, X (anciennement Twitter) s'en est retiré l'année dernière), il pourrait s'avérer un outil utile dans la lutte contre les fausses informations.

En fonction de la situation concrète dans laquelle se produisent les deepfakes, de très nombreuses infractions de droit commun sont pertinentes. Pensons par exemple, dans le cadre des deepnudes, à certaines infractions sexuelles telles que la diffusion non consentie de contenus à caractère

[3] Vincente KERKHOFS, "Artificiële intelligentie en strafrechtelijke verantwoordelijkheid", *Nullum Crimen* 2022, p. 26.
[4] Julie PETERSEN, *AI criminaliteit. Nieuwe uitdagingen in het (ondernemings)strafrecht*, Louvain, éditions LeA, 2024, n° 16-20, p. 11-13.
[5] Disponible via https://digital-strategy.ec.europa.eu/fr/policies/code-practice-disinformation

sexuel (art. 417/9 du Code pénal, la détention et la diffusion d'images d'abus sexuels de mineurs (art. 417/43 à 417/49 du Code pénal) ou même au voyeurisme (art. 417/8 du Code pénal)[6].

En fonction du contexte dans lequel les deepfakes sont utilisés, ils pourraient également relever de la qualification infractionnelle de certains délits d'expression, tels que la calomnie et la diffamation (art. 443 du Code pénal) ou l'incitation à la haine sur la base de l'un des critères protégés (art. 20 de la loi antiracisme, art. 22 la loi antidiscrimination et art. 27 de la loi genres).

Dans le contexte du droit pénal des sociétés, il convient d'évoquer les infractions suivantes : l'escroquerie (art. 496 du Code pénal) et la fraude informatique (art. 504*quater* du Code pénal) ainsi que le faux en écritures (art. 193 à 196 du Code pénal) et le faux en informatique (art. 210*bis* du Code pénal).

5. **L'utilisation de l'IA est-elle considérée comme une circonstance aggravante, notamment dans les cas impliquant :**
   - ☐ **deepfakes à caractère sexuel**
   - ☐ **harcèlement sexuel en ligne**
   - ☐ **processus électoraux**
   - ☐ **utilisation de drones autonomes pour tuer quelqu'un**
   - ☐ **fraude d'une importance notoire**
   - ☐ **autre : …**

Une telle circonstance aggravante n'existe pas.

6. **Y a-t-il des exemples de jurisprudence nationale ou de pratiques d'enquête (par exemple, enquêtes pénales, évaluations du parquet) impliquant des infractions commises ou facilitées par l'intelligence artificielle ? Si oui, merci de résumer le(s) cas ou de décrire les problématiques, si possible.**

Nous n'avons pas connaissance d'une jurisprudence ou de pratiques d'enquête pénale nationales concernant des infractions commises par l'intelligence artificielle.

B. Plans futurs

1. **Le législateur de votre pays prévoit-il des réformes législatives concernant la responsabilité (pénale) et les infractions liées à l'IA ?**

La matière doit faire l'objet d'une évaluation avant toute décision quant à l'opportunité d'entreprendre une réforme législative.

2. **Le législateur de votre pays prévoit-il des réformes législatives concernant les circonstances aggravantes lorsque qu'une infraction est commise, facilitée, renforcée ou assistée par l'utilisation de systèmes d'IA ?**

La matière doit faire l'objet d'une évaluation avant toute décision quant à l'opportunité d'entreprendre une réforme législative.

[6] Pour de plus amples informations à ce sujet, voir S. ROYER et C. CONINGS, « Catfishing, cyberbullying, deepfakes, dickpics, doxing, grooming, sextortion... Cyberfenomenen en hun strafrechtelijke kwalificaties", droit PI et ICT 2023, vol. 125, 81-153.

3. **Votre législateur envisage-t-il de relever les nouveaux défis liés à la protection effective des droits mis en péril par l'utilisation des systèmes d'IA par des mesures autres que l'adoption de nouvelles lois pénales ? Si oui, comment ?**
   Le législateur de votre pays prévoit-il des réformes législatives concernant la protection du droit d'auteur en lien avec l'utilisation de l'IA (par exemple, en raison du web scraping, du web harvesting ou de l'extraction de données à partir de sites web pour entraîner des modèles linguistiques de grande taille) ?

La matière doit faire l'objet d'une évaluation avant toute décision quant à l'opportunité d'entreprendre une réforme législative.
En ce qui concerne spécifiquement la protection du droit d'auteur, on peut en principe s'appuyer sur l'article XI.293 du CDE ,qui prévoit le délit de contrefaçon[7]. La doctrine est plutôt d'avis que cela ne peut être imputé à un système d'intelligence artificielle. Une distinction est établie à cet égard entre 2 situations. 1° Si le système d'IA est utilisé en tant qu'outil technique, il reste un auteur humain ; 2° Si l'IA génère des résultats de manière autonome sans intervention d'un être humain dans le traitement final des données, il n'y a pas de protection des droits d'auteur puisqu'un droit d'auteur ne peut exister qu'à l'égard d'une personne humaine[8].

4. **Le législateur de votre pays prévoit-il des réformes législatives concernant le développement d'applications facilitant la production de deepfakes (à caractère sexuel), ou l'utilisation ou la diffusion de deepfakes (à caractère sexuel) ?**

La matière doit faire l'objet d'une évaluation avant toute décision quant à l'opportunité d'entreprendre une réforme législative.

5. **Au regard de votre contexte national et des évolutions juridiques, existe-t-il d'autres comportements ou activités impliquant l'intelligence artificielle que vos autorités estiment devoir être pénalement réprimés à l'avenir ? Le cas échéant, veuillez décrire ces comportements et, si possible, en expliquer les raisons.**

La matière doit faire l'objet d'une évaluation avant toute décision quant à l'opportunité d'entreprendre une réforme législative à cet égard en vue d'incriminer d'autres comportements ou activités.

C. Évaluation de la nécessité d'un nouvel instrument

1. **Voyez-vous la nécessité d'un nouveau type d'infraction liée à l'IA obscure (« dark AI ») ?**
   (Ceci fait référence aux systèmes d'IA spécialement conçus à des fins malveillantes, tels que le piratage, le cracking ou d'autres cyberattaques, ainsi qu'aux IA destinées à cibler les infrastructures critiques, à créer des risques sérieux pour la sécurité publique ou à faciliter la commission de toute infraction.)

Aucune incrimination spécifique n'est nécessaire pour l'instant.

[7] Julie PETERSEN, *AI criminaliteit. Nieuwe uitdagingen in het (ondernemings)strafrecht*, Louvain, éditions LeA, 2024, n° 90-92, p. 74-75.
[8] F. GOTZEN en M.-C. JANSSENS, "Kunstmatige Kunst. Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", Auteurs en Media 2018-2, n° 3, 323-342.

2. **Considérez-vous qu'il est nécessaire d'introduire un nouveau type d'infraction visant à réprimer la mise sur le marché, la mise en service, la production, l'acquisition pour usage personnel, l'importation ou la fourniture à des tiers – sous quelque forme que ce soit – d'un système d'IA interdit par la législation nationale ou européenne ?**

Aucune incrimination spécifique n'est nécessaire pour l'instant.

3. **Considérez-vous nécessaire d'adopter des mesures spécifiques pour traiter le « dilemme de la négligence » résultant des actions autonomes des systèmes d'IA ?**

Pour l'instant, aucune mesure spécifique n'est prise à cet effet.

4. **Voyez-vous la nécessité de créer un instrument international (Convention sur l'IA et les infractions) similaire à la Convention de Budapest sur la cybercriminalité, qui définirait et pénaliserait les actes pouvant être commis, facilités, renforcés ou aidés par des systèmes d'IA ?**

Une telle convention pour les aspects pénaux n'est pas forcément nécessaire eu égard à la problématique de l'imputation à un système d'IA et à l'impossibilité d'imposer des sanctions à un système d'IA. Elle peut permettre aux États membres de prévoir un cadre législatif pénal spécifique en la matière.

D. Contenu d'un éventuel nouvel instrument, s'il est élaboré

1. **Selon vous, quels éléments suivants un éventuel nouvel instrument international (Convention sur l'IA et les infractions) pourrait-il inclure ?**

□ **définitions**
□ **dispositions procédurales**
☐ **dispositions relatives à la compétence juridique**
☐ **questions d'extradition et d'entraide judiciaire**
☐ **problématiques liées aux preuves numériques**
☐ **collaboration des plateformes numériques d'IA avec les poursuites pénales**
☐ **autres questions …**

Un nouvel instrument éventuel devrait déjà comporter tous ces éléments.

2. **Êtes-vous d'accord pour que les définitions s'alignent sur celles de la loi sur l'IA (AI Act) ? Merci de préciser.**

Il semble indiqué à cet égard d'aligner la terminologie sur celle de la loi sur l'IA.

3. **Parmi les questions ci-dessus (le cas échéant), lesquelles considérez-vous comme les plus urgentes à traiter en matière d'IA et de droit pénal ?**

Compte tenu de ce qui précède, il n'y a pas de questions urgentes à cet égard.

4. **Quels seraient, selon vous, les avantages ou les inconvénients d'un instrument mondial unique traitant de l'IA et du droit pénal, par rapport à des lois distinctes dans des domaines spécifiques ?**

Les inconvénients sont la préférence pour une approche civile, la responsabilité civile et la responsabilité du fait des produits.

Les avantages sont la prévision de comportements pénaux spécifiques dans le domaine de l'IA qui lèvent les difficultés éventuelles dans l'application des incriminations de droit commun.

BOSNIA AND HERZEGOVINA

A: Existing Frameworks

1. **Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?**
   If so, could you please:
   (1) provide, if available, the relevant texts (in English or in French);
   (2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
   If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Criminal legislation in Bosnia and Herzegovina currently does not contain specific provisions governing criminal liability in the context of criminal offences related to the use of artificial intelligence (AI) and machine learning. Furthermore, at this stage we are unable to provide relevant case law of the Court of Bosnia and Herzegovina, as it remains uncertain whether there is any case law addressing the criminal liability of natural or legal persons who have, intentionally or negligently, used artificial intelligence for the purpose of committing criminal offences under the Criminal Code of Bosnia and Herzegovina. In the context of the use of modern technologies, including artificial intelligence, it is important to emphasise that the legal framework of the Federation of Bosnia and Herzegovina recognises computer-related criminal offences and prescribes sanctions against them. These criminal offences are regulated under Chapter XXXII of the Criminal Code of the Federation of Bosnia and Herzegovina and cover computer fraud, disruption of electronic data processing systems and networks, and unauthorised access to electronic data processing protected system and network, with the legislation aligned with the provisions of the Budapest Convention. The Criminal Code of the Republika Srpska regulates these offences under Chapter XXXII, as well as the Criminal Code of the Brčko District of Bosnia and Herzegovina.
Bosnia and Herzegovina has not yet adopted a national cybersecurity strategy or specific legislation addressing artificial intelligence, meaning that its current legislation is not fully aligned with international conventions such as the Budapest and Lanzarote Conventions. The legislative framework in Bosnia and Herzegovina is outdated when it comes to new forms of digital crime.
1) Relevant texts: There are no specific laws related to AI available in English or French.
2) Criminal responsibility is attributed to natural persons, based on general rules on intent or negligence. AI itself is not considered a subject of criminal liability.
The legislation of the Brčko District of BiH, namely the Criminal Code of the Brčko District of BiH, does not recognize the term "artificial intelligence", nor does it prescribe a criminal offense directly related to it, however, Chapter XXXII of the Criminal Code of the Brčko District of BiH prescribes criminal offenses against electronic data processing systems, namely:
Article 387 Damage to computer data and programs, what work does he do:
(1) Whoever damages, alters, deletes, destroys or otherwise renders another person's computer data or computer programs unusable or inaccessible shall be punished by a fine or imprisonment for a term not exceeding one year.
(2) Whoever, despite protective measures, accesses computer data or programs without authorization or intercepts their transmission without authorization, shall be punished by a fine or imprisonment for a term not exceeding three years. Whoever disables or hinders the operation or use of a computer system, computer data or programs or computer communication shall be punished by the punishment referred to in paragraph 2 of this Article.
(3) If the criminal offense referred to in paragraphs 1 to 3 of this Article is committed in relation to a computer system, data or program of a government body, public service, public institution or company of special public interest, or if significant damage is caused, it shall be punishable by imprisonment for a term of three months to five years.
(4) Whoever, without authorization, manufactures, acquires, sells, possesses or makes available to another special devices, means, computer programs or computer data created or adapted for

the purpose of committing the criminal offense referred to in paragraphs 1 to 3 of this Article, shall be punished by a fine or imprisonment for a term not exceeding three years.
(5) Special devices, means, computer programs or data created, used or adapted for the purpose of committing criminal offenses, with which the criminal offense referred to in paragraphs 1 to 3 of this Article was committed, shall be confiscated.

Article 388 Computer forgery:
(1) Whoever, without authorization, creates, enters, modifies, deletes or renders unusable computer data or programs that have value for legal entities, with the aim of using them as real or using such data or programs himself, shall be punished by a fine or imprisonment for a term not exceeding three years.
(2) If the criminal offense referred to in paragraph 1 of this Article is committed in relation to computer data or programs of a body, public service, public institution or company of special public interest, or if significant damage is caused, it shall be punishable by imprisonment for a term of three months to five years.
(3) Whoever, without authorization, manufactures, acquires, sells, possesses or makes accessible to another special devices, means, computer programs or computer data created or adapted for the purpose of committing the criminal offense referred to in paragraphs 1 and 2 of this Article, shall be punished by a fine or imprisonment for a term not exceeding three years.
(4) Special devices, means, computer programs or data created, used or adapted for the purpose of committing criminal offenses, with which the criminal offense referred to in paragraphs 1 or 2 of this Article was committed, shall be confiscated.
Article 389 Computer fraud:
(1) Whoever, without authorization, enters, damages, alters or conceals computer data or a program or otherwise influences the outcome of electronic data processing with the aim of obtaining unlawful material gain for himself or another and thereby causing material damage to another, shall be punished by imprisonment for a term of six months to five years.
(2) If the criminal offense referred to in paragraph 1 of this Article resulted in the acquisition of property exceeding 10,000 KM, the perpetrator shall be punished by imprisonment for a term of two to ten years. (3) If the criminal offense referred to in paragraph 1 of this Article resulted in the acquisition of property exceeding 50,000 KM, the perpetrator shall be punished by imprisonment for a term of two to twelve years.
(4) Whoever commits the criminal offense referred to in paragraph 1 of this Article solely with the aim of causing harm to another person shall be punished by a fine or imprisonment for a term not exceeding three years.
Article 390 Interference with the operation of electronic data processing systems and networks:
Whoever, by unauthorized access to an electronic data processing system or network, causes a standstill or disrupts the operation of that system or network shall be punished by a fine or imprisonment for a term not exceeding three years.
Article 391 Unauthorized access to a protected electronic data processing system and network:
(1) Whoever unauthorizedly accesses an electronic data processing system or network in violation of protection measures shall be punished by a fine or imprisonment for a term not exceeding one year.
(2) Whoever uses information obtained in the manner referred to in paragraph 1 of this Article shall be punished by imprisonment for a term not exceeding three years.
(3) If the criminal offense referred to in paragraph 2 of this Article causes serious consequences to another person, the perpetrator shall be punished by imprisonment for a term of six months to five years.
Article 392 Computer sabotage:
Whoever enters, alters, deletes or conceals computer data or a program or otherwise interferes with a computer system, or destroys or damages electronic data processing devices with the aim of disabling or significantly disrupting the electronic processing of data of importance to government bodies, public services, public institutions, commercial companies or other legal entities of special public interest, shall be punished by imprisonment for one to eight years.
Regarding general rules on liability, the Criminal Code of the Brčko District of BiH provides the following:
APPLICATION OF CRIMINAL LAW IN BRČKO DISTRICT

Exclusion of the application of criminal legislation in the Brčko District of BiH to children who have not reached the age of 14.
Article 9
Criminal legislation in the Brčko District does not apply to a child who was under the age of fourteen at the time of the commission of the criminal offense.
Application of criminal legislation in the Brčko District towards minors
Article 10
Criminal legislation in the Brčko District is applied to minors in accordance with the Law on the Protection and Treatment of Children and Minors in Criminal Procedure of the Brčko District of BiH.
Application of criminal legislation in the Brčko District to legal entities
Article 11
Criminal legislation in the Brčko District shall apply to legal persons in accordance with Chapter XIV (Liability of Legal Persons for Criminal Offences) of this Law and other laws in the Brčko District.
Application of criminal legislation of the Brčko District to anyone who commits a criminal offense on the territory of the Brčko District
Article 12
(1) The criminal legislation of the Brčko District shall apply to anyone who commits a criminal offense on the territory of the Brčko District.
(2) The criminal legislation of the Brčko District shall apply to anyone who commits a criminal offense on a domestic vessel, regardless of where the vessel was located at the time the criminal offense was committed.
(3) The criminal legislation of the Brčko District shall apply to anyone who commits a criminal offense on a domestic aircraft while it is in flight, regardless of where the aircraft was located at the time the criminal offense was committed.
Application of the criminal legislation of Brčko District to a resident of Brčko District who commits a criminal offense abroad and a foreigner who commits a criminal offense abroad
Article 13
(1) The criminal legislation of the Brčko District applies to a resident of the Brčko District when he commits a criminal offense abroad, if he finds himself on the territory of the Brčko District or is extradited.
(2) The criminal legislation of the Brčko District shall also apply to a foreigner who commits a criminal offense against the Brčko District or its residents outside its territory, if he is found on the territory of the Brčko District or is extradited.
(3) The criminal legislation of the Brčko District is also applied to a foreigner who commits a criminal offense against a foreign state or a foreigner abroad for which, according to the law of that state, imprisonment of five years or a heavier sentence can be imposed, when found in the territory of the Brčko District. If this law does not prescribe otherwise, the court in such a case cannot impose a punishment more severe than the punishment prescribed by the law of the country where the criminal offense was committed.
(4) If, in cases referred to in Article 12 of this Law, criminal proceedings have been initiated but have not been legally completed in another state, the Prosecutor of the Brčko District shall decide whether to initiate prosecution.
(5) In cases referred to in Article 13 of this Law, prosecution shall be undertaken only when the criminal offence is also punishable under the law of the country in which the offence was committed. Even in such a case, prosecution shall not be undertaken if, under the law of that country, prosecution is undertaken at the request of the injured party, and such a request has not been submitted.
(6) The prosecutor may initiate the prosecution referred to in Article 13, paragraph 3 of this Law, regardless of the law of the country in which the criminal offense was committed, if the offense in question was considered a criminal offense under the rules of international law at the time it was committed.
(7) In cases referred to in Article 12 of this Law, the prosecution of foreigners may be transferred to a foreign state under conditions of reciprocity.
Application of the general part of this law
Article 14

(1) The provisions of the general part of this law shall apply to perpetrators of all criminal offenses prescribed by laws in the Brčko District.
(2) The provisions of the general part of this law shall apply to minors, unless otherwise prescribed by law.
(3) The provisions of the general part of this Law shall apply to legal entities, unless otherwise prescribed by this Law.

2. **What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?**

General rules of criminal law, such as the principles of fault, intent or negligence, as well as the general principles of punishment and evidence in criminal proceedings, apply in such cases. Accordingly, criminal liability for a criminal offence committed with the assistance of an AI system is attributed to the actual persons (natural or legal) who developed, used or operated the system, provided that their fault can be established. At present, the general provisions of criminal law would apply. Thus, a person who uses or operates a particular AI system and whose acts or omissions lead to the commission of an offence is held criminally liable (e.g., operator, programmer, client, etc.).
The Criminal Code of the Brčko District of BiH does not recognize tools for the intentional commission of criminal offenses (such as murder, manslaughter, or theft) when using AI systems.

3. **According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?**

In Bosnia and Herzegovina, there is currently no specific case law or legal provision explicitly addressing the use of AI systems as an aggravating circumstance in the commission of a criminal offence. Nevertheless, courts may, in line with the general principles of criminal law, take into consideration the method and means of committing an offence. Where the use of an AI system is intentional and served the commission of a criminal offence, it may be regarded as an aggravating circumstance, on account of the increased social harmfulness, the degree of threat, or the violation of a protected legal good.
The Criminal Code of the Brčko District of BiH, Article 49 General Rules for Sentencing, paragraph 1, stipulates the following: "The court shall impose a sentence on the perpetrator of a criminal offense within the limits prescribed by law for that criminal offense, taking into account the purpose of punishment and taking into account all circumstances that influence the sentence to be lower or higher (mitigating and aggravating circumstances), and in particular: the degree of guilt, the motives for the crime, the severity of the threat or violation of protected property, the circumstances under which the crime was committed, the perpetrator's previous life, his personal circumstances and his behavior after the crime was committed, as well as other circumstances relating to the perpetrator's personality." Therefore, the aforementioned article does not explicitly stipulate the use of AI systems as an aggravating circumstance.

4. **Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?**

Current legislation does not contain explicit provisions addressing the use of specific AI technologies, such as deepfakes, small unmanned aerial vehicles (drones), or other forms of AI, for the purpose of committing or attempting to commit criminal offences. Nevertheless, existing criminal law applies to offences committed with the aid of such technologies, including fraud, homicide, sexual abuse, violations of privacy, and offences concerning the protection of children and other vulnerable groups. Expert discussions and considerations are ongoing on possible amendments to the legislation, with a view to ensuring a more effective and timely response to the challenges posed by the development of artificial intelligence.
Note:

- Concerns have been raised regarding the emergence of so-called deepfake sextortion, i.e. blackmail based on fabricated sexual recordings. Such offences are currently prosecuted under the general provisions on blackmail, extortion, or unauthorised recording.
- Judicial and investigative experts report a growing number of cases involving the misuse of AI tools (e.g., DeepNude) to generate unauthorised sexualised images.
- As part of international investigations (e.g., INTERPOL), a case was recorded in Bosnia and Herzegovina, revealing a network engaged in the production of child sexual abuse material using AI technologies.

The Criminal Code of the Brčko District of BiH does not address the use of specific AI technologies to commit criminal offenses/crimes, e.g. the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of self-piloted drones to kill someone, or specific forms of fraud.

5. **Is the use of AI considered an aggravating circumstance, particularly in cases involving:**
   - ☐ **sexual deepfakes**
   - ☐ **online sexual grooming**
   - ☐ **electoral processes**
   - ☐ **use of autonomous drones to kill someone**
   - ☐ **fraud of notorious importance**
   - ☐ **other: …**

Under the current criminal law framework, the use of artificial intelligence is not explicitly prescribed as an aggravating circumstance. However, general principles of punishment and evidence in criminal proceedings will apply, as indicated in our reply to the second question in your questionnaire.

Article 48 of the Criminal Code of Bosnia and Herzegovina (Official Gazette of BIH, no. 3/2003, 32/2003-correction, 37/2003, 54/2004,61/2004, 30/2005, 53/2006, 55/2006, 8/2010, 47/2014, 22/2015, 40/2015,35/2018, 46/2021, 31/2023 and 47/2023) prescribes the following:

(1) The court shall impose the punishment within the limits provided by law for that particular offence, having in mind the purpose of punishment and taking into account all the circumstances bearing on the magnitude of punishment (extenuating and aggravating circumstances), and, in particular: the degree of guilt, the motives for perpetrating the offence, the degree of danger or injury to the protected good, the circumstances in which the offence was perpetrated, the past conduct of the perpetrator, his personal situation and his conduct after the perpetration of the criminal offence, as well as other circumstances related to the personality of the perpetrator.

(2) In ruling on the punishment for the criminal offence in recidivism, the court shall take into special consideration whether the most recent offence is of the same type as the previous one, whether both acts were perpetrated from the same motive, and it will also consider the period of time which has elapsed since the pronunciation of the previous conviction, or since the punishment has been served or pardoned.

(3) In fixing a fine, the court shall take into consideration the situation of the perpetrator in terms of property, taking into account the amount of his salary, his other income, his assets and his family obligations.

Judicial and investigative authorities are, however, faced with an increasing number of cases in which AI has been used as a means to commit or facilitate criminal offences. In this context, although AI is not formally considered an aggravating circumstance, the fact that the perpetrator used sophisticated technology, including AI tools, may, under a broader interpretation, be taken into account when assessing the degree of culpability, intent and seriousness of the offence. This, in turn, may influence the gravity of the sanction in a specific case.

In cases such as:

- sexual deepfake manipulations;
- AI-generated materials used in sextortion;
- online grooming supported by chatbots or deepfake identities;
- manipulation of electoral information through generative AI;
- fraud facilitated by false AI simulations of persons,

there is clear awareness among domestic authorities of the harmfulness of these practices and the need for a regulatory response; however, the legal framework has yet to systematically address these forms of crimes.
The use of AI is not considered an aggravating circumstance in the context of the Criminal Code of the Brčko District of BiH, given that the aforementioned law does not recognize the concept of the use of AI in its content, but it could be interpreted as such in light of judicial and prosecutorial practice, which is within the jurisdiction of the aforementioned judicial authorities.

6. **Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.**

Although there are no final court decisions explicitly addressing criminal offences committed through the use of artificial intelligence, there is relevant investigative practice and professional awareness of the growing challenges associated with AI.

- As part of international investigations conducted in cooperation with partner agencies (e.g., Europol, Interpol), cases were identified involving the use of tools to generate false sexualized images of minors (deepfake content), which resulted in the arrest of several suspects in Bosnia and Herzegovina. These offences were prosecuted under the existing criminal provisions on child pornography and abuse of information technology, as the law does not yet recognise “AI-generated content” as a separate category.
- At judicial forums and training sessions, cases were presented in which artificial intelligence was used to manipulate or blackmail victims through falsely generated images, and experts have warned of the growing prevalence of sextortion and other forms of digital violence facilitated by AI tools (e.g., DeepNude and similar applications).
- In proceedings concerning high-tech crime, courts in Bosnia and Herzegovina have begun to accept evidence from encrypted applications (Sky ECC, ANOM). Although not directly related to AI, these investigations open the possibility of using AI technology for the analysis and verification of digital evidence.
- According to statements by investigators and court experts, prosecutors’ offices in Bosnia and Herzegovina have expressed concern about the possible misuse of AI in political manipulation and electoral campaigns, but no specific cases have yet been prosecuted before the competent courts.

The issue does not concern the Judicial Commission of the Brčko District of BiH, it is within the jurisdiction of the Brčko District Police of BiH, the Brčko District Prosecutor's Office of BiH and the courts of the Brčko District of BiH.

B. Future plans

1. **Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?**

Although there are currently no legislative proposals specifically regulating criminal liability related to AI, Bosnia and Herzegovina is closely monitoring developments in domestic and international criminal law and is prepared and open to adjustments that would enable more effective prosecution of AI-related criminal offences.
At its 81st regular session, held on 12 June 2025, the Council of Ministers of Bosnia and Herzegovina adopted the draft Basis for Accession to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. At the same session, the Ministry of Human Rights and Refugees of Bosnia and Herzegovina was tasked with submitting all necessary documentation, following the signing of the Convention, to the Ministry of Foreign Affairs of Bosnia and Herzegovina in order to initiate the official ratification process. The Ministry of Foreign Affairs expressed support for the signing of this important Convention, noting its full alignment with the provisions of international law. The text of the Framework Convention also received positive opinions from the relevant ministries at the state, entity and cantonal level, as well as at the level of the Brčko District of Bosnia and Herzegovina.

By signing this Framework Convention, Bosnia and Herzegovina will undertake the obligation to enact new and align existing laws and by-laws in accordance with the Convention, with the aim of strengthening the protection of human rights and the rule of law, which could also impact amendments to the criminal law framework in combating the misuse of artificial intelligence.
The Statute of the Brčko District of BiH in Article 1 Basic Principles, paragraph 4, stipulates the following: The Constitution of Bosnia and Herzegovina, as well as the applicable laws and decisions of the institutions of Bosnia and Herzegovina, are directly applicable throughout the territory of the District. The laws and decisions of all authorities of the District must be in accordance with the applicable laws and decisions of the institutions of Bosnia and Herzegovina. Accordingly, if future amendments to the criminal law include the issue of artificial intelligence, they will be incorporated into the laws of the Brčko District of BiH.

2. **Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?**

There are currently no planned legal reforms regarding aggravating circumstances when a criminal offense/crime is committed, enabled, enhanced, or assisted through the use of AI in Brčko District of BiH.

3. **Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?**
   Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

Although there is currently no formal initiative, judicial authorities and experts emphasize the need for:
- alignment with European Union legislation (e.g., the AI Act),
- continuous education of judges, prosecutors and investigators,
- institutional strengthening of capacities for detecting and prosecuting AI-related crimes.

At the state level, Bosnia and Herzegovina has the Law on Consumer Protection (Official Gazette of BiH, No. 25/2006 and 88/2015), which contains certain relevant provisions that may be useful in the context of protecting consumer rights endangered by the use of advanced AI tools by producers and traders. Article 29 of this Law stipulates that advertising of products and services must not contravene laws or other regulations, offend human dignity or violate fundamental human, economic, social or cultural rights. Paragraph 2) further provides that advertisements must not contain any statement or visual representation which, directly or indirectly, by omission, ambiguity, or exaggeration, could mislead consumers, especially regarding the characteristics of a product, its usability, effectiveness and effects, quantity, quality, commercial or geographical origin, environmental impact, warranty conditions, copyright and related rights, or certificate of homogenization. The Law prohibits misleading and aggressive commercial practices, which is important when it comes to algorithmic systems capable of manipulating consumers.
Pursuant to the Law on Personal Data Protection of Bosnia and Herzegovina (Official Gazette of BiH, No. 12/2025), the principles and elements of lawful data collection are emphasized. All personal data or datasets must be protected against unauthorized access, which is crucial for artificial intelligence systems that process large volumes of data. In cases where data processing is based on consent, the Law requires the data controller to prove that the data subject has provided consent for the processing of their personal data. Article 27 of the same Law prescribes that data controllers, when determining the means of processing and during the processing itself, must implement appropriate technical and organizational measures, such as pseudonymization, in order to ensure effective data protection, taking into account the latest technological developments and associated risks.
Bosnia and Herzegovina does not have a specific law or clear guidelines regulating how copyright applies to the use of data for AI training or automated data collection. In such cases, the general principles of copyright, set out in the Law on Copyright and Related Rights (Official Gazette of BiH,

No. 63/2010), apply. At present, no reform proposals exist concerning copyright and the manner of using content for AI training. Nevertheless, Bosnia and Herzegovina closely follows modern developments in domestic and international criminal law and remains prepared and open to adjustments in order to ensure effective prosecution of AI-related criminal offences.
Currently, no such measures or legal reforms regarding copyright protection related to the use of AI are planned in Brčko District of BiH.

4. **Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?**

There are currently no legislative initiatives concerning the development or distribution of tools used for creating deepfake content. Nevertheless, Bosnia and Herzegovina closely follows modern developments in domestic and international criminal law and remains prepared and open to adjustments in order to ensure effective prosecution of AI-related criminal offences.
There are currently no planned legal reforms regarding the development of applications that enable the production of (sexual) deepfakes, or the use of (sexual) deepfakes for dissemination in Brčko District of BiH.

5. **Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.**

Based on investigative and judicial trends, it is expected that the following activities may be subject to criminalisation in the future:
- Sextortion using deepfake content;
- AI-generated material depicting child sexual abuse;
- Fraud, misrepresentation or electoral manipulation using AI tools;
- Unauthorized use of identity or personal data through AI.

C. Scoping the need for a new instrument

1. **Do you see a need for a new type of offence related to dark AI? (This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)**

Authorities in Bosnia and Herzegovina recognise the need for regulatory consideration of a new category of offences involving so-called dark AI. Given that the current legislative framework does not contain specific provisions addressing AI systems engineered for malicious purposes, it is deemed necessary to:
- analyse new forms of cybercrime enabled by automation and generative AI tools;
- precisely criminalise the use of AI for attacks on critical infrastructure, large-scale hacking or deepfake-based destabilisation of public order and security;
- monitor international legislative examples, particularly within the European Union, to ensure that the domestic system is prepared to respond to the risks posed by dark AI.

In light of the rapid development of artificial intelligence and its forms, we believe that it is necessary to establish new types of offenses related to dark AI.

2. **Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?**

Authorities in Bosnia and Herzegovina support the introduction of new legal provisions that would criminalise:

- production, distribution, sale, procurement or use of AI systems that are prohibited by law due to the threat they pose to fundamental rights, security or democratic order (e.g., AI for real-time biometric surveillance, AI for electoral manipulation, autonomous weapons, etc.),
- importation and provision of such technologies to third parties, especially when they contravene international standards for the protection of rights and security.

Although such acts may currently be covered by general criminal law provisions (e.g., unlawful production of weapons, unauthorised access to systems), there is a need for more precise categorisation and modernisation of the legislation.
The need to establish a new type of offence has been identified to criminalise the placing on the market, putting into use, production, acquisition for personal use, import or provision to third parties - in any form - of an AI system that is prohibited under national/state or European legislation.

3. **Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?**

Yes. Bosnia and Herzegovina recognises the challenges posed by the autonomous behaviour of advanced AI systems—particularly when harmful consequences occur without direct human control or intent.

- Current legislative framework, based on fault principles, is difficult to apply in cases where an AI errors, supervisory or technical failures causes harm.
- It is necessary to consider the introduction of new legal liability mechanisms or amendments to existing liability standards (e.g., strict liability, manufacturer liability, system supervisor liability, etc.).
- We believe that an international-level discussion on liability standards in the context of autonomous AI actions is needed to harmonise legal practices across jurisdictions.

We see the need to adopt specific measures to address the “negligence dilemma” arising from the autonomous actions of AI systems.

4. **Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?**

Authorities in Bosnia and Herzegovina fully support the initiative to develop a new international instrument — such as Convention on AI and Crimes.

- The Budapest Convention on Cybercrime (ETS 185) of the Council of Europe represents a key framework for combating cybercrime, but it is not fully applicable to new criminal offences that would be specific to AI, such as manipulation of deepfake content, autonomous weapons, mass disinformation and blackmail.
- We consider that such a convention should:

o clearly define criminal offences facilitated or enhanced by AI,
o cover standardised forms of international cooperation in investigations (e.g., timely sharing of digital evidence),
o establish common principles of liability for and supervision of AI systems.

Bosnia and Herzegovina expresses its readiness to participate in consultations and contribute to the development of such an instrument.
There is a need to create an international document that would define and criminalize acts that can be committed, enabled, enhanced, or aided through AI systems, given the increasing frequency of "cyber attacks," fraud, or manipulation.

D. Content of a prospective new instrument, if developed

1. **In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?**

□ **definitions**

□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

Bosnia and Herzegovina considers that a prospective international instrument concerning AI and crimes should include the following key components:
a. Definitions
• Clear, legally binding definitions of key terms such as: artificial intelligence, autonomous system, generative AI, deepfake, high-risk AI system, dark AI, etc.
• Definitions should be aligned with the European Union AI legislation to ensure mutual legal recognition and facilitate cooperation.
b. procedural provisions
• Specific measures regarding collection, preservation and verification of digital evidence obtained through AI-based technologies.
• Mechanisms for swift action (emergency measures, blocking, freezing access).
c. jurisdiction provisions
• Introduction of provisions on universal or extended jurisdiction for AI-related crimes with transnational elements.
d. extradition and mutual assistance issues
• Mechanisms providing efficient extradition of persons accused of AI-related criminal offences.
• Standardisation of requests for mutual legal assistance among states, including access to digital evidence.
e. problems with digital evidence
• Rules on authenticity, integrity and forensic processing of AI-generated data.
• Introduction of records on data origin (data provenance) to facilitate tracking the origin of AI-generated content.
f. collaboration of digital AI platforms with criminal prosecutions
• Prescribing obligations for AI service providers/platforms with regard to data retention, user identification and urgent cooperation with competent authorities.
• Introduction of measures against providers enabling anonymous, unregulated or unlawful use of AI systems.
d. Protection of fundamental rights (children, minorities and vulnerable groups) in the context of AI-related crimes.
• Supervision mechanisms for the development of high-risk AI technologies.
• Education and training of judges, prosecutors and investigators on AI-related criminal offences.
All the above elements should be included in the new instrument (Convention on AI and Offenses/Crime).

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

Yes. Bosnia and Herzegovina regards alignment of definitions with the European Union AI Act (EU AI Act) as both beneficial and recommendable for several reasons:
• The EU AI Act has already established standardised definitions recognized within the broader European legal framework, including the terms such as:
o AI system (Article 3 of the EU AI Act),
o high-risk AI system,
o biometric identification,
o autonomous decision-making, etc.
• Alignment with these definitions:
o enables legal recognition and mutual understanding among EU Member States and associated countries (such as BiH),

- facilitates international legal cooperation and extradition, and
- ensures legal certainty for economic operators, investigative authorities and courts.

Bosnia and Herzegovina is in the process of alignment of its legislation with the EU acquis communautaire, and a prospective international convention using aligned definitions would provide operational advantages and facilitate domestic implementation.
The definitions prescribed in the Law on AI should be in line with the new instrument, i.e. the Convention on AI and Criminal Offences/Crime.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

The most urgent issues requiring priority attention in the context of AI technology and criminal law include:
a. Criminalisation of the misuse of generative AI
– especially deepfake technology in the context of sexual exploitation, blackmail, political manipulation and disinformation.
b. Legal control of so-called dark AI
– AI systems specifically developed for harmful or malicious purposes, including hacking, attacks on infrastructure, dissemination of malware, etc.
c. Legal and technical processing of digital evidence generated by AI systems
– including authenticity, verification and the chain of custody of AI evidence (data provenance), as well as the need for specialised forensic tools.
d. Cooperation between judicial authorities and digital/AI service providers
– as the lack of legally binding mechanisms prevents access to key data in investigations and trials.
e. Introduction of new forms of liability (including strict liability)
– considering the autonomous behaviour of advanced AI systems and the complexity of establishing human guilt in such cases.
These issues represent critical legal gaps where the current legislative framework in Bosnia and Herzegovina, as well as in many other countries, is unable to provide effective protection for citizens or efficient prosecution in the field of artificial intelligence.
We believe that the adoption of Conventions on AI and criminal offences/crime is a priority in addressing the global problem that AI can cause.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

We believe that a single global instrument addressing AI and criminal law may provide the following advantages:
- Alignment of legal definitions and standards – facilitates international cooperation and the extradition of perpetrators of AI-related crimes.
- Clearly defined frameworks of jurisdiction and responsibility – especially for transnational AI criminal offences.
- Shared platform for the exchange of information and best practices among states.
- Strengthening global security – through a collective response to cross-border threats.
- Harmonized approach toward private actors and tech companies, especially in terms of their obligations to cooperate and preserve data

We believe that a single global instrument addressing AI and criminal law may provide the following disadvantages:
- Differences in legal systems and capacities among states may complicate the implementation of universal rules.
- Lengthy negotiation processes – international instruments often take years to adopt and enter into force.
- Sovereignty concerns and adaptation to local context – states may prefer flexibility to regulate AI technology through national laws.

Conclusion:

Bosnia and Herzegovina believes that a single international instrument, such as a convention, would provide significant legal and operational value but should be complemented by national/domestic legislation to ensure flexibility, contextual adaptation and effective implementation in practice.
The advantage of a single global instrument is to define crime in the context of AI, set defined standards of accountability, foresee mechanisms of international cooperation for both the investigation and prosecution of AI crime, especially appreciating the fact that such systems do not know national borders. All of the above would aim to protect human rights and fundamental freedoms, ensure legal certainty, and prevent the misuse of AI systems.

CZECHIA

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

It does not. General rules apply in such situations.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

AI system could constitute instrumentalities of criminal activity according to Section 135a of the Criminal Code (Act no. 40/2009 Coll.) – item intended or used for commission of a criminal offence.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

There is no such specific aggravating circumstance laid down.
Nevertheless, where certain criminal offences are committed, use of AI system could fall under some of aggravating circumstances defined in broader terms, in particular commission of a criminal offence in breach of an important obligation arising from occupation, profession, position or function or imposed by law, such as e. g. in Section 273(2)(b) of the Criminal Code (Negligent Public Menace), where required standards of handling of AI systems would not be adhered to, even negligently. It is also possible to imagine applying aggravating circumstance consisting in commission of a criminal offence with a weapon, where AI system would be considered a weapon, although only provided that an attack against a person's body would be concerned and the AI system would be able to make such attack more powerful (Section 118 of the Criminal Code, imaginable in particular as regards autonomous drones or humanoid robots equipped with AI or AI driven vehicles).
Where efficacy of any criminal offence is increased due to use of AI, the use of AI would in fact be considered general aggravating circumstance (although not due to the mere use but due to its effects).

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

With effect from 1. 1. 2026, the Criminal Code will newly specifically address use of deepfakes both in sexual area and generally (amendment no. 270/2025 Coll.), although use of AI technologies for that purpose is not specifically addressed.
Section 181(2) will provide general protection against deepfakes criminalizing persons who "with an intention to seriously harm rights of another, produce a piece of work that, without right, depicts, captures or otherwise uses looks or expressions of personal nature of another person, which appear to be real, while knowing they are not, or make such piece of work publicly available, arrange it, put it into circulation, sell it or otherwise procure it to another person".

Section 191a will provide a more specific protection against abuse of identity for production of pornography and its distribution criminalizing persons who “produce, import, export, transit, offer, make publicly available, arrange, put into circulation, sell or otherwise procure to another person photographic, film, computer, electronic or other pornographic piece of work depicting or otherwise using a person, about which the perpetrator knows that he or she did not consent with such depicting”.
Other specific provisions have not been laid down. The Criminal Code remains technologically neutral, in principle.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ **sexual deepfakes**
☐ **online sexual grooming**
☐ **electoral processes**
☐ **use of autonomous drones to kill someone**
☐ **fraud of notorious importance**
☐ **other: …**

See above in answers to questions 3 and 4. The mentioned aggravating circumstances, however, are not applicable to the specific offences listed in this question. Nevertheless, where efficacy of any criminal offence is increased due to use of AI, the use of AI would in fact be considered general aggravating circumstance (although not due to the mere use but due to its effects).

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

There are no such examples registered.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

Certain amendments have recently been adopted and will apply from 1. 1. 2026 (see answer do question A. 4).
Other reforms have not been proposed.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

No such reforms have been proposed and we don´t think using AI system should be considered special aggravating circumstance. We prefer keeping criminal law technologically neutral as much as possible.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

The Ministry of Industry and Trade is drafting the proposal for the Act on Artificial Intelligence which should implement provisions of the European Union AI Act that require it.

No other reforms have been proposed.

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

See answer to question A. 4.

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

With regard to rapid development of Artificial Intelligence systems in the latest years and months which seems to be gaining more and more momentum, it is difficult to predict which conducts related to AI might become relevant in the future.

(i) As long as AI systems only constitute a tool (instrumentalities) used for commission of offences which might also be committed without their abuse and as long as they closely adhere to instructions (prompts) of their user, establishing new specific criminal offences related to AI does not seem necessary since related conducts already seem to be covered by international and European instruments, at the Council of Europe level particularly by the Convention on Cybercrime (ETS No. 185) and its additional protocols. AI systems should be understood as falling under "computer system" as defined in Article 1(a) of that Convention.

(ii) With regard to rapidly growing level of autonomy, adaptiveness and creativity of the AI systems, enforcement of a certain kind of liability of persons developing, training, implementing or using AI systems in breach of applicable standards (without due diligence) might become even more relevant. It is expected that where not handled with due diligence, future AI systems (with regard to their level of advancement, particularly level of autonomy) might be able to cause harm to the interests protected by law including criminal law which were not intended by the person handling them. But if a sufficient level of due diligence was exercised in their development, training, implementation and use, causing such harm could have been prevented. Such cases could include situations where the set up and/or instruction (prompt) requires an AI system to pursue a certain goal and does not take into consideration that effects of autonomous decisions of the AI system aimed at achieving that goal are likely to harm interests protected by law, although such decisions and their effects could and should have been expected and prevented provided that due diligence was exercised. Liability of the (natural or legal) person concerned should be excluded if sufficient effort was made to prevent such possible effects.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

In general, conducts which might be committed not only with use or abuse of AI systems, but similarly also with use or abuse of other technologies, already seem to be sufficiently addressed by existing standards. The current standards should be interpreted as technologically neutral and thus AI systems must be understood as falling under existing relevant definitions, such as the definition of "computer system" in the Convention on Cybercrime.

Our efforts on this forum should not focus on conducts that might be committed both with use of the AI systems and with the use of other technological tools.

Regarding question 1 in particular, we do not see such need given the broad scope of Article 6 of the Convention on Cybercrime.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

As a Member State of the EU we do not see such urgent need, since relevant conducts seem to be covered and prohibited by Article 5 of the AI Act and Article 99(3) of that Act lays down high thresholds of fines for non-compliance with those prohibitions. Administrative regulations should be enforced primarily by administrative means. States may provide for additional criminalization in cases which they specify.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

This area should be explored since handling of AI systems in breach of applicable standards or generally without due diligence may have serious detrimental results in the future. Where developing, training, implementing or using of AI system is not diligent and advanced AI systems that are expected to be in place already in a very near future are concerned, detrimental results may easily occur although not intended by any person. Nature of criminal law as a tool of the last resort (ultima ratio) should be retained. See also point II. in answer to question B. 5.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

See answers to questions B. 5. and C. 1.

We do not see any added value in creating a new instrument which would aim at confirming that rules on criminal offences and other institutes of criminal law applicable under other Council od Europe instruments, particularly the Convention on Cybercrime, also apply where criminal offences are committed with use or abuse of AI systems. That fact seems to be apparent even without such specific tool. Creating unnecessary duplicities should be avoided. Similarly, we do not see a need to provide for specific aggravating circumstances related to the use of AI since we advocate for technological neutrality and since the mere fact that an offence was committed with use of a certain tool does not typically increase gravity of such offence.

However, discussions on possible conducts of persons results of which might be specific based on the use of AI systems due to their autonomy, adaptiveness and creativity which other systems lack (see also point II. in answer to question B. 5.) seem relevant. In doing so, it should be taken into account that criminal law should be used as a last resort.

Feasibility of a possible solution at the Council of Europe level to the outlined problem, which seems to relate mainly to the *mens rea* of the perpetrator, needs to be duly considered.

If considered feasible, in order to possibly address such specific emerging threats by means of criminal law, the form of another additional protocol to the Convention on Cybercrime could be considered, rather than a brand-new independent convention which could create duplicities and undesirable overlaps with the Convention of Cybercrime or other instruments. Many provisions of the Convention on Cybercrime seem to be applicable in relation to AI systems, therefore that possible additional protocol could only supplement it in a relatively narrow extent with possible provisions on criminal offences clearly specific for the AI systems only, if any identified. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), could serve as an example as regards the scope.

Another issue related to AI technologies which will likely constitute a challenge in criminal proceedings as well as other proceedings and is concerning is the authenticity of evidence. Nevertheless, we do not consider it feasible to regulate the assessment of evidence at the Council of Europe level.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

See answer to question C. 4. We do not advocate for a brand-new convention. The mentioned elements, apart from definitions, do not seem to be specific for AI system - related cases but are similar in any cybercrime case. Therefore, we do not see any urgent to lay down other provisions on the listed elements than those of the Convention on Cybercrime and its additional protocols, which should apply also in AI system – related cases.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

The possible definitions should draw from the existing standards but being definitions of a possible Council of Europe instrument, they should particularly consider the definition of artificial intelligence systems a laid down in Article 2 of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). However, AI development that took place after laying down the existing definitions needs to be taken into account.
Other definitions, if necessary, should by aligned with the Council of Europe instruments, unless a deviation justifiable by relevant arguments is necessary

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

See above particularly in answers to questions B. 5. and C. 4. No issue listed in question D. 1. seems urgent or even relevant for the purpose of the possible new instrument.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

As stated above, we currently do not share the view that a comprehensive self-standing instrument is needed or that many new criminal offences or other provisions need to be laid down. We believe that, if considered necessary and feasible, the Convention on Cybercrime could be supplemented with specificities inherent to the use and abuse of AI systems only, if those will be identified and assessed as relevant from the viewpoint of criminal law.

FINLAND

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Not currently.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

The general principles of criminal law, adopted in the Finnish Criminal Code, apply to all crimes regardless of whether an AI system, for example, has been used. Most of the criminal provisions, including murder, manslaughter, or theft, have been drafted to be technology-neutral.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

The use of AI systems in itself cannot be considered an aggravating circumstance under Finnish law. However, the general grounds for increasing the punishment apply to all crimes, including those committed by using of an AI system. For example, according to Chapter 6, section 5 of the Criminal Code, a premeditated nature of the criminal activity may be a basis for increasing the punishment and could be relevant to crimes where an AI system has been used. In addition, some Criminal Code provisions specifically mention a particular premeditation as an aggravated factor to the crime in question. For example, according to Chapter 38, section 8a, the perpetrator shall be sentenced for aggravated unlawful access to an information system, if the crime (unlawful access to an information system regulated in section 8) is committed in a particularly aggravated manner.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

As a general rule, criminal provisions can be applied to criminal activities regardless of whether AI technologies have been used. There are no provisions of specific AI technologies for committing crimes, or of deepfakes specifically, in the Criminal Code. The Criminal Code provisions of fraud and other dishonesty, in Chapter 36, are technology-neutral in the sense that they can be applied regardless of whether an AI system was used. There are also criminal provisions of forgery offences (Chapter 33), and data and communication offences (Chapter 38), that may be relevant to crimes committed with an AI system.

However, according to the Chapter 20, section 7 of the Criminal Code, a person who unlawfully presents or disseminates an image or a visual recording that factually or realistically depicts another person in a sexual manner, so that the act significantly violates the person's right to sexual self-determination, shall be sentenced for non-consensual dissemination of a sexual image to a fine or to imprisonment for at most two years. According to subsection 2 of said section, an image

or a visual recording is factual in the manner referred to in subsection 1 if it has been produced in a situation where the person in actual fact appears in the image or visual recording referred to in subsection 1, and realistic if it is deceptively similar to an image or a visual recording produced through photography or in another equivalent manner in a situation where the person in actual fact appears in the manner referred to in subsection 1. Therefore, the section can be applied to the use of sexual deepfakes, too.

A similar formulation is included in Chapter 20, section 19 (Distribution of an image depicting a child in a sexual manner) and Chapter 17, section 18 (Distribution of a sexually obscene image). The provision of solicitation of a child for sexual purposes (Chapter 20, section 18) is a technology-neutral provision that can be applied for online sexual grooming, too.

Regarding sexual deepfakes, the provision of defamation (Chapter 24, section 9), may also be relevant.

The use of autonomous drones to kill someone is not directly addressed in the Criminal Code. However, if in a criminal proceeding the use of autonomous drones was considered to reflect deliberate premeditation or a particularly brutal or cruel manner, the criminal provision of murder (Chapter 21, section 2) could be applied instead of the less severely punishable provision of manslaughter (Chapter 21, section 1).

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:

☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:

The use of AI is not considered an aggravating circumstance in itself under Finnish criminal law.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

It is known that there are and have been crimes committed or facilitated by artificial intelligence under criminal investigations. So far, there are no significant national case law examples.

In many cases, it can be difficult to distinguish the use of artificial intelligence and other forms of cybercrime. The significance of information technology to crime trends overall is continuously growing. The same applies to effective crime prevention which requires keeping pace with technological development. In Finland, information technology tools are used in crime prevention and criminal investigations to some extent.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

Not currently.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

Not currently.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

Finland views that, as well as in other areas, the principle of criminal law as a last resort is important in this matter. First of all, the Finnish Criminal Code is, as a general rule, technology-neutral regarding both the general principles and the specific criminal provisions. The current national criminal legislation may be applied to situations where an AI system has been used. Second, the rights that need protection from the risks that AI may pose can also be protected through other measures than criminal law provisions. For example, insurance legislation, product liability rules, and tort liability may be relevant to protect these rights. The questions that arise should be addressed sector-by-sector since criminal legislation might be relevant to some issues but not all. The national implementation of the EU Artificial Intelligence Act of 13th of June 2024 is being prepared by a working group scheduled to finish its work on 30th June 2026.

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

There are no active legal reform projects concerning the Finnish copyright law.

5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

Not currently.

6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

So far, Finland does not consider any specific behaviours or activities involving AI to be criminalised in the future.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

At the moment, Finland does not see a need for a new type of offence related to dark AI precisely. Finland views that the issue relates to effective crime prevention.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

It should first be examined whether the national or European prohibition laws are efficient enough to prevent these acts. The prohibition laws can themselves include criminal provisions to the most serious violations.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

Finland views that, in most cases, the liable person can reliably be determined following the general principles and rules of criminal law. According to Chapter 3, section 5 of the Finnish Criminal Code, intent or negligence is a prerequisite for criminal liability. Intent is the basic premise for culpability as according to section 5, unless otherwise provided, an act referred to in the Criminal Code is only punishable when intentional. These general principles and rules form the basis for the entire criminal liability system.

If exceptions to these principles are proposed, they must be limited, as they may have unforeseen consequences for the general principles of criminal law.

Finland remains open to discussions on the negligence dilemma but at this point views that the question should be addressed from the point of view of the current general principles of criminal liability.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

If the working group chooses to proceed with the creation of an international instrument, Finland views that the instrument should remain on a recommendatory level.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

As stated in C. 4. of this questionnaire, Finland views that the possible instrument should remain on a recommendatory level. At this stage, Finland is open to discuss any elements, as long as the instrument remains recommendatory.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

It would be wise to aim at consistency with other relevant regulations on AI as long as it is possible without difficulty.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

Finland does not at present recognize any specific urgent issues.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

The biggest advantage of a single global instrument, at a recommendatory level, would be the better compatibility of AI related criminal law policies between member states. AI systems perform

cross-border, and it may be difficult to determine the country where the criminal offence was committed, for example.

On the other hand, for example in Finland, the domestic legislation can already sufficiently be applied to most AI related crimes even without AI-specific criminal provisions. Especially if a global instrument would be adopted as a legally binding convention, at this stage it could impose an unnecessary regulatory burden on member states in relation to its benefits. If the scope of the possible future instrument is not carefully considered and limited, there are risks of the instrument having consequences too far-reaching also to criminal law more generally. Since AI systems develop fast, a binding regulatory instrument would also be at risk of expiring.

Finally, Finland views that approaching the broad issue of artificial intelligence and criminal law would be wisest to do sector-by-sector, so that it would be more feasible to assess whether the issues in question can be dealt with less intrusive measures than criminal law.

FRANCE

A: Cadres existants

1. Votre législation nationale et/ou votre jurisprudence abordent-elles spécifiquement la responsabilité pénale ou les infractions liées à l'intelligence artificielle ?
Le cas échéant, pourriez-vous s'il vous plaît :
(1) fournir, si disponible, les textes pertinents (en anglais ou en français) ;

À ce jour, la France ne dispose pas d'une législation nationale consacrée à l'utilisation infractionnelle des systèmes d'intelligence artificielle (IA).
Cependant, il existe déjà en France certaines infractions prévoyant spécifiquement l'utilisation de l'intelligence artificielle, à savoir celles portant sur la publication de contenus reproduisant l'image ou les paroles d'une personne sans son consentement, lorsque ces contenus sont générés par l'IA, venant ainsi incriminer les hypertrucages (« deepfakes ») dans ces contextes.
Ainsi, l'article 15 de la Loi « Sécuriser et Réguler l'espace numérique » (SREN) du 21 mai 2024 a élargi le champ d'application du délit prévu à l'article 226-8 du code pénal, qui réprime la publication d'un montage réalisé avec les paroles ou les images d'une personne sans son consentement, aux cas dans lesquels le contenu a été généré par un traitement algorithmique (incluant les systèmes d'IA), lorsqu'il n'apparaît pas de manière évidente qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.
Une nouvelle circonstance aggravante, applicable aux délits prévus par cet article, permet par ailleurs de porter les peines à deux ans d'emprisonnement et 45 000 euros d'amende lorsque la publication a été réalisée en utilisant un service de communication au public en ligne, permettant de couvrir les situations dans lesquelles ces contenus ont été publiés sur les réseaux sociaux.
De plus, cette loi SREN a également introduit l'article 226-8-1 du code pénal portant création d'un nouveau délit de publication d'un montage présentant un caractère sexuel sans le consentement de la personne. Cet article punit de deux ans d'emprisonnement et de 60 000 euros d'amende le fait de porter à la connaissance du public ou d'un tiers, sans son consentement, un montage ou un contenu visuel ou sonore à caractère sexuel généré par un traitement algorithmique et réalisé avec les paroles ou l'image d'une personne.
Les peines sont portées à trois ans d'emprisonnement et 75 000 euros d'amende lorsque la publication du montage ou du contenu généré par ce traitement algorithmique a été réalisée en utilisant un service de communication au public en ligne.
Par ailleurs, il n'existe pas encore de jurisprudence en France abordant spécifiquement la responsabilité pénale ou les infractions liées à l'intelligence artificielle.

(2) indiquer si la responsabilité pénale est attribuée à une personne spécifique (physique ou morale, par exemple : conducteur, producteur, programmeur, superviseur de flotte, téléopérateur, etc.) et sur quel fondement elle repose (à savoir : responsabilité objective, négligence, intention).
Dans le cas contraire, les règles générales s'appliqueront-elles dans les situations où des infractions sont commises, facilitées, renforcées ou assistées par l'intelligence artificielle ?
La législation française n'aborde pas spécifiquement la responsabilité pénale liée à l'utilisation de l'intelligence artificielle. S'agissant des articles 226-8 et 226-8-1 du code pénal précités, la personne qui a utilisé l'IA pour générer ledit contenu ne sera considérée comme pénalement responsable que dans le cas où elle a également porté le contenu à la connaissance du public ou d'un tiers.
Ce seront donc les règles générales de la responsabilité pénale qui trouveront à s'appliquer, avec les distinctions existantes en droit pénal français. Certaines conditions sont par exemples prévues pour encadrer l'engagement de la responsabilité d'une personne morale (121-2 du code pénal) ou encadrer l'engagement de responsabilité en cas de faute non intentionnelle, en réservant cette possibilité à certains délits notamment. (121-3 du code pénal). Une éventuelle responsabilité par le biais de la complicité pourra être envisagée, mais cette notion exige du complice qu'il agisse sciemment. La complicité est définie en droit français par l'article 121-7 du code pénal.

2. Quelles règles générales sont appliquées dans votre droit lorsque des systèmes d'intelligence artificielle (tels que définis à l'article 2 de la CAI, STCE n° 225) sont utilisés comme outils pour la commission intentionnelle d'infractions pénales (telles que le meurtre, l'homicide involontaire ou le vol) ?

Pour les infractions déjà incriminées en droit français et pour lesquelles l'IA pourrait être utilisée comme outil de commission, la responsabilité pénale afférente a vocation à être déterminée au cas par cas selon les articles 121-1 à 122-9 du code pénal régissant la responsabilité pénale de droit commun.

3. Selon votre droit interne et/ou votre jurisprudence, l'utilisation de systèmes d'intelligence artificielle peut-elle être considérée comme une circonstance aggravante ?

À l'heure actuelle en France, il ne ressort ni du droit français ni de la jurisprudence que l'utilisation de systèmes d'intelligence artificielle puisse constituer une circonstance aggravante d'une infraction existante.

4. Votre législation traite-t-elle de l'utilisation de technologies spécifiques d'intelligence artificielle pour commettre des infractions, par exemple l'utilisation de deepfakes dans certains contextes (tels que les deepfakes à caractère sexuel, le harcèlement sexuel en ligne, ou lors des processus électoraux), l'utilisation de drones autonomes pour tuer quelqu'un, ou des formes spécifiques de fraude ?

Voir réponse à la question A.1 (1) supra.

5. L'utilisation de l'IA est-elle considérée comme une circonstance aggravante, notamment dans les cas impliquant :

☐ deepfakes à caractère sexuel
☐ harcèlement sexuel en ligne
☐ processus électoraux
☐ utilisation de drones autonomes pour tuer quelqu'un
☐ fraude d'une importance notoire
☐ autre :

Tel qu'indiqué précédemment, l'utilisation de l'IA n'est pas considérée comme constituant une circonstance aggravante dans les cas impliquant la publication de deepfakes à caractère sexuel en droit français, mais seulement comme un mode de création parmi d'autres de contenus à caractère sexuel reproduisant l'image ou les paroles d'une personne sans son consentement.

6. Y a-t-il des exemples de jurisprudence nationale ou de pratiques d'enquête (par exemple, enquêtes pénales, évaluations du parquet) impliquant des infractions commises ou facilitées par l'intelligence artificielle ? Si oui, merci de résumer le(s) cas ou de décrire les problématiques, si possible.

Il apparait que des dossiers portant sur des infractions commises en matière d'hypertrucages (« deepfakes ») font l'objet d'investigations et de procédures pénales en cours sur le territoire français.

Il a notamment été constaté ces derniers mois que de plus en plus de procédures pénales portant sur des faits de deepfakes à caractère sexuel ont été initiées, et ce sur l'ensemble du territoire national.

Compte-tenu du secret de l'enquête et de l'instruction régissant les procédures pénales en cours en France, le Ministère de la Justice n'est pas en mesure de fournir plus de détails sur ces affaires.

En outre, il n'existe pas encore de jurisprudence en France s'agissant d'infractions commises ou facilitées par l'intelligence artificielle.

B. Plans futurs

2. Le législateur de votre pays prévoit-il des réformes législatives concernant la responsabilité (pénale) et les infractions liées à l'IA ?

La France n'a pas de réforme législative en cours concernant la responsabilité pénale et les infractions liées à l'IA.

3. Le législateur de votre pays prévoit-il des réformes législatives concernant les circonstances aggravantes lorsque qu'une infraction est commise, facilitée, renforcée ou assistée par l'utilisation de systèmes d'IA ?

La France n'a pas de réforme législative en cours concernant les circonstances aggravantes liées à l'utilisation de l'IA.

3. Votre législateur envisage-t-il de relever les nouveaux défis liés à la protection effective des droits mis en péril par l'utilisation des systèmes d'IA par des mesures autres que l'adoption de nouvelles lois pénales ? Si oui, comment ? Le législateur de votre pays prévoit-il des réformes législatives concernant la protection du droit d'auteur en lien avec l'utilisation de l'IA (par exemple, en raison du web scraping, du web harvesting ou de l'extraction de données à partir de sites web pour entraîner des modèles linguistiques de grande taille) ?

La France n'a pas de réforme législative en cours sur ce sujet.

4. Le législateur de votre pays prévoit-il des réformes législatives concernant le développement d'applications facilitant la production de deepfakes (à caractère sexuel), ou l'utilisation ou la diffusion de deepfakes (à caractère sexuel) ?

La France n'a pas de réforme législative en cours sur ce sujet.

5. Au regard de votre contexte national et des évolutions juridiques, existe-t-il d'autres comportements ou activités impliquant l'intelligence artificielle que vos autorités estiment devoir être pénalement réprimés à l'avenir ? Le cas échéant, veuillez décrire ces comportements et, si possible, en expliquer les raisons.

La France n'envisage pas, à ce stade, de nouvelles incriminations.

C. Évaluation de la nécessité d'un nouvel instrument

1. Voyez-vous la nécessité d'un nouveau type d'infraction liée à l'IA obscure (« dark AI ») ? (Ceci fait référence aux systèmes d'IA spécialement conçus à des fins malveillantes, tels que le piratage, le cracking ou d'autres cyberattaques, ainsi qu'aux IA destinées à cibler les infrastructures critiques, à créer des risques sérieux pour la sécurité publique ou à faciliter la commission de toute infraction.)

En ce qu'il semble apparaitre que l'utilisation de systèmes d'IA spécialement conçus à des fins malveillantes n'aboutit pas à la commission d'infractions inédites, mais facilitent ou permettent la commission d'infractions déjà incriminées en droit français, il ne paraît pas nécessaire à ce stade d'incriminer spécifiquement l'utilisation d'un tel système qui n'est pas par essence illicite et qui ne constitue qu'un moyen de commission de l'infraction.

2. Considérez-vous qu'il est nécessaire d'introduire un nouveau type d'infraction visant à réprimer la mise sur le marché, la mise en service, la production, l'acquisition pour

usage personnel, l'importation ou la fourniture à des tiers – sous quelque forme que ce soit – d'un système d'IA interdit par la législation nationale ou européenne ?

Compte-tenu de l'état actuel de la législation française et du développement des technologies liées à l'intelligence artificielle, il pourrait être envisagé des travaux sur la nécessité d'incriminer spécifiquement la production, la mise en service, la mise sur le marché, l'acquisition pour usage personnel, l'importation ou la fourniture à des tiers de certains système d'IA interdit par la législation nationale ou européenne, en fonction de la gravité des interdictions violées. Cette incrimination apparaitrait notamment opportune au regard du développement des marchés illicites proposant des systèmes d'IA conçus à des fins infractionnelles, et compte-tenu également de la difficulté croissante des services d'enquête pour identifier des contenus générés par l'IA. Il conviendrait toutefois qu'une telle incrimination soit formulée en des termes adaptés, permettant à la fois de respecter les principes à valeur constitutionnelle et de s'adapter aux évolutions technologiques. Comme indiqué à la réponse D1,

3. Considérez-vous nécessaire d'adopter des mesures spécifiques pour traiter le « dilemme de la négligence » résultant des actions autonomes des systèmes d'IA ?

Il apparait pour l'instant prématuré d'adopter des mesures spécifiques pour traiter le « dilemme de la négligence » résultant des actions autonomes des systèmes d'IA qui pourraient être utilisés en France, compte-tenu du manque de recul concernant l'ensemble des situations dans lesquelles ces actions autonomes pourraient intervenir et ce qu'elles pourraient impliquer à long terme, eu égard aux conditions d'utilisation de ces systèmes d'IA par les personnes. À l'heure actuelle, et conformément au (« IA Act »), les systèmes d'IA à haut risque doivent en principe respecter des exigences strictes en matière de contrôle humain, permettant de limiter les problématiques de négligence résultant d'actions autonomes de systèmes d'IA à haut risque.

4. Voyez-vous la nécessité de créer un instrument international (Convention sur l'IA et les infractions) similaire à la Convention de Budapest sur la cybercriminalité, qui définirait et pénaliserait les actes pouvant être commis, facilités, renforcés ou aidés par des systèmes d'IA ?

Il apparait que les actes actuellement identifiés comme susceptibles d'être commis, facilités, renforcés ou aidés par des systèmes d'IA constituent essentiellement des infractions déjà incriminées en droit pénal français, et pouvant couvrir l'utilisation de l'IA à ces fins.

En outre, il pourrait à long terme être préjudiciable de définir et de pénaliser une liste trop limitative d'actes, compte-tenu du spectre extrêmement large d'actes pouvant être concernés et des évolutions technologiques très rapides dans ce domaine.

Par conséquent, il ne nous apparaît pas nécessaire à ce stade qu'un nouvel instrument international définisse et pénalise les actes pouvant être commis, facilités, renforcés ou aidés par des systèmes d'IA.

D. Contenu d'un éventuel nouvel instrument, s'il est élaboré

1. Selon vous, quels éléments suivants un éventuel nouvel instrument international (Convention sur l'IA et les infractions) pourrait-il inclure ?

□ **définitions**
□ **dispositions procédurales**
☐ **dispositions relatives à la compétence juridique**
☐ **questions d'extradition et d'entraide judiciaire**
☐ **problématiques liées aux preuves numériques**
☐ **collaboration des plateformes numériques d'IA avec les poursuites pénales**
☐ **autres questions**

La plupart des éléments ne présentent pas une véritable plus-value justifiant la création d'un nouvel instrument spécifique, compte-tenu des instruments déjà existants (IA Act pour les définitions, paragraphe 2 de l'article 14 de la Convention de Budapest sur la cybercriminalité pour les dispositions procédurales et ses articles 16 à 19 pour les problématiques liées aux preuves numériques et pour la collaboration des plateformes numériques d'IA avec les autorités judiciaires). Il en va de même pour les questions de compétences, qui relèvent des législations nationales pour les infractions prévues en droit interne, et de la Convention de Budapest.

2. Êtes-vous d'accord pour que les définitions s'alignent sur celles de la loi sur l'IA (AI Act) ? Merci de préciser.

Les définitions prévues par le règlement européen (UE) 2024/1689 sur l'intelligence artificielle du 13 juin 2024 (« IA Act ») présentent l'avantage d'être suffisamment larges pour inclure les systèmes d'IA identifiés à l'heure actuelle et probablement ceux à venir, et sont rédigées en des termes se rapprochant des formulations déjà existantes dans les législations nationales.

3. Parmi les questions ci-dessus (le cas échéant), lesquelles considérez-vous comme les plus urgentes à traiter en matière d'IA et de droit pénal ?

Face au développement exponentiel des infractions dont la commission est facilitée ou permise par un recours à des systèmes d'IA et au caractère par nature international de ces faits, il apparait important de pouvoir disposer d'un cadre de coopération judiciaire efficient, notamment avec des Etats qui ne sont pas des Etats parties à la Convention de Budapest ou à la Convention européenne d'extradition et ses protocoles additionnels. Toutefois, un nouvel instrument apparaît moins pertinent que le fait d'inciter d'autres Etats à ratifier les textes existants.

4. Quels seraient, selon vous, les avantages ou les inconvénients d'un instrument mondial unique traitant de l'IA et du droit pénal, par rapport à des lois distinctes dans des domaines spécifiques ?

Comme indiqué ci-dessus, la perspective d'un instrument mondial unique paraît illusoire. La plus-value d'un tel instrument entre pays membres du CoE apparait quant à elle limitée.

Les infractions liées à l'IA constituent un spectre très large d'infractions, et la menace liée à l'utilisation infractionnelle de l'IA peut venir de n'importe où au regard de sa démocratisation et des outils d'IA permettant la traduction de contenus. Un nouvel instrument permettrait également d'inclure dans les infractions liées à l'IA la production, la mise en service, la fourniture, l'importation et l'acquisition de systèmes d'IA conçus ou modifiés à des fins infractionnelles, afin de disposer d'un cadre harmonisé en la matière. Toutefois, la création d'un champ infractionnel spécifique presente également des inconvénients. L'approche par le droit commun (les infractions finales aux fins desquelles l'IA est employée, combinées avec les notions de complicité, association de malfaiteurs, recel, etc.) nous paraît bien plus efficace et robuste face aux changements technologiques. A défaut, il faudrait creer un nouvel instrument pour chaque nouvelle technologie susceptible d'être employée pour commettre des infractions.

GEORGIA

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Currently, the legislation of Georgia does not explicitly address criminal liability related to artificial intelligence. In cases where AI systems are involved in criminal acts, general criminal law provisions apply.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

When AI systems are used as tools to commit intentional offences (e.g., theft, murder), general criminal provisions apply. The law attributes responsibility to the natural or legal person. The standard of liability is generally based on intent or negligence, depending on the circumstances of the offence.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

Domestic law does not currently list the use of AI systems as a specific aggravating circumstance. However, courts may consider the sophisticated nature or scale of harm caused by AI-assisted actions as a factor during sentencing.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

There are no specific provisions targeting the use of particular AI technologies to commit crimes. However, the existing general legal framework applies when these technologies are involved.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other: …

Domestic law does not currently list the use of AI systems as a specific aggravating circumstance.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by

artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

To date, there are limited cases in Georgia involving crimes committed or facilitated specifically by AI. However, considering the increasing use of AI technologies, cases may arise in different areas, such as online fraud or other AI-facilitated offences.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

For the time being, no legislative process has been underway specifically addressing the criminal liability and offences related to AI. However, relevant authorities are monitoring developments in AI technology and international frameworks to assess whether future legislative measures may be necessary.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

Currently, there are no specific legislative initiatives to introduce aggravating circumstances for crimes facilitated by AI systems. Nonetheless, the potential for AI-assisted criminal activity is under consideration by relevant bodies, and legislative updates may follow as AI use becomes more widespread.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

While no specific legislative initiatives have been tabled thus far, Georgian authorities may consider deploying non-criminal measures to protect rights at risk from AI use. Such measures could include regulatory frameworks for AI deployment, risk assessments, data protection and privacy regulations, and oversight mechanisms for AI applications, rather than relying solely on criminal law.

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

At present, there are no specific legislative initiatives in Georgia addressing copyright issues arising from the use of AI.

5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

For the time being, no relevant legislative initiatives are in place.

6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

No specific suggestions at this stage.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

While current legislation may cover some aspects under cybercrime or general criminal provisions, the unique capabilities and autonomous nature of AI systems may require reviewing certain concepts of criminal liability in this regard.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

While we recognise the need to develop international standards for appropriate criminalisation, establishing such standards at this stage calls for caution. Most national jurisdictions have not yet introduced specific criminal offences addressing the placing on the market, putting into service, production, acquisition for personal use, importation, or provision of prohibited AI systems. It would therefore be more appropriate to thoroughly study the national developments across different jurisdictions and legal systems before moving towards any international regulation.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

Negligence dilemma is perhaps one of the most acute challenges in criminal law in light of the AI systems developments. We are, however, cautious about developing any relevant international norms at this stage as relevant domestic laws are either absent or at a very early stage of development. It may also go beyond the scope of criminal law in some aspects.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

We recognise the potential value of such an instrument. However, its scope would need to be carefully defined to ensure its broad acceptance and relevance over time.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

We generally support the proposed list, albeit with reservations regarding the scope of each item. We also have concerns about the item “collaboration of digital AI platforms with criminal prosecutions,” insofar as it may imply the introduction of vertical regulations. None of the existing global cybercrime instruments (such as the Budapest Convention or the new UN Convention) contain such provisions. We would, however, support the introduction of voluntary cooperation rules, similar to those under Article 32 of the Budapest Convention.

Furthermore, we do not see the added value of the item “problems with digital evidence,” as long as the intended rules are limited to admissibility issues, which remain primarily within the domain of domestic law.

We are not also convinced about any added value of procedural law provisions, since these aspects could be addressed by existing cybercrime frameworks. However, this issue may still merit further consideration.

We would also propose adding substantive law provisions to this list.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

While we broadly support alignment with the AI Act, we believe that other international developments should also be considered to ensure the instrument achieves broader global acceptance.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?
Perhaps, definitions, substantive law provisions as well as international cooperation measures should be prioritised.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

Advantage of adopting a global instrument would be preventing any challenges in cross-border cooperation that may arise due to divergences in criminalization.

GERMANY

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

German criminal law does not specifically address crimes related to artificial intelligence, but general rules do apply. Depending on the specific circumstances of the case, criminal liability may be established under general criminal law provisions, e.g., when AI systems are used as instrumentalities in the perpetration of a criminal offence. Certain offences already cover scenarios where the use of AI does not appear unlikely. For instance, the use of AI in cyber espionage may fall under Sections 99 (working as agent for intelligence service) and 109f (intelligence activity endangering national security) of the German Criminal Code (StGB). Similarly, AI-driven cyber sabotage could be addressed under Sections 87 (acting as secret agent for purpose of sabotage) or 109e (sabotage against means of defence) StGB.
In addition, Sections 184b and 184c of the German Criminal Code criminalise dissemination, procurement and possession of child and youth pornographic content. Child or youth pornographic content which reproduces actual, realistic or even fictitious content is covered. Acts relating to content generated by AI are essentially also covered.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

Any technical means can be considered instrumentalities of a criminal offence.
In principle, AI systems become relevant under criminal law if, with their involvement, a violation or endangerment of a legal interest occurs. This raises the question of criminal liability. According to the constitutional principle of guilt, the imposition of penalties requires that a natural person can be personally accused of the crime (nulla poena sine culpa). Therefore, the fulfilment of a criminal offence requires a human act (action or omission). Criminal liability of machines, robots, or other technical systems is not provided for.

The criminal liability of natural persons in connection with damage caused by AI systems is governed by general criminal law principles. This means that, as a rule, the perpetrator must have caused the crime in a causal and objectively attributable manner. There are no special requirements if the perpetrator deliberately uses an AI system as a tool for the crime. However, the assessment can be complex due to the so-called black box problem. This refers to the fact that, due to the high degree of autonomy, the decisions of AI systems cannot always be fully understood, meaning that causality and objective attribution cannot be easily assessed. However, it is possible to view AI systems as products and apply the developed principles of criminal product liability. According to the Federal Court of Justice's landmark “leather spray” decision, it is not necessary to explain all mechanisms of action in detail to affirm a causal connection, as long as other possible causes of damage can be ruled out. Accordingly, it is sufficient if the AI system used demonstrably caused the violation or endangerment of a legal interest. In any event, humans cannot exonerate themselves by using a technical system. This case law becomes relevant in negligence-based offences, especially when the AI independently develops functions that were not intended by the manufacturer or operator.

The use of AI systems by companies can lead to criminal charges if a responsible person can be identified. Due to the principle of culpability and the lack of direct punishment for legal entities in Germany, it is essential that responsibility be attributed to a natural person. In large companies, this presents the challenge that, due to the large number of actors involved ("many hands") and the intertwining of work areas, it is difficult to single out a single individual for criminal prosecution. In practice, however, and depending on the circumstances of the individual case, the company management can be held accountable according to German case law and the so-called principle of joint responsibility.
Last but not least, the recently adopted EU AI Act (AIA) will also be of particular importance for the assessment under criminal law. The Regulation is aimed at providers, operators, importers, and distributors of AI systems and, in addition to prohibiting certain AI practices, stipulates, in particular, far-reaching obligations with regard to so-called high-risk AI for the various addressees. These obligations can have an impact on substantive criminal law as individual due diligence obligations (particularly in cases of negligence). Furthermore, non-compliance with the obligations under the Regulation is subject to sanctions (Article 99 AI Regulation).

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

Yes, it is possible depending on the circumstances of the specific case. According to Section 46(2) of the German Criminal Code, the court weighs the circumstances which speak in favour of and those which speak against the offender when fixing the penalty. Among other circumstances, the modus operandi and the consequences of the offence may be taken into consideration to the extent that the offender is to blame for them.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

As noted above (see question A.1.), German criminal law does not specifically address the use of particular AI technologies for committing crimes. However, general criminal provisions apply depending on the circumstances of the case.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:

The use of AI can be considered an aggravating circumstance in respect of all criminal offences mentioned above. See the answer to question A.3. The sentencing regulation of Section 46 of the German Criminal Code is a general rule that applies to all criminal offences.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

Currently, no relevant case law is known on this matter.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

No, as general rules apply to crimes related to AI and no gaps have been identified so far. See answers to questions A.1., A.2. and A.4.
In the context of the implementation of the European Commission's proposal for a recast of the Directive of the European Parliament and of the Council on combating the sexual abuse and the sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (2011/93/EU), it will be examined whether there is still a need for further adaptation due to the possible provisions contained therein (for example, with regard to offences concerning child or youth pornographic content).

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

No, because the general sentencing regulation of Section 46 of the German Criminal Code applies to all crimes and no gaps have been identified so far. See answers to question A.3. and A.5.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?
No. The recently adopted EU AI Act (AIA) addresses and classifies certain AI systems/activities posing severe risks on health, safety, fundamental rights and other harmful effects based on the degree of risk emanating from those AI systems (risk-based approach). For example, Art. 5 AIA prohibits the use of certain practices and Art. 6 AIA stipulates extended requirements for AI systems with a high risk. Article 50 contains provisions regarding deepfakes. Non-compliance with any obligation introduced by the AIA may result in severe administrative fines (Art. 99 AIA). The corresponding provisions on fines and penalties will be implemented in the German national implementation law for the AI Act. According to Article 112 AIA, the aforementioned provisions will be evaluated on a regular basis and the need for amendment will be assessed by the EU Commission.

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

No. The relevant exclusive rights, as well as the exception for text and data mining, are harmonized at EU level (Directive (EU) 2019/790) – DSM-Directive). The EU Commission plans to review the DSM-Directive from mid-2026.
Regarding criminal law and copyright in general, the German Copyright Act already entails provisions on criminal liability for the unlawful exploitation of copyrighted works (Sec. 106 et seq. Act on Copyright and Related Rights).

5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

As previously stated, the EU AI Act contains transparency obligations regarding deepfakes (Art. 50(2) and (4) AIA) that will apply from 2 August 2026 onwards. Furthermore, the Coalition agreement provides for the closing of “criminal liability loopholes” in the distribution of deepfakes; the best way to implement this requirement is currently being evaluated.

6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

The AI Act provides for sanctions in the event of violations of the AI Act. Against this background, and as general rules apply, we see currently no need for adjustment; we refer to the answers to questions A.2 and B.5.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI? (This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

Currently, we do not see a need for a new type of offence related to dark AI. Art. 5 AIA stipulates a general prohibition of certain practices comprising manipulative and exploitative practices (Art. 5(1)(a) and (b)). Non-compliance with this prohibition will be subject to penalties (Art. 99 AIA).

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

No, we currently do not see a need for a new type of offence to criminalise such behaviour. The existing criminal law provisions adequately cover the phenomenon. In particular, the AI Act sanctions non-compliance with Article 5 (prohibitions).

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

No. According to German case law there is no negligence dilemma, as it is possible to view AI systems as products and apply the developed principles of criminal product liability. According to the Federal Court of Justice's landmark “leather spray” decision, it is not necessary to explain all mechanisms of action in detail to affirm a causal connection, as long as other possible causes of damage can be ruled out. Accordingly, it is sufficient if the AI system used demonstrably caused the violation or endangerment of a legal interest. In any event, humans cannot exonerate themselves by using a technical system. This case law becomes relevant in negligence-based offences, especially when the AI independently develops functions that were not intended by the manufacturer or operator. Furthermore, the due diligence obligations stipulated in the AI Act also affect the interpretation of the concept of negligence (see answer to question A.2.)

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

No, because general rules apply to crimes related to AI. Experience with the AI Act, which supplements existing law, should also be awaited, especially since no regulatory gaps have been identified so far. Our focus should therefore be on consolidating and effectively applying of existing instruments.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**

☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

An answer is not required. As already explained in response to questions C1 to C4, Germany does not currently consider a further instrument to be necessary. The aforementioned aspects are already covered by existing European or national legal instruments, such as the AI Act or the E-Evidence Act. New rules on extradition and mutual assistance are also not necessary. Those topics are already included in existent CoE treaties. No loopholes have yet been identified in the practical application of those treaties.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

We see no need for further definitions, as the AI Act and the CoE Framework Convention on AI already provide definitions. In any event, a consistent set of definitions should be sought to create a coherent and harmonised framework on AI. Therefore, we strongly encourage the alignment of any definition with those in the AI Act and in the CoE Framework Convention on AI.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

None, we refer to the answers to question D.1.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

A single global instrument addressing AI and criminal law has the advantage of being one cohesive piece of legislation, as opposed to individual legislation for specific areas that may contradict each other on certain issues. However, individual pieces of legislation have the advantage of easier passage and more targeted approaches to specific areas in the field of AI and criminal law. The more targeted approach particularly favours individual, limited pieces of legislation, e.g. concerning definitions and collaboration of digital AI platforms with criminal prosecution. A global instrument and/or individual pieces of legislation on procedural provisions and jurisdiction provisions, however, are not seen as necessary due to the existing legislation and the fact that procedural provisions remain in the national purview and should respect national systems.

IRELAND

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

The Criminal Justice (Offences against Information Systems) Act 2017 may be of relevance here criminalizes a range of cyber- offences such as unauthorised access, data interference or using hacking tools but doesn't specifically mention AI- enabled crimes.

The Harassment, Harmful Communications and Related Offences Act 2020 defines the term "intimate image" broadly to capture AI- generated deepfakes but doesn't specifically mention AI-enabled crimes: (emphasis added)

1. '"intimate image", in relation to a person, means any visual representation (including any accompanying sound or document) made by any means including any photographic, film, video or digital representation—
(a) of what is, or purports to be the person's genitals, buttocks or anal region and, in the case of a female, her breasts,

(b) of the underwear covering the person's genitals, buttocks or anal region and, in the case of a female, her breasts,
(c) in which the person is nude, or
(d) in which the person is engaged in sexual activity;'

The Child Trafficking and Pornography Act 1998 is framed so that no distinction can made between AI- generated material and other child sexual abuse material; (emphasis added)

'"child pornography" means—
2.(a) any visual representation—
(i) that shows, or in the case of a document relates to, a person who is or is depicted as being a child and who is engaged in or is depicted as being engaged in real or simulated sexually explicit activity,
(ii) that shows, or in the case of a document relates to, a person who is or is depicted as being a child and who is or is depicted as witnessing any such activity by any person or persons, or
(iii) that shows, for a sexual purpose, the genital or anal region of a child or of a person depicted as being a child,
(b) any audio representation of a person who is or is represented as being a child and who is engaged in or is represented as being engaged in explicit sexual activity,
(c) any visual or audio representation that advocates, encourages or counsels any sexual activity with children which is an offence under any enactment, or
(d) any visual representation or description of, or information relating to, a child that indicates or implies that the child is available to be used for the purpose of sexual exploitation within the meaning of section 3,
irrespective of how or through what medium the representation, description or information has been produced, transmitted or conveyed and, without prejudice to the generality of the foregoing, includes any representation, description or information produced by or from computer-graphics or by any other electronic or mechanical means but does not include—

(I) any book or periodical publication which has been examined by the Censorship of Publications Board and in respect of which a prohibition order under the Censorship of Publications Acts, 1929 to 1967, is not for the time being in force,
(II) any film in respect of which a general certificate or a limited certificate under the Censorship of Films Acts, 1923 to 1992, is in force, or
(III) any video work in respect of which a supply certificate under the Video Recordings Acts, 1989 and 1992, is in force;'

Criminal liability in all three Acts is attributed to the creator/ actor and is based on intent.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

N/A

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

No.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

The Harassment, Harmful Communications and Related Offences Act 2020 defines the term "intimate image" broadly in order to capture all of the potential means by which intimate images may be produced. This covers AI-generated materials and deepfakes. The term "intimate image" in the Act "means any visual representation (including any accompanying sound or document) made by any means including any photographic, film, video or digital representation". The 2020 Act also criminalises the distribution, publishing, or threats to distribute or publish such deepfakes. The Act contains both summary and indictable offences - including imprisonment for a term not exceeding seven years and class A fines.

The Child Trafficking and Pornography Act 1998 is already framed so that no distinction can made between AI- generated material and other child sexual abuse material. Section 2(2) provides that: "The reference in paragraph (a) of the definition of child pornography to a person shall be construed as including a reference to a figure resembling a person that has been generated or modified by computer-graphics or otherwise". The existing penalties in Ireland's national legislation exceed all of the maximum sentences in the Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA and also exceed all of the revised maximum sentences proposed in the Revising Directive currently being negotiated at EU level.

There is no stand-alone provision under Irish law that provides that identity theft/fraud constitutes an offence, however it is addressed through a combination of legislative measures, primarily the Criminal Justice (Theft and Fraud) Offences Act 2001 and the Criminal Justice (Offences Relating to Information Systems) Act 2017.

Section 6(1) of the 2001 Act provides a broad offence of making gain or causing loss by deception which can be applied to the fraudulent use of another person's identity. This can capture a range of identity-based misconduct where deception results in financial or personal gain. While acts like phishing may not be offences in themselves, they could be prosecuted where they form part of a wider deceptive scheme that meets the criteria of this section.

This is supplemented by the 2017 Act, which was introduced to address cybercrime and related offences such as unauthorised access to systems, data interference, and the use of malware. While the 2017 Act does not create a specific offence of identity theft, it recognises the seriousness of identity misuse by considering it as an aggravating factor for an offence under s.3 (Interference with information system without lawful authority) or s.4 (Interference with data without lawful authority). Section 8(4)(a) provides for this, dealing with offences such as data interference committed using false personal data, where the court is required to treat this as grounds for imposing a more severe penalty.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:

☐ sexual deepfakes

☐ online sexual grooming

☐ electoral processes

☐ use of autonomous drones to kill someone

☐ fraud of notorious importance

☐ other:

No

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

The use of biometrics in law enforcement for the detection, prevention, investigation and prosecution of criminal offences is currently being legislated for. Offences will be included in that legislation for falsifying, concealing, destroying, or otherwise disposing of information obtained as a result of the use of biometrics in law enforcement, and for permitting, inducing, coercing or requesting same.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

5. Based on your national context and legal developments, are there any other behaviours or activities
involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

This is already in place:
Section 6 of the Offences against Information Systems Act 2017
6. A person who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under section 2 , 3 , 4 or 5 —
(a) any computer programme that is primarily designed or adapted for use in connection with the commission of such an offence, or
(b) any device, computer password, unencryption key or code, or access code, or similar data, by which an information system is capable of being accessed, shall be guilty of an offence.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

ITALY

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?

Not yet. Nevertheless, on March 20, 2025, the Italian Senate approved bill 1146/2024 ('AI Bill') which delegates the Government to adopt, within 12 months a legislative decree to adapt national legislation to Regulation (EU) 2024/1689 ('AI Act'). The bill is currently under examination by the Chamber of Deputies and in few days the Bill should by finally approved and become formally law. Relevant provisions include:
(1) Criminal aggravating circumstances: The Draft Law establishes the introduction of a new common aggravating circumstance for having committed the act using artificial intelligence systems, when such systems, by their nature or manner of use, have constituted insidious means or when their use has obstructed public or private defence, or aggravated the consequences of the offence.
(2) Specific AI-related offenses: The bill introduces A1ticle 612-quater of the Criminal Code(" I.Ilicit dissemination of artificially generated or manipulated content") which states: "Anyone who, with the aim of causing harm to a person and without his consent sends, delivers, cedes publishes or otherwise disseminates the image, video or voice, falsified or altered through the use of artificial intelligence systems and suitable to mislead as to their genuineness is punished with imprisonment from six months to three years. If unjust damage results from the act, the penalty is imprisonment from one to five years".
Criminal responsibility attribution: The legislation attributes criminal responsibility to specific natural persons (drivers producers, programmers, operators, etc.) based on general criminal law principles of intent and negligence. Aggravating circumstances are provided for money laundering offenses the use of money assets or benefits of i Ilicit origin and self-laundering when the acts are committed by AI. If ge11eFal FUles den't apply: Yes General criminal law rules apply when crimes are committed facilitated enhanced or aided by artificial intelligence supplemented by the new AI- speci fie provisions.

2. What general rules are applied in your law when AI systems are used as tools for the intentional commission of criminal offences'?

When AI is used insidiously hinders public or private defence, or contributes to aggravating the consequences of a crime specific aggravating circumstances apply that increase the punishment. The following general principles apply:
- Standard criminal liability rules under the Italian Criminal Code (Cadice Penale)
- Enhanced penalties through the new AI aggravating circumstance
- Specific offenses for AI-manipulated content (deepfakes)
- Traditional fraud and computer fraud provisions with enhanced penalties when AI Is involved

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

Yes. The Italian AI Bill introduces a specific aggravating circumstance for the use of AI systems: the punishment is increased when AI is used insidiously, hinders public or private defence or contributes to aggravating the consequences of a crime.
The bill stipulates that the use of AI for money laundering represents an aggravating element. The draft bill proposes heavier penalties for market rigging involving the use of AI tools.

4. Does your law address the use of specific AI technologies for committing crimes?

Yes. The legislation specifically addresses:
- Deepfakes and manipulated content: Article 612-quater specifically targets falsified images videos, or audio content generated through AI systems
- Market manipulation: Enhanced penalties for A I-assisted market rigging
- Money laundering: AI use as an aggravating factor
- Fraud: Computer fraud offenses punished more severely when committed using AI
- Online sexual grooming and deepfakes

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:

Sexual deepfakes - Yes covered under Article 612-quarter; Online sexual grooming - Yes, general aggravating circumstances apply; Electoral processes - Yes through general AI aggravating circumstances; Use of autonomous drones to kill someone - Yes general aggravating circumstances would apply; Fraud of notorious importance - Yes, specifically addressed with enhanced penalties; Other: Market manipulation, money laundering.

6. Are there any examples of national case law or investigative practice involving crimes committed or facilitated by artificial intelligence?

Here's a comprehensive summary of the AI-related criminal cases and investigations m Italy, translated into English:
Summary of AI-Related Criminal Cases in Italy

1. Voice Cloning Fraud Cases (2025)
Italian Postal Police received multiple reports throughout 2025 of criminal using AI voice cloning technology to impersonate family members. In these cases, fraudsters generated synthetic voices using audio clips taken from social media or old voice messages to pose as children or grandchildren in distress successfully obtaining sensitive banking data and OTP codes to empty bank accounts.

2. The Fake Minister of Defence High-Profile Scam (2025)
A sophisticated fraud targeting Italy's wealthiest entrepreneurs used AI to clone Defence Minister's voice. The scammers contacted high-profile victims. The criminals posed as ministry staff and demanded large sums for alleged ransoms of Italian journalists kidnapped abroad, promising reimbursement from the Bank of Italy. At least one entrepreneur transferred approximately €1 million to foreign accounts before discovering the fraud.

3. ENI CEO Deepfake Investigation
The Postal Police, collaborating with ENI's security service uncovered a criminal group exploiting deepfake videos of ENI CEO to promote fake investment platforms. The investigation resulted in:
- 473 websites accounts and advertisements shut down
- Identification of subjects involved in monetizing illegal proceeds
- A broader investigation into cryptocurrency investment fraud

4. Celebrity Deepfake Cases
Multiple Italian celebrities filed complaints after being featured in unauthorized deepfake videos promoting cryptocurrency scams and get-rich-quick schemes including celebrity chefs restaurateurs, TV personalities, fashion influencers, TV presenters.

5. Law Enforcement Statistics
Italian authorities report a significant increase in complaints about:
- Fake call centres using AI-generated voices
- Voice cloning targeting elderly and less digitally literate individuals
- Manipulated videos featuring well-known TV personalities

- Sophisticated phishing campaigns enhanced by AI technology

These cases demonstrate that Italy is experiencing a substantial wave of AI-enabled criminal activity across multiple sectors, with law enforcement actively investigating and adapting to these new technological threats. The cases provide concrete examples of the types of crimes the pending AI Bill aims to address with its new criminal provisions.
These fake videos were primarily distributed through sponsored campaigns on Facebook and TikTok, directing victims to fraudulent platforms.

B. Future Plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

Yes. The AI Bill delegates the Government to adopt within 12 months, a legislative decree to adapt national legislation to the EU AI Act. The Draft Law foresees additional and autonomous criminal offenses to protect specific legal interests exposed to risks due to the use of artificial intelligence systems.

2. Does the legislator plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by AI systems?

Yes. The comprehensive aggravating circumstance framework is already included in the current AI Bill and will be implemented upon final approval.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by AI systems through measures other than adopting new criminal laws?

Yes. The AI Bill includes provisions concerning copyright protection, requiring labelling of AI-generated content, and establishing obligations for online platforms to adopt measures protecting users from AI-generated misinformation.
Additional measures include:

- Copyright law amendments
- Content labeling requirements
- Platform obligations for AI-generated content detection
- Civil liability frameworks

4. Does the legislator plan legal reforms concerning the development of applications that facilitate the production or dissemination of deepfakes?

Yes. The legislation specifically addresses the illicit dissemination of content generated or manipulated with artificial intelligence sy terns through the new Article 612-quater, with imprisonment from six months to three years, or one to five years if unjust damage results.

5. Are there any other behaviours or activities involving AI that your authorities consider should be criminalized in the future?

The legislation anticipates further developments including:

- Security measures for AI system manufacturers
- Professional responsibility for AI system developers
- Enhanced cooperation mechanisms for cross-border AI crimes
- Specific provisions for AI use in critical infrastructure

C. Scoping the Need for a New Instrument

1. Do you see a need for a new type of offense related to dark AI?

Yes. The Italian approach recognizes the need for autonomous offenses relating to combating the failure to adopt or adapt security measures by manufacturers for AI systems production circulation, and professional use.

2. Do you see a need for a new type of offense to criminalize placing prohibited AI systems on the market?

Yes. This would complement the EU AI Act's administrative framework with criminal sanctions for serious violations.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from autonomous AI systems?

Yes. The legislation anticipates addressing cases where AI systems significantly impact offenses to protected legal interests, including personal and state property.

4. Do you see a need for an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime?

Yes. Italy supports international cooperation frameworks, particularly given the transnational nature of AI-related crimes and the need for coordinated enforcement mechanisms.

D. Content of a Prospective New Instrument

1. Which elements could a prospective new international instrument include?

☑ Definitions - Essential for legal certainty; ☑ Procedural provisions - Cross-border investigation procedures; ☑ Jurisdiction provisions - Clear rules for international cases; ☑ Extradition and mutual assistance issue - Critical for enforcement; ☑ Problems with digital evidence - Technical standards needed; ☑ Collaboration of digital AI platforms with criminal prosecutions - Platform cooperation frameworks.

2. Should definitions align with those in the AI Act?

Yes, they should.

3. Which issues do you consider most urgent to address in relation to AI and criminal law?

1. Deepfakes and manipulated content - immediate harm to individuals
2. AI-assisted fraud and financial crimes - economic security
3. Cross-border enforcement mechanisms - jurisdictional challenges
4. Evidence preservation and authenticity - procedural safeguards

4. What would be the advantages or disadvantages of a single global instrument addressing AI and criminal law?

Advantages:
- Harmonized definitions and standards
- Effective cross-border cooperation
- Reduced regulatory fragmentation
- Enhanced enforcement capabilities

Disadvantages:
- Potential conflicts with national sovereignty
- Different legal system compatibility issues
- Implementation timeline challenges
- Need for flexibility in rapidly evolving technology

LATVIA

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Latvian Criminal law does not regulate criminal liability or crimes connected to artificial intelligence per se, but the Criminal law does provide for liability Influencing the election process by using deepfake technology.

In connection with deep fakes, amendments to the Criminal Law came into force on May 22, 2024, adding two new articles, namely, Article 90.1 “Influencing the election process using deepfake technology” and Article 90.2 “Influencing the process of electing, appointing or confirming a public official in the Saeima using deepfake technology”. There are currently no practical examples of these articles of the Criminal Law.
Section 90.1 of the Criminal law regulates criminal liability for the deliberate creation or dissemination of false and discrediting information about a political organization (party) or association of political organizations (parties) or a candidate for the Saeima of the Republic of Latvia, a local government council or the European Parliament using deepfake technology, if committed during the pre-election campaign period or on election day. In addition, Section 90.2 of Criminal law regulates criminal liability for the deliberate creation or dissemination of false discrediting information using deepfake technology in relation to a candidate for a public office who is elected, appointed or confirmed by the Saeima, if this is done during the process of election, appointment or confirmation of a public official, as stipulated by law. These Sections were specifically created to prevent threads to senior officials and influence the electoral process. While creating these Sections it was pointed out that the use or creation of deepfakes as such should not be criminalized, since any method, including deepfakes, can already be used in the commission of any crime. In other words, deepfakes are considered a type of crime or a method of committing a crime. But we note that deepfakes are just a small part of the AI systems.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

There are no specific rules applied when AI systems are used as tools for criminal offences.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?
No, our domestic or case law does not consider use of AI systems as aggravating circumstance.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

As mentioned above, Criminal law does regulate criminal liability for the deliberate creation or dissemination of false discrediting information using deepfake technology in relation to a candidate for a public office who is elected, appointed or confirmed by the Saeima, if this is done during the

process of election, appointment or confirmation of a public official, as stipulated by law (under Section 90.2) And Criminal law also regulate criminal liability for the deliberate creation or dissemination of false and discrediting information about a political organization (party) or association of political organizations (parties) or a candidate for the Saeima of the Republic of Latvia, a local government council or the European Parliament using deepfake technology, if committed during the pre-election campaign period or on election day (under Section 90.1).

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:

As of now, the Criminal law does not consider AI use as an aggravating circumstance in these crimes. However Criminal law addresses data automated processing system use as an qualifying feature in specific crimes. For example, Section 150 (2) regulates criminal liability for the criminal offence provided for in Paragraph one of this Section, if it has been committed by a public official, or a responsible employee of an undertaking (company) or organisation, or a group of persons, or if it is committed using an automated data processing system. We note that in general our Criminal law is open and neutral in the environment the crime has been committed. With that said if a person commits any crime using an automated data processing system, the person will be held accountable even if the crime has been committed using this automated data processing system (even if the Criminal law does not mention this action).

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

Regarding pornographic materials, on March 13, 2025, a prosecutor's indictment was adopted in criminal case No. 18300003224 pursuant to the second part of Article 166 of the Criminal law. According to the indictment /person 1/, during the pre-trial criminal proceedings, at a place and time not precisely determined, with the aim of satisfying his sexual desires, he intentionally, aware that he was producing child pornography, using an image processing program that was not precisely determined in the pre-trial criminal proceedings, altered images of children showing clothed underage girls, creating realistic images of underage girls with non-existent child genitalia, after which the images produced /person 1/ were stored on data carriers in his possession.
In another criminal case, there were suspicions, but during the investigation, no confirmation was obtained (the fraudsters in question were not detained and no searches were carried out on them) that the fraudsters were using voice deepfakes.
In addition, it was found that artificial intelligence or its elements are used in the creation of illegal electronic content, and, in most cases, artificial intelligence is used in the production of child pornography.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

As of now, European Commission proposal for a directive on combating sexual abuse, sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (recast) is being developed. Considering this Directive there are talk about AI use in crimes that are related to sexual abuse, sexual exploitation of children and child pornography. As of now there are no specific regulation that this proposal regulates, but there are talk on regulating

definitions regarding use of AI in crimes that are related to sexual abuse, sexual exploitation of children and child pornography. Therefore, when this Directive entries into force, there might be reforms to comply with this Directives regulation.
In addition, Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 may 2024 on combating violence against women and domestic violence Article 5 regulates that a) making accessible to the public, by means of information and communication technologies ('ICT'), images, videos or similar material depicting sexually explicit activities or the intimate parts of a person, without that person's consent, where such conduct is likely to cause serious harm to that person; b) producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person's consent, where such conduct is likely to cause serious harm to that person; c) threatening to engage in the conduct referred to in point (a) or (b) in order to coerce a person to do, acquiesce to or refrain from a certain act should be considered as an criminal offence. Therefore, there might be amendments in our national regulation to ensure the national regulation complies with this Directive.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

Any possible reforms concerning aggravating circumstances will be considered taking into account in the last question mentioned Directives (and proposal) and the regulation of the Directives.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

The term "artificial intelligence system" corresponds to the term "automated data processing system" used in the Criminal Law of Latvia, namely, an automated data processing system is any device or group of interconnected devices whose purpose is to perform an automatic data processing process or other function.
We would like to point out that in Latvia no separate liability is assigned for offences committed using artificial intelligence or automated data processing systems, i.e., liability arises regardless of the tools or methods used to commit the criminal offense. Artificial intelligence is just another tool of automated data processing systems, with the help or support of which most of the criminal offenses provided for in the Criminal Law can be committed. In certain criminal offenses, the commission of a criminal offense using an automated data processing system may be a qualifying feature of the criminal offense, for which a more severe penalty is provided than for the basic offense.
At the same time, the Criminal Law specifically defines certain criminal offenses that can be committed by using an automated data processing system or by influencing its operation, for example: Section 177.1 "Fraud in an automated data processing system"; Section 241 "Unauthorized access to an automated data processing system"; Section 243 "Interference with the operation of an automated data processing system and illegal handling of information contained in this system"; Section 244 "Illegal actions with devices that affect the resources of an automated data processing system".
In relation to deepfakes, we would like to inform you that on May 22, 2024, amendments to the Criminal Law came into force, adding two new articles, namely, Section 90.1 "Influencing the election process using deepfake technology" and Section 90.2 "Influencing the process of electing, appointing or confirming a public official in the Saeima using deepfake technology".
In addition to criminal law regulations, other measures aimed at protecting individuals' rights in the context of the use of artificial intelligence systems are also being implemented within Latvia's regulatory and institutional framework. Preparations are currently underway at the national level for the implementation of the European Union's Artificial Intelligence Act (AI Act), which provides for the establishment of governance and oversight mechanisms, including risk assessment, transparency, and human control requirements for high-risk artificial intelligence systems. The Ombudsman's Office assesses the impact of automated decisions on the observance of

fundamental rights, in particular regarding privacy, equality and the right to effective legal protection. At the same time, the Data State Inspectorate monitors whether the processing of personal data, including through the use of artificial intelligence solutions, complies with the requirements of the General Data Protection Regulation (GDPR). These measures form an important part of the preventive mechanism aimed at protecting the rights of individuals outside the criminal justice framework.
In parallel with potential amendments to the Criminal Law, the need to provide for administrative liability for the use of artificial intelligence for illegal purposes may also be assessed.
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?
As of now, there are no plans for any reforms concerning the protection of copyright in connection with the use of AI. Right now Section 147 of Criminal law regulates criminal liability for a person who commits intentional disclosure of an invention or a design without the consent of the owner of the inventor, designer or the successors in rights thereof prior to the relevant person disclosing the invention or design himself or herself or prior to it be being disclosed with the consent of such persons, as well as commits appropriation of authorship or compelling of joint authorship of an invention or design. In addition, Section 148 of Criminal law regulates criminal liability for a person who commits infringement of copyright or neighbouring right if such infringement has caused substantial harm. We note that these infringements can also be done with the use of AI and considering Criminal law is open and neutral in the environment the crime has been committed, if the infringement has been committed with the use of AI, this will be considered a criminal offence, even if the Section does not specify the use of AI.

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

As mentioned above, in the future there might be reforms considering European Commission proposal for a directive on combating sexual abuse, sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (recast) and Directive 2024/1385 concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes.

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

As mentioned above, artificial intelligence is just another tool in an automated data processing system that can be used to commit most of the criminal offenses provided for in the Criminal law.
In view of the above, the use of artificial intelligence in certain criminal offenses where its use is particularly pronounced or harmful could be defined as an aggravating circumstance (qualifying element).
In view of the above, only in specific cases should special criminal offences related to the use of artificial intelligence be defined.
In addition to the above, given the rapid development of technology and the potential use of artificial intelligence for harmful purposes, Latvian law may in future consider criminalizing certain types of conduct, especially with regard to the production of synthetically generated child sexual material, even if it does not depict a real person, as well as the automated dissemination of disinformation (e.g., in the form of deepfakes) that may threaten national security or public order. Currently, such cases are assessed within the framework of existing norms, but in the future, their inclusion in specific criminal offenses could be considered.
At the same time, in implementing the requirements of the European Union's Artificial Intelligence Regulation (AI Act), Latvia is developing a regulatory and institutional framework aimed at monitoring high-risk artificial intelligence systems, particularly regarding the protection of fundamental rights. This approach may reduce the need for extensive development of new criminal

law provisions, based on the development of preventive, administrative, and supervisory mechanisms.
There is a high risk that the amount of illegal content created by artificial intelligence (especially content containing elements of child pornography) could increase rapidly in the future. The popularization of deepfake technology, which could potentially have a negative impact on national and public security, must also be considered. In view of the above, discussions are underway on determining responsibility.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)
2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

With regard to questions 1 and 2, we would like to point out that Section 244 of the Criminal Law, "Illegal activities with devices that influence the resources of automated data processing systems," already provides for criminal liability for the unauthorized manufacture, adaptation for use, or distribution of such tools (devices, computer programs, computer passwords, access codes or similar data) intended to influence the resources of automated data processing systems. implementation, distribution, acquisition, transfer or storage of tools (devices, computer programs, computer passwords, access codes or similar data) intended to influence the resources of an automated data processing system or with the help of which it is possible to access an automated data processing system or part thereof for the purpose of committing a criminal offense.
At the same time, liability should be provided for the development of intellectual support tools that facilitate criminal offenses, such as terrorist attacks, tax evasion, etc. For example, ChatGPT, which answers these questions in detail or prepares false documents. Unlike support, the intent in such cases may be vague regarding the perpetrator of the crime, as they do not and cannot know who will use the tool. For example, by selling access to this tool on the dark web.
Given the ability of artificial intelligence to adapt and make decisions outside the original programmed framework, it may be necessary in the future to assess whether existing norms are sufficient to clearly and effectively distinguish AI solutions designed for malicious purposes from technologies that are mistakenly used for illegal purposes.
An artificial intelligence system is also a computer program, so the aforementioned section of the Criminal Law already partially covers it.
Under the European Union's Artificial Intelligence Regulation (Regulation (EU) 2024/1689 on the use of artificial intelligence — Article 5 (Prohibited AI systems)), certain AI systems may be completely banned due to the risks they pose. In such cases, the need to establish clear criminal liability for their circulation, including transfer or use, could be assessed in the future if this cannot be covered sufficiently effectively by the application of existing rules.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

In accordance with Section 8 of the Criminal Law, only a person who has committed a criminal offense intentionally (deliberately) or through negligence shall be found guilty of that offense. When determining the form of guilt of a person who has committed a criminal offense, the mental attitude of that person towards the objective characteristics of the criminal offense must be established.
The fourth part of Section 10 of the Criminal Law specifically emphasizes that an offense under the Criminal Law is not criminally punishable if the person did not foresee, did not need to foresee, and could not foresee the harmful consequences of their actions or inaction.
In the context of the attached problem description document, the issue is basically related to the driving of automated (artificial intelligence-controlled) vehicles and the determination of liability in

cases where a road traffic accident has occurred. We believe that before a new legal instrument is developed at the level of the Council of Europe to determine liability for the driving or operation of automated vehicles, a legal framework should be established to determine what types of automated vehicles would be permitted on the road and what technical and safety requirements they would have to meet, as well as how and how often the driver is required to monitor the automated vehicle while it is in traffic.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

Given the nature and rapid spread of the use of artificial intelligence for illegal purposes, the initiative to create an international instrument is timely and should be supported.
Given that the use of artificial intelligence is closely linked to cybercrime in general, it would be necessary not to develop a new international instrument, but rather to supplement the existing Budapest Convention on Cybercrime with regard to the use of artificial intelligence, namely with the legally necessary elements that are not currently covered by the Budapest Convention.
The development of a new instrument would in fact largely duplicate what is already covered by the Budapest Convention, for example Article 11 - Attempt and participation or incitement, Article 12 - Liability of legal persons, Article 13 - Sanctions and measures, Subsection 2 - Procedural rules, Subsection 3. Jurisdiction, Chapter 3. International cooperation, Chapter 4 - Final provisions.
Furthermore, Article 44 of the Budapest Convention, "Amendments," stipulates that amendments to this Convention may be proposed by any Party and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to non-member States but which have participated in the elaboration of this Convention, as well as to any other State which has acceded to or been invited to accede to this Convention in accordance with the provisions of Article 37. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDCP), which shall submit its opinion on the proposed amendment to the Committee of Ministers. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the European Committee on Crime Problems (CDCP) and, after consulting the non-member States, the Parties to this Convention shall adopt the amendment.
The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
Any amendment adopted in accordance with paragraph 3 of this article shall enter into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance.
If it is not possible to incorporate amendments concerning the use of artificial intelligence directly into the articles of the Budapest Convention, the related issues may be addressed in a separate protocol to be annexed to the Budapest Convention.
.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
X definitions
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

Yes, the definitions should align with those in the AI Act.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?
4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

In response to questions 3 and 4, the most important issues are definitions and possible criminal offenses related to the use of artificial intelligence.
All other issues have already been addressed in the Budapest Convention and should not be duplicated in the new legal instrument (see previous answer).
In the context of the relevance of the intergovernmental instrument, we would like to inform you that, within the framework of Interpol cooperation, the illegal circulation of uncontrolled artificial intelligence-generated content (AI-generated CSAM (hereinafter - AIG-SCAM)) has been detected, which poses serious problems for law enforcement authorities. AIG-SCAM is widely used, including for the purpose of altering photos or videos of real people in order to blackmail them, extort money, etc. Artificial intelligence models are freely available online that can be adapted and specifically trained to produce such material. Investigating incidents involving AIG-SCAM requires specialised police personnel with specific knowledge and extensive experience. Working with such materials places an enormous burden on law enforcement agencies and prevents them from focusing on cases involving real victims. Companies, countries, and law enforcement agencies are developing tools that could effectively combat AIG-SCAM, but there is a lack of coordination of these initiatives at the international level. In this context, there is also an active increase in the use of fake news, deep fakes, specialized bots – commentators and bot farms – for illegal purposes. A specialized mechanism for international cooperation would also be necessary to combat this phenomenon.

LITHUANIA

A: Existing Frameworks

2. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Lithuanian legislation and case law do not address criminal liability and offences involving artificial intelligence. General rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

At national level, there are no specific rules in relation to criminal offences under use of AI systems.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

There is no national case law or domestic law that would address usage of AI as aggravating circumstance.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

Lithuanian legislation does not address specific AI technologies in relation to criminal offences. General rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:
The use of AI is not addressed as an aggravating or mitigating circumstance in national legislation.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

No, there are no examples of national case law or investigative practice relating to crimes committed or facilitated by artificial intelligence.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

The Lithuania legislator has no immediate plans for legal reforms related to artificial intelligence in the context of criminal liability. Of course, the Republic of Lithuania is always ready to assess situations where the use of artificial intelligence tools may cause greater harm or criminal consequences. If we identify a specific need to distinguish criminal acts committed with the help of artificial intelligence, where general provisions are no longer sufficient, we would initiate amendments to the relevant legislation.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

The Lithuanian legislator has no immediate plans for legal reforms on aggravating circumstances where a crime is committed, facilitated, aggravated or assisted by the use of artificial intelligence systems.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

In the case of criminal acts committed with the aid of artificial intelligence, we believe that this is exclusively a matter for criminal law.

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

The Lithuanian legislator has no immediate plans for legal reforms related to copyright protection in the context of the use of artificial intelligence. General rules apply in situations where such actions, if deemed illegal, would be committed, facilitated, enhanced, or aided by artificial intelligence.

5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

Currently, the Lithuanian legislator has no plans for legal reforms related to the development of applications facilitating the creation of deepfakes or the use or distribution of deepfakes. Material of this nature, if it involves pornographic content or the sexual exploitation of children, is criminalized in Lithuania regardless of whether it is real or created with the help of artificial intelligence.

6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

At present, the Ministry of Justice of the Republic of Lithuania has not received any proposals or requests to extend the scope or grounds for criminal liability in relation to artificial intelligence. We believe that even criminal offences committed with the help of artificial intelligence, although they may be more dangerous, are covered by the general provisions on criminal offences.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

At present, we see no specific need to tighten existing criminal liability for the aforementioned actions in order to single out artificial intelligence systems. Of course, practices and situations are constantly changing with the rapid development of technology, so we are always ready to respond and initiate legislative changes when there is a clear need.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

If an increase in the use of such technologies and the criminal acts committed using them were to be identified, it is likely that there would be a real need to criminalize the possession of the prohibited technology itself.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

This is a complex issue, and there are currently no answers. The question arises as to whether legislation could regulate such situations, but there is no doubt that it is worthwhile to discuss and seek the most effective solutions to this issue.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

We certainly do not rule out this possibility and are always willing to discuss the creation of new legislation, provided that a thorough impact assessment has been carried out and there is a real need for it.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
X definitions
X procedural provisions,
X jurisdiction provisions
☐ extradition and mutual assistance issues
☐ problems with digital evidence
☐ collaboration of digital AI platforms with criminal prosecutions
☐ other issues

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

Yes, the definitions should align with those in the AI Act, to ensure uniformity in regulation and guidelines, as well as recommendations preceding it, and to ensure clarity in regulation.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

Cybercrime by using AI systems.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

Advantages:
- Uniformity in regulation;
- Clarity in use of definitions, base rules, principles;
- Possible uniformity in practice and policy.

Disadvantages:
- Could undermine AI and related market progress;
- A singular regulation could undermine national legal traditions (be in prejudice with them);
- An international global instrument could become more sever sanctions-wise than a national one.

MALTA

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Maltese legislation does not currently contemplate criminal liability for non-living entities. Criminal liability requires the presence of two factors, namely the actus reus, which is the prohibited action or conduct, and the mens rea, which is the intention to commit the said action or conduct.
General principles of responsibility for wilful acts or acts of negligence will be attributed where these can be detected on the person of programmer, user or hacker where applicable.
Where companies are invlved criminal corporate liability may additionally be invoked.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

Under general principles of criminal law they are deemed to be instruments or weapons in the commission of the crime. The responsibility will be borne by the user / programmer where it can be shown that he/she has acted with criminal intent or negligence.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

No this is not the case.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

No it does not. This would fall under the generic offence of “computer misuse”, which, generally speaking would be the offence of interfering with software or hardware (importing/exporting/altering/modifying etc).

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:

No. If computer misuse is detected, it would be treated as an additional offence.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

No

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

N/A

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

N/A

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

N/A

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

N/A

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

N/A

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

N/A

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
□ definitions
□ procedural provisions,
☐ jurisdiction provisions
☐ extradition and mutual assistance issues
☐ problems with digital evidence
☐ collaboration of digital AI platforms with criminal prosecutions
☐ other issues

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

MONACO

A: Cadres existants

1. Votre législation nationale et/ou votre jurisprudence abordent-elles spécifiquement la responsabilité pénale ou les infractions liées à l'intelligence artificielle ?
Le cas échéant, pourriez-vous s'il vous plaît :
(1) fournir, si disponible, les textes pertinents (en anglais ou en français) ;
(2) indiquer si la responsabilité pénale est attribuée à une personne spécifique (physique ou morale, par exemple : conducteur, producteur, programmeur, superviseur de flotte, téléopérateur, etc.) et sur quel fondement elle repose (à savoir : responsabilité objective, négligence, intention).

Dans le cas contraire, les règles générales s'appliqueront-elles dans les situations où des infractions sont commises, facilitées, renforcées ou assistées par l'intelligence artificielle ?

a) Législation et jurisprudence :
À ce jour, la législation monégasque ne prévoit pas de disposition spécifique relative à la responsabilité pénale de l'intelligence artificielle. Le Code pénal monégasque ne reconnaît pas de personnalité juridique à l'intelligence artificielle et aucune jurisprudence nationale n'a encore eu à trancher une affaire impliquant directement une intelligence artificielle autonome en tant qu'auteur ou objet d'infraction.

b) Application du droit pénal général :
En droit positif interne, les règles générales du Code pénal s'appliquent dans les situations où des infractions seraient commises ou facilitées par une intelligence artificielle.

Les textes applicables relèvent alors du droit pénal général.

L'article 4 du Code pénal pose le principe de la responsabilité pénale personnelle. Ainsi, « nul n'est responsable pénalement que de son propre fait ». L'auteur d'une infraction est celui qui commet le fait incriminé ou qui tente de commettre un crime, ou un délit lorsque la loi érige le délit au régime de la tentative punissable (C.P., art. 2, 3 et 4-3). Il n'y a point de crime ou de délit sans intention de le commettre, hormis les cas où la loi prévoit qu'un délit puisse être réalisé par imprudence, négligence, voire par le manquement à une obligation de prudence ou de sécurité (C.P., art. 4-2).

Les personnes morales peuvent également voir leur responsabilité pénale engagée, à l'exclusion de l'État, de la commune ou des établissements publics, lorsqu'un crime ou un délit a été commis pour son compte, par l'un de ses organes ou de ses représentants (C.P., art. 4-4). Bien entendu, l'engagement de la responsabilité pénale d'une personne morale n'exclut en rien la possibilité de poursuivre, en qualité de co-auteurs ou de complices, des personnes la représentant au moment des faits.

A ce titre, concernant la complicité, l'article 42 qualifie de complice d'un crime ou d'un délit toute personne :
- Qui aura provoqué, donné des instructions, ou bien facilité sa commission par dons, promesses, menaces, abus d'autorité ou de pouvoir, machinations ou artifices ;
- Qui aura procuré des armes, des instruments ou tout autre moyen qui aura servi à l'action, sachant qu'ils devaient y servir ;
- Qui aura, avec connaissance, aidé ou assisté l'auteur ou les auteurs de l'action dans les faits qui l'auront préparée ou facilitée, ou dans ceux qui l'auront consommée, sans préjudice des peines qui seront spécialement portées par le présent code contre les auteurs de complots ou de provocations attentatoires à la sûreté intérieure ou extérieure de l'État, même dans le cas où le crime qui était l'objet des conspirateurs ou des provocateurs n'aurait pas été commis.

Les complices d'un crime ou d'un délit sont punis des mêmes peines que les auteurs de ces crimes ou délits, sauf les cas où la loi en disposerait autrement (C.P., art. 41).

c) Application dans le cadre d'infraction réalisée par ou au moyen d'une intelligence artificielle :
En l'absence de dispositions spécifiques, la responsabilité pénale d'une personne physique ou morale peut être engagée si cette personne est impliquée soit dans la conception ou l'usage d'une intelligence artificielle à des fins infractionnelles, soit dans les conséquences dommageables de ladite IA dans le cas de l'incrimination de faits involontaires. Selon les circonstances, cela pourrait viser :

- Le concepteur ou programmeur : en cas de programmation défectueuse ou de défaut de supervision, voire d'une intention délinquantielle (dol) dans la conception du système d'intelligence artificielle afin que ce dernier soit un logiciels malveillants auto-apprenants programmé pour réaliser des cyberattaques autonomes.
- L'opérateur humain ou superviseur (par action ou omission), qui peut, par exemple être assisté d'une intelligence artificielle afin de réaliser des escroqueries ou des fraudes.
- La personne morale exploitant le système, si l'infraction a été commise pour son compte par l'un de ses organes ou de ses représentants.

2. Quelles règles générales sont appliquées dans votre droit lorsque des systèmes d'intelligence artificielle (tels que définis à l'article 2 de la CAI, STCE n° 225) sont utilisés comme outils pour la commission intentionnelle d'infractions pénales (telles que le meurtre, l'homicide involontaire ou le vol) ?

a) Absence de cadre juridique spécifique à l'intelligence artificielle :
Le Code pénal monégasque n'intègre pas la notion d'intelligence artificielle. Ainsi, l'intelligence artificielle utilisée comme un « outil » dans la commission d'une infraction est juridiquement traitée comme tout autre moyen technique (ex. : arme, logiciel, véhicule).

b) Application des règles générales en cas d'usage d'une intelligence artificielle comme instrument d'une infraction :
Conformément à la réponse précédente, pour les personnes physiques, seul l'auteur de l'infraction, son co-auteur, et le complice ou le receleur peuvent voir leur responsabilité pénale engagée. Si ces derniers sont les organes ou représentants d'une personne morale et qu'ils ont agit pour son compte, la responsabilité pénale de la personne morale pourrait également être engagée.

N'ayant pas la personnalité juridique, une intelligence artificielle n'est pas titulaire ni de droits ni d'obligations juridiques. Elle ne peut donc pas être considéré comme un auteur ou un co-auteur.

Dans le cadre d'un meurtre réalisé au moyen d'une intelligence artificielle, ce système informatique serait considéré comme un instrument matériel, un moyen technique, ayant permis de faciliter la réalisation de l'infraction.

3. Selon votre droit interne et/ou votre jurisprudence, l'utilisation de systèmes d'intelligence artificielle peut-elle être considérée comme une circonstance aggravante ?

À ce jour, la législation pénale monégasque ne prévoit pas expressément que l'usage de l'intelligence artificielle constitue une circonstance aggravante. Toutefois, en l'absence de disposition spécifique, certains articles du Code pénal peuvent être invoquer.

L'utilisation d'un outil technologique perfectionné (comme l'intelligence artificielle) peut être prise en compte comme une forme de préméditation selon les circonstances d'espèce, voire comme la démonstration de la vulnérabilité ou d'un état de dépendance de victime.

La préméditation est définie par l'article 233 du Code pénal comme « le dessein formé, avant l'action, d'attenter à la personne d'un individu déterminé ou même de celui qui sera trouvé ou rencontré, quand bien même ce dessein serait dépendant de quelque circonstance ou de quelque condition ».

La vulnérabilité ou l'état de dépendance de la victime peut être démontré, notamment, par des manipulations de l'auteur au moyen d'un système d'intelligence artificielle ou encore par l'emploi de l'hypertrucage ou deepfake.

4. Votre législation traite-t-elle de l'utilisation de technologies spécifiques d'intelligence artificielle pour commettre des infractions, par exemple l'utilisation de deepfakes dans certains contextes (tels que les deepfakes à caractère sexuel, le harcèlement sexuel en ligne, ou lors des processus électoraux), l'utilisation de drones autonomes pour tuer quelqu'un, ou des formes spécifiques de fraude ?

Le droit monégasque ne comporte pas de dispositions pénales spécifiques relatives à l'usage de technologies d'IA telles que :

- Les deepfakes hypertrucages, y compris à caractère sexuel ou en contexte électoral ;
- Les drones autonomes utilisés pour commettre des homicides ;
- Les algorithmes d'escroquerie ou de fraude automatisée.

S'agissant des drones, l'article 391-1 bis, relatif à l'acte de terrorisme, parle du « pilotage d'aéronefs » ; le drone totalement autonome, « non piloté » n'est pas spécialement incriminé. Il serait fait alors usage de l'article 241 du code pénal :
« Constituent des armes, au sens de l'article précédent tous objets qui, par leur nature ou par l'usage auquel leur porteur les destine, peuvent servir à provoquer des blessures ».

Cependant, les incriminations existantes peuvent s'appliquer à ces situations en fonction de l'infraction sous-jacente. Par exemple :

- L'usage d'un hypertrucage deepfake peut être poursuivi au titre d'atteinte à l'intimité de la vie privée. L'article 22 de la Constitution garanti le droit au respect de la vie privé et familiale et l'article 22 du Code civil précise que ce droit est protégé pour toute personne vivante ou décédée. De facto, toute atteinte à ce droit est pénalement répréhensible. En effet, l'article 308-3 , chiffre 2, du Code pénal, réprime le fait d'avoir sciemment porté où tenter de porter atteinte au droit à la vie privée d'une personne, notamment par fixation ou transmission d'image, sans qu'il n'y ait eu consentement de celle-ci, en publiant, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image de la personne concernée.

- L'utilisation d'un drone létal, s'il est contrôlé par une personne physique ou qu'il est programmé à cette fin, peut engager la responsabilité pour meurtre (C.P., art. 220), voire d'assassinat si la préméditation est démontrée (C.P., art. 221).

- La fraude via une intelligence artificielle relève des dispositions sur l'escroquerie (C.P., art. 330), notamment si l'intelligence artificielle a été utilisée comme moyen de tromperie technologique.

5. L'utilisation de l'IA est-elle considérée comme une circonstance aggravante, notamment dans les cas impliquant :
☐ deepfakes à caractère sexuel
☐ harcèlement sexuel en ligne
☐ processus électoraux
☐ utilisation de drones autonomes pour tuer quelqu'un
☐ fraude d'une importance notoire
☐ autre :

À ce jour, la législation pénale monégasque ne prévoit pas expressément que l'usage de l'intelligence artificielle constitue une circonstance aggravante.

6. Y a-t-il des exemples de jurisprudence nationale ou de pratiques d'enquête (par exemple, enquêtes pénales, évaluations du parquet) impliquant des infractions commises ou facilitées par l'intelligence artificielle ? Si oui, merci de résumer le(s) cas ou de décrire les problématiques, si possible.

À ce jour, il n'existe pas de jurisprudence publiée ni de cas publics recensés à Monaco concernant des infractions pénales impliquant directement des systèmes d'intelligence artificielle.

B. Plans futurs

1. Le législateur de votre pays prévoit-il des réformes législatives concernant la responsabilité (pénale) et les infractions liées à l'IA ?

Aucun projet de réforme législative spécifique relatif à la responsabilité pénale ou aux infractions impliquant des systèmes d'intelligence artificielle n'est inscrit à l'agenda législatif monégasque. Toutefois, une veille juridique est assurée par les autorités compétentes, notamment face à l'évolution du droit européen et aux instruments élaborés ou qui sont en cours d'élaboration au sein du Conseil de l'Europe et la Direction des Services Judiciaires devrait dans les prochains mois proposer des ajustements normatifs.

2. Le législateur de votre pays prévoit-il des réformes législatives concernant les circonstances aggravantes lorsque qu'une infraction est commise, facilitée, renforcée ou assistée par l'utilisation de systèmes d'IA ?

Aucune réforme en ce sens n'est actuellement envisagée. La Direction des Services Judiciaires devrait toutefois dans les prochains mois proposer des ajustements normatifs.

3. Votre législateur envisage-t-il de relever les nouveaux défis liés à la protection effective des droits mis en péril par l'utilisation des systèmes d'IA par des mesures autres que l'adoption de nouvelles lois pénales ? Si oui, comment ?

Monaco adopte une approche transversale et coordonnée reposant sur l'éducation numérique de la population, le renforcement des capacités des magistrats, des services d'enquête et des autorités de poursuite dans le domaine de la criminalité technologique, ainsi que sur une coopération internationale renforcée. Cette coopération se manifeste notamment par l'adhésion de la Principauté à des instruments internationaux comme la Convention de Budapest sur la cybercriminalité et la Convention de Lanzarote sur la protection des enfants contre l'exploitation sexuelle, qui couvrent certains aspects liés aux risques technologiques.

Dans le cadre de sa stratégie numérique « Extended Monaco » lancé en 2019, le Gouvernement princier met en œuvre des actions de sensibilisation du public aux usages responsables du numérique, tout en développant des dispositifs de protection face aux risques émergents, notamment en matière de cybersécurité, de désinformation et de manipulation technologique. Ces politiques publiques visent à anticiper l'évolution des menaces liées aux technologies d'intelligence artificielle, sans exclure, à moyen terme, une adaptation du cadre législatif si les circonstances l'exigent.

4. Le législateur de votre pays prévoit-il des réformes législatives concernant la protection du droit d'auteur en lien avec l'utilisation de l'IA (par exemple, en raison du web scraping, du web harvesting ou de l'extraction de données à partir de sites web pour entraîner des modèles linguistiques de grande taille) ?

Actuellement, aucun projet de réforme spécifique ne concerne le droit d'auteur en lien avec l'utilisation de l'IA, en particulier sur le web scraping ou l'entraînement de modèles linguistiques.

5. Le législateur de votre pays prévoit-il des réformes législatives concernant le développement d'applications facilitant la production de deepfakes (à caractère sexuel), ou l'utilisation ou la diffusion de deepfakes (à caractère sexuel) ?

Aucune disposition spécifique ne vise aujourd'hui la création ou la diffusion de deepfakes, y compris à caractère sexuel. La réglementation existante sur les atteintes à la vie privée, à l'image et à la dignité peut toutefois s'appliquer à ces situations. Des évolutions législatives futures ne sont pas exclues si la pratique venait à s'intensifier.

6. Au regard de votre contexte national et des évolutions juridiques, existe-t-il d'autres comportements ou activités impliquant l'intelligence artificielle que vos autorités estiment devoir être pénalement réprimés à l'avenir ? Le cas échéant, veuillez décrire ces comportements et, si possible, en expliquer les raisons.

A ce jour, aucun comportement infractionnel ou seulement problématique impliquant l'intelligence artificielle n'a été constaté par les instances de la Principauté de Monaco.

C. Évaluation de la nécessité d'un nouvel instrument

1. Voyez-vous la nécessité d'un nouveau type d'infraction liée à l'IA obscure (« dark AI ») ? (Ceci fait référence aux systèmes d'IA spécialement conçus à des fins malveillantes, tels que le piratage, le cracking ou d'autres cyberattaques, ainsi qu'aux IA destinées à cibler les infrastructures critiques, à créer des risques sérieux pour la sécurité publique ou à faciliter la commission de toute infraction.).

La législation pénale monégasque ne comporte à ce jour aucune disposition spécifique relative à l'intelligence artificielle, et aucun régime autonome ne vise les systèmes d'intelligence artificielle conçus à des fins malveillantes. Toutefois, dans une perspective d'anticipation, il pourrait être pertinent de réfléchir à la reconnaissance d'une infraction autonome visant les usages spécifiquement délictueux de systèmes qualifiés de « dark AI ». Ces systèmes, lorsqu'ils sont développés dans le but de contourner des dispositifs de sécurité, de faciliter des cyberattaques ou de porter atteinte à la sécurité publique ou à des infrastructures critiques, peuvent s'avérer difficilement saisissables par les qualifications pénales traditionnelles, notamment en l'absence d'un lien direct entre l'auteur humain et l'acte commis.

Dans ce contexte, sans préjuger de l'évolution du droit positif monégasque, une incrimination future pourrait permettre de mieux appréhender l'intentionnalité dans la conception ou la diffusion de telles technologies, et de combler les éventuelles lacunes que les qualifications classiques (telles que l'accès frauduleux à un système automatisé, le sabotage ou l'atteinte à la sûreté de l'État) ne couvriraient pas entièrement.

La Direction des Services Judiciaires reste donc attentive aux développements doctrinaux et aux initiatives internationales dans ce domaine, en particulier celles portées par le Conseil de l'Europe, afin de proposer ou de participer aux travaux relatifs à une incrimination à moyen terme, dans le respect des principes fondamentaux du droit pénal monégasque.

2. Considérez-vous qu'il est nécessaire d'introduire un nouveau type d'infraction visant à réprimer la mise sur le marché, la mise en service, la production, l'acquisition pour usage personnel, l'importation ou la fourniture à des tiers – sous quelque forme que ce soit – d'un système d'IA interdit par la législation nationale ou européenne ?

La législation monégasque ne prévoit actuellement aucune incrimination autonome visant la mise sur le marché, la mise en service, la production, l'acquisition à usage personnel, l'importation ou la fourniture à des tiers de systèmes d'intelligence artificielle interdits. En l'état du droit, de tels

comportements ne sont appréhendés qu'à travers les qualifications pénales classiques éventuellement applicables, en fonction de l'usage final ou des conséquences de ces technologies.

Cela étant, dans une logique de prévention et de sécurité juridique, il pourrait s'avérer opportun, à court/moyen terme, de réfléchir à l'introduction d'une infraction spécifique permettant de sanctionner l'ensemble des comportements liés à la diffusion de systèmes d'intelligence artificielle explicitement prohibés par des normes nationales ou internationales.

3. Considérez-vous nécessaire d'adopter des mesures spécifiques pour traiter le « dilemme de la négligence » résultant des actions autonomes des systèmes d'IA ?

Le développement de systèmes autonomes soulève le besoin d'adopter des mesures spécifiques pour traiter ce que l'on désigne comme le « dilemme de la négligence ». Dans certains cas, des dommages ou infractions pourraient être générés sans action humaine directe, du fait d'un défaut de conception, de supervision ou de maintenance. Le droit pénal étant fondé sur la responsabilité personnelle, il conviendrait d'adapter les notions de faute, d'imprudence ou de négligence à la réalité des systèmes autonomes, de manière à garantir l'imputabilité juridique tout en respectant les principes fondamentaux de la responsabilité pénale du fait involontaire. Cette adaptation permettrait d'éviter à la fois les impunités techniques et les imputations excessives de responsabilité.

4. Voyez-vous la nécessité de créer un instrument international (Convention sur l'IA et les infractions) similaire à la Convention de Budapest sur la cybercriminalité, qui définirait et pénaliserait les actes pouvant être commis, facilités, renforcés ou aidés par des systèmes d'IA ?

Au regard de l'évolution rapide des technologies et de la nature transnationale des menaces, la création d'un instrument international dédié à l'intelligence artificielle et aux infractions paraît opportune. À l'instar de la Convention de Budapest sur la cybercriminalité, un tel instrument pourrait définir les principales infractions commises ou facilitées par l'intelligence artificielle, encadrer les procédures de coopération internationale et offrir aux États un cadre commun pour lutter contre les abus technologiques.

D. Contenu d'un éventuel nouvel instrument, s'il est élaboré

1. Selon vous, quels éléments suivants un éventuel nouvel instrument international (Convention sur l'IA et les infractions) pourrait-il inclure ?

- ✓ **Définitions**
- ✓ **Dispositions procédurales**
- ✓ **Dispositions relatives à la compétence juridique**
- ✓ **Questions d'extradition et d'entraide judiciaire**
- ✓ **Problématiques liées aux preuves numériques**
- ✓ **Collaboration des plateformes numériques d'IA avec les poursuites pénales**
- ✓ **Autres questions : mesures de prévention et d'alerte, protection des victimes, mécanismes de supervision éthique des IA à haut risque.**

2. Êtes-vous d'accord pour que les définitions s'alignent sur celles de la loi sur l'IA (AI Act) ? Merci de préciser.

Un alignement avec les définitions prévues par le règlement européen sur l'intelligence artificielle (AI Act) est en principe souhaitable, dans un objectif de cohérence juridique, technique et réglementaire à l'échelle européenne et internationale. Le AI Act fournit un cadre structuré pour identifier les systèmes d'intelligence artificielle, leurs niveaux d'autonomie, leurs usages et leurs

niveaux de risque, ce qui peut s'avérer utile pour encadrer juridiquement les technologies concernées.
Toutefois, dans le contexte spécifique du droit pénal, une transposition intégrale et automatique de ces définitions pourrait se révéler inadaptée. Le champ pénal implique de caractériser des éléments subjectifs comme l'intention criminelle, la négligence, ou la conscience du risque, ainsi que d'établir un lien de causalité entre l'action humaine et le résultat dommageable. Or, les définitions du AI Act, élaborées dans une logique de régulation économique et préventive, n'intègrent pas ces éléments fondamentaux du droit répressif.
Il conviendrait donc que les définitions techniques issues du AI Act soient adaptées, dans un instrument pénal, aux exigences propres à la matière pénale. Cette articulation est indispensable pour garantir à la fois la clarté juridique et l'efficacité des poursuites, tout en évitant les imprécisions ou les lacunes dans la qualification des comportements illicites liés à l'intelligence artificielle.

3. Parmi les questions ci-dessus (le cas échéant), lesquelles considérez-vous comme les plus urgentes à traiter en matière d'IA et de droit pénal ?

- La diffusion de contenus illicites générés par IA (deepfakes, faux documents, etc.) ;
- La fraude algorithmique à grande échelle ;
- La responsabilité des personnes impliquées dans la chaîne IA (concepteur, exploitant, utilisateur) ;
- La coopération transfrontalière pour la saisie des preuves générées ou traitées par des systèmes IA.

4. Quels seraient, selon vous, les avantages ou les inconvénients d'un instrument mondial unique traitant de l'IA et du droit pénal, par rapport à des lois distinctes dans des domaines spécifiques ?

La mise en place d'un instrument international unique en matière d'intelligence artificielle et de droit pénal présenterait plusieurs avantages importants. Elle permettrait notamment une harmonisation des définitions et des procédures applicables entre les États, ce qui favoriserait la cohérence des approches juridiques. Elle faciliterait également la coopération pénale entre les juridictions nationales, en posant un socle commun pour la poursuite d'infractions commises ou facilitées par des systèmes d'intelligence artificielle. Par ailleurs, un tel instrument renforcerait la capacité des États à répondre efficacement aux menaces transnationales, notamment celles qui relèvent de la cybercriminalité automatisée, de la désinformation numérique ou de la fraude algorithmique.

Néanmoins, la création d'un instrument global pourrait soulever certaines difficultés. L'adaptation de normes communes à la diversité des systèmes juridiques nationaux pourrait se révéler complexe, tant sur le plan technique que constitutionnel. Il existe également un risque de dilution des spécificités juridiques propres à certains États, notamment en matière de responsabilité pénale ou de garanties procédurales. Enfin, la nature évolutive et rapide des technologies d'intelligence artificielle pose la question de la réactivité d'un cadre international, qui pourrait ne pas suivre suffisamment rapidement l'émergence de nouvelles pratiques ou de nouveaux outils.

En conséquence, tout en reconnaissant les bénéfices d'une approche unifiée, il conviendrait de veiller à ce que cet instrument soit conçu de manière souple, adaptable, et respectueuse des particularités juridiques des États parties.

NETHERLANDS

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?

If so, could you please:

(1) provide, if available, the relevant texts (in English or in French);

(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).

If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Dutch criminal law is technology-neutral and does not specifically address AI-specific criminal liability. However, conduct using or targeting AI is prosecuted under existing offences such as:

o Article 252

Any person who distributes, offers, publicly displays, manufactures, imports, exports, acquires, possesses, or obtains access to a visual representation of a sexual nature or with an unmistakably sexual connotation involving a person who is clearly under the age of eighteen, or who appears to be under the age of eighteen, shall be punished with imprisonment of up to six years or a fine of up to five hundred thousand dollars. imports, transports, exports, acquires, possesses, or obtains access to it shall be punished with imprisonment of up to six years or a fifth-category fine.

With the entry into force of the Sexual Offenses Act, Article 252 of the Criminal Code has become the legal successor to Article 240b of the Criminal Code, which remained in force until July 1, 2024.

Based on the legislative history of Article 240b (old) of the Criminal Code, case law has determined that the element ‘apparently involved’ in the description of the offense in Article 240b (old) of the Criminal Code means that this criminal provision also includes a realistic image of a non-existent child, in the sense that the image cannot be distinguished from the real thing. Computer animations therefore fall within the scope of Article 240b (old) of the Criminal Code if they cannot be distinguished from reality at first glance.

Case law shows that this is the case when images depicting sexual acts involving persons who have reached the age of twelve but not yet the age of sixteen are realistic at first glance and cannot be distinguished from real images. Case law also shows that such images are intended to arouse sexual excitement and are therefore child pornographic in nature. The foregoing means that these virtual child pornographic images also fall within the scope of Article 240b (old) of the Dutch Criminal Code.

It should be noted that computer animation is not necessarily a form of AI. Animations can simply be created using traditional 2D or 3D software such as Blender, Maya, or drawing programs. AI only comes into play when techniques are used to automatically generate or improve animations. This is becoming increasingly common nowadays. Generative AI can be used, among other things, to:

- modify existing photos (e.g., deepfakes or so-called “nudify” apps),

- create entirely new, artificially generated children or people, and create animations or videos based on a text description (“text-to-video”).

Legally, it makes no difference whether the fake child pornographic image was created with AI or classic animation software; in both cases, it falls under Article 252 of the Criminal Code and Article 240b (old) of the Criminal Code and is punishable by law.

A sexual deepfake, also known as a ‘pornographic deepfake’ or ‘deepnude’ of and featuring adults, is punishable under Article 254ba of the Criminal Code.

o Article 254ba of the Dutch Criminal Code

1 Any person that intentionally and unlawfully:

(a) consolidates a visual representation of a sexual nature;

(b) has a visual representation as referred to under a, while he knows or should reasonably suspect that it has been obtained by or as a result of an act established under a,

shall be punished with imprisonment of not more than one year or fine of the fourth category.

2 Any person that

(a) publishes a visual representation as referred to in paragraph 1(a) while knowing or reasonably suspecting that it has been obtained by or as a result of an act punishable under the first paragraph, under a;

(b) publishes a visual representation of a sexual nature of a person, while knowing that such publication may be detrimental to that person,

shall be punished with imprisonment of up to two years or fine of the fourth category.

With the entry into force of the Sexual Offenses Act, Article 254ba of the Criminal Code has become the legal successor to Article 139h of the Criminal Code, which remained in force until July 1, 2024.

A court ruling has established that a deepfake pornographic video falls within the scope of Article 139h of the Criminal Code (old)/Article 254ba of the Criminal Code. essentially boils down to whether the element of sexual imagery/visual representation of a sexual nature in that article can be proven in that case.

According to the ruling in question, the interest to be protected is that sexually suggestive images may not be produced against a person's will, or that such images must remain private if their disclosure could be detrimental to the person depicted. The ruling stipulates that sexually explicit images in the form of deepfake images also fall under this interest to be protected, provided that the images in question appear so real that it is not immediately apparent that they have been manipulated.

In that case, it is important that the average, reasonably minded person who views the footage with an open mind (and therefore without prior knowledge of the fact that it is a deepfake) can reasonably believe at first glance that the person depicted in the footage is actually that person. In such a case, it may be clear to the person depicted that the images are not real, but this is not necessarily the case for the outside world. This interpretation is in line with what the legislator

states in the explanatory memorandum, namely that an image of a sexual nature is an image that ‘is of such an intimate sexual nature that it will be considered private by any reasonable person’. The degree of invasion of privacy involved in the production and/or publication of an authentic video is not substantially different from that involved in the production and/or publication of a deepfake that is indistinguishable or barely distinguishable from the real thing.

In such cases, the court is of the opinion that deepfake sexual imagery can be classified as an image of a sexual nature/a visual representation of a sexual nature as referred to in Article 139h Sr/254ba of the Criminal Code.

Neither article explicitly refers to AI-generated material, but such material does fall within the scope as it refers to a 'visual representation'.

Moreover, it is a criminal offence to possess, manufacture, acquire, etc. a technical aid that has been designed or modified for the purpose of committing a cybercrime such as computer-hacking (article 138ab of the Criminal Code). AI systems can be such technical aid.

Article 139d of the Criminal Code reads as follow:

1. Any person who has a technical device installed in a particular place with the intention of unlawfully using it to eavesdrop on, intercept or record a conversation, telecommunications or other type of data transfer or data processing by a computerised device or system shall be liable to a term of imprisonment not exceeding two years or a fine of the fourth category.

2. Any person who:

a. manufactures, sells, obtains, imports, distributes or otherwise makes available or has in his possession a technical device that has been primarily adapted or designed for the commission of such serious offence, or

b. manufactures, sells, obtains, distributes or otherwise makes available or has in his possession a computer password, access code or similar data that can be used for accessing a computerised device or system or a part thereof;

with the intention of using it in the commission of a serious offence, as referred to in article 138ab(1), 138b or 139c, shall be liable to the same punishment.

3. Any person who commits the offence referred to in subsection (2) with a view to the commission of a serious offence as referred to in article 138a(2) or (3), shall be liable to a term of imprisonment not exceeding four years or a fine of the fourth category

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

That AI is used to commit a criminal offence is in itself not relevant.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

There is no legal provision that automatically considers the use of AI to be an aggravating factor. Let alone that criminal offenses are punished more severely solely because of the use of AI.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

No.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:

☐ sexual deepfakes

☐ online sexual grooming

☐ electoral processes

☐ use of autonomous drones to kill someone

☐ fraud of notorious importance

☐ other:

No

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

We are encountering problems with nudity apps or websites. These are sometimes hosted in the EU, at times in the US. It is the question whether producing such an app could be a crime in itself; as it is mostly used in malicious ways. It could also be the case that unlawful collected data is used for training the model (so for example child pornography or adult nude images used without consent).

In regards to case law:

ECLI:NL:RBAMS:2023:6923 concerns a judgment of the court of first instance.

The facts:

The complainant filed a report on September 29, 2022, after learning on October 28, 2021, that a so-called deepfake porn video of her was circulating on the internet. This porn video involved the face of a female porn actress being replaced with the complainant's face using a computer program. In response, the complainant made a documentary, and as part of that documentary, cyber investigators traced the IP address of the person who posted the deepfake porn video. Based on this IP address, the police tracked down the suspect. The suspect confessed to the police and in court that he had made the deepfake porn video using software developed for that purpose and that he had then posted it on the internet.

Charges:

In short, the defendant is charged with the following offenses committed in Amersfoort between November 1, 2020, and October 28, 2021:

Fact 1: intentionally and unlawfully produced one or more images and/or videos of a sexual nature of the complainant by digitally editing a pornographic video in such a way that the face/head of the complainant was placed on the face/head of another (unknown) naked woman;

Fact 2: made this pornographic video public, while he knew that such disclosure could be detrimental to the complainant.

Legal assessment

Fact 1

With regard to the charge under 1, it must be assessed whether the defendant intentionally and unlawfully produced an image of a sexual nature of a person.

Intentional and unlawful production

The report indicates that the act was unlawful. After all, the complainant did not give the defendant permission to make a deepfake pornographic video of her. The defendant selected a pornographic video clip, collected images of the complainant, and then used special software to create a deepfake pornographic video, proving that the defendant produced it. The defendant acted deliberately and knew that he did not have the complainant's consent, so that intent to commit an unlawful act has also been proven.

An image of a sexual nature

The court has determined that sexual deepfake images can be classified as images of a sexual nature of a person when, in short, they appear so real that, at first glance, a reasonable person cannot distinguish them from real images. In the present case, it has been established that the defendant made a deepfake pornographic video. The court viewed the deepfake pornographic video in question in chambers. Naturally, the court was already aware at that point that the video was not real, but a deepfake pornographic video. With this knowledge, the court carefully examined the video and observed a number of inconsistencies. However, for the average, reasonably minded person who watches the deepfake porn video with an open mind and without this prior knowledge, these inconsistencies will not detract from the realism of the images, and the video will give the impression that the person whose head is seen in the video is also the person performing and undergoing the sexual acts. In the court's opinion, the deepfake porn video of the complainant made by the defendant can therefore be regarded as an image of a sexual nature of a person. The text placed on the video by the defendant stating that it is a deepfake does not change this. In addition, the court takes into account that the criminality of the conduct lies in the production of the sexual images themselves.

Even if the suspect had left the deepfake porn video on his own computer, this would still have constituted a criminal offense as referred to in Article 139h(1)(a) of the Dutch Criminal Code. In that sense, it does not matter whether or not the video states that it is a deepfake. The defense counsel's argument on that point is therefore unsuccessful.

Fact 2

With regard to the charge under 2, it must be assessed whether the suspect made public an image of a sexual nature, knowing that such publication could be detrimental to that person.

An image of a sexual nature

As the court has considered above, this concept has the same meaning in the second paragraph under b of Article 139h as in the first paragraph under a of that article. Therefore, with regard to fact 2, the deepfake porn video can also be regarded as an image of a sexual nature.

Disclosure and the knowledge of the possible harm it could cause to the complainant

It is not disputed that the defendant made the deepfake pornographic video public. The defendant has denied that he knew that this disclosure could be harmful to the complainant. In his own words, he ‘did not think about it’. However, in the opinion of the court, the outward appearance of the defendant's actions proves that the defendant at least consciously accepted the considerable risk that the disclosure of the deepfake porn video would be detrimental to the complainant. Firstly, the material in question is explicitly pornographic, which means that it can reasonably be assumed that the complainant would not want to be associated with it. In addition, the defendant stated that he regretted posting the video online fairly soon after doing so, after which he attempted to remove the video and, when that failed, set a very high price for the deepfake video in order to discourage downloading. From this, the court concludes that the defendant realized that posting the deepfake video on a publicly accessible website could be detrimental to the complainant, but that he accepted this risk, at least initially.

In view of the above, the court finds that the defendant's actions mean that all elements of the charge under Article 139h of the Dutch Criminal Code can be proven.

Reasons for the sentence

The defendant is guilty of producing a deepfake pornographic video of the complainant without her consent and making it public, while knowing that this could be detrimental to the complainant. These are serious criminal offenses. The psychological consequences for victims of whom a deepfake pornographic video has been made and made public without their consent can be serious and long-lasting. Feelings of shame, powerlessness, and insecurity often prevail. A factor in this is that once material has been distributed on the internet, it often cannot be (completely) removed and destroyed, so that victims can continue to be confronted with it for a long time after publication and through various (social media) channels. This seriously compromises the (online) safety of victims and violates their sexual autonomy, identity, and (sexual) privacy. The video made by the defendant is shocking and distasteful. The defense also acknowledges this at the hearing. The defendant became familiar with deepfake porn videos and wondered if he could make them too. He then studied the process and set to work making such videos. The video of the complainant is just one of many he has made.

Because, in his own words, he wanted to know “what others thought of it,” the defendant also posted the video online. In doing so, he paid little attention to the consequences this could have for the complainant. The court holds this against him. Given the seriousness of the facts, this should in principle be responded to with a substantial unconditional sentence.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

There are no plans to amend the legislation: for now, the application appears to fall within the existing scopes.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

No, at this moment in time it is also not seen as aggravating.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

Not at this moment.

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

We do not plan legal reforms concerning the protection of copyright in connection with AI. The European AI Act and the Dutch Copyright Act provide sufficient safeguards to protect the rights of creators and ensure fair compensation when their work is used. Our priority is implementing and monitoring the current legal framework.

5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

There are no considerations for new legislation.

6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

No

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?

(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

Using AI to commit an offence is, as mentioned before, not relevant. Depending on the offence itself, it would fall under the scope of existing legislation.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

No, this should fall under the scope of existing legislation.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

At this stage, no position has been taken on that.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

We would await the outcomes of the AI Act and CAI in order to assess whether supplementary instruments are required.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

□ **definitions**

□ **procedural provisions,**

☐ **jurisdiction provisions**

☐ **extradition and mutual assistance issues**

☐ **problems with digital evidence**

☐ **collaboration of digital AI platforms with criminal prosecutions**

☐ **other issues**

At this stage, no position has been taken on that.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

By aligning definitions with the AI Act and CAI, CETS No. 225, the new legal instrument would benefit from legal certainty and clarity, making enforcement more straightforward and reducing confusion among stakeholders. Moreover, using established definitions could help streamline compatibility within existing regulatory frameworks.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

At this stage, no position has been taken on that.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

A global instrument could lead to alignment of definitions, which would reduce ambiguity and enhance legal certainty. This could prevent the exploitation of discrepancies between national legal systems.

NORTH MACEDONIA

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?

No

If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

We are planning the adoption of a new Criminal Code aligned with the international standards. The specific solutions that will be incorporated into the new Criminal Code regarding AI will depend on prior analyses of existing international standards and comparative solutions in this field.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

See the answer under B - Q1

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

See the answer under B - Q1

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

See the answer under B - Q1

5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

Yes, we have already prepared a draft version of a new criminal offense (Deepfake) and we plan for this offense to be part of the first set of upcoming amendments and additions to the Criminal Code that will be adopted by the Parliament.

6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

There is still no analysis for this in our country.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)
Yes

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

Yes

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

Yes

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

Yes

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

✓ definitions

✓ procedural provisions,

✓ jurisdiction provisions

☐ extradition and mutual assistance issues

✓ problems with digital evidence

✓ collaboration of digital AI platforms with criminal prosecutions

✓ other issues (criminal offences).

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

We do not have adopted AI Law.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

Criminal offences, digital evidence and collaboration of digital AI platforms with criminal prosecutions.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

The existence of a single global instrument will enable the unification of criminal offenses in this area and facilitate international cooperation.

NORWAY

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Overall, neither the Norwegian Penal Code of 20 May 2005 No. 28 nor provisions on criminal liability in other parts of the Norwegian legislation specifically address criminal liability or crimes connected to artificial intelligence ('AI'). In general, the Penal Code is technology-neutral, regardless of the means used to prepare and commit a criminal offence.
In other words, the general rules of the Penal Code on culpability, negligence, contribution, attempt etc., as well as the criminal offences, will generally apply where crimes are committed, facilitated, enhanced or aided by AI.
An exception to the above is the Act 15 December 2017 No. 112 on Testing Self-Driving Vehicles, which is only available in Norwegian. The act provides more specific rules for the testing of self-driving vehicles in Norway, including a provision concerning criminal liability, see Section 18 of the Act (see more under question C3).
Lastly, there is no case law from the Norwegian Supreme Court which specifically addresses criminal liability or crimes connected to AI. However, there are a few judgments from the lower courts, which will be elaborated upon in the answer to question A6 below.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

See above.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

Section 77 of the Penal Code contains a non-exhaustive list of aggravating circumstances. Like the Penal Code in general, this provision is technology-neutral, and contains no specific rules concerning the use of AI systems. Whether the use of AI systems will be considered an aggravating circumstance must be considered on a case-by-case basis. To the best of our knowledge, there is no case law establishing the use of AI systems as an aggravating circumstance.
However, we would like to mention two judgements from Oslo District Court from 2025 concerning AI-generated depictions of sexual abuse of children or depictions that sexualises children, see the answer to question A6 below.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

See the answer to question A1 above.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:

- **sexual deepfakes**
- **online sexual grooming**
- **electoral processes**
- **use of autonomous drones to kill someone**
- **fraud of notorious importance**
- **other:**

See above under question A3.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

At this moment, there is no Supreme Court case law involving crimes committed or facilitated by AI. Although we do not have a complete overview of all case law from the lower courts, we are aware of some examples of cases concerning Section 311 of the Penal Code, which covers the production, possession, acquisition etc. of depictions of sexual abuse of children or depictions which sexualises children:

- Judgement of Frostating Court of Appeal 14.01.2025 (LF-2024-187871): The case concerned an appeal against the sentencing for violations of provisions in the Penal Code regarding sexual assault (rape) on a child under 14 years of age and depiction of sexual abuse of children or depiction which sexualises children. The defendant had, in addition to other crimes, used AI to produce depictions that sexualised two actual children, and had later kept these depictions. When reviewing the sentencing, the Court of Appeal focused on the most serious offence, which in this case was sexual assault of a minor under the age of 14 years. The court made no comment on the production and keeping of AI-generated depictions of sexual abuse of children.
- Judgement of Oslo District Court 15.05.2025 (25-075638ENE-TOSL/01): The case concerned production and possession of depictions of sexual abuse of children and depictions that sexualise children. The defendant gave a full confession, and the case was handled as a single judge confession trial. Most of the depictions were generated using AI, and the court decided on a lower sentence than the prosecution authority had proposed, and held that, even though producing child sexual abuse material is more culpable than downloading it online, producing fictional material is not equal to producing real material, as the production of fictional material involves no direct victims.
- Judgement of Oslo District Court 04.06.2025 (25-060140ENE-TOSL/01): The case concerned acquisition and possession of AI-generated pictures depicting sexual abuse of children or sexualising children. The defendant gave a full confession, and the case was handled as a single judge confession trial. In the sentencing assessment, the court agreed with the prosecution authority that possession of fictional pictures shall be punished somewhat more leniently than pictures of real children and real abuse. The court also agreed that representations that appear to depict actual abuse of children shall be punished more severely than clearly fictional representations, which is in line with Supreme Court jurisprudence concerning the sentencing for possessing fictional child sexual abuse material, cf. HR-2018-2315-A. The court also agreed that when using artificial generative intelligence, weight should be afforded to the fact that the algorithms used to produce such material must necessarily have been trained on real children and actual abuse, and that depending on the size of the dataset and the nature of the input provided, the use of such tools may result in outputs that closely resemble real children and actual abuse.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

In its government platform, the current Norwegian government has promised, more generally, to strengthen the capacity to combat cybercrime, including online abuse. However, no specific legal

reforms are planned with respect to criminal liability and AI. Even so, it cannot be ruled out that a need for legal reform may arise in the future.
Norway has, however, signed the second additional protocol to the Budapest Convention on Cybercrime, and is considering signing the UN Convention against Cybercrime. Moreover, for the sake of completeness, it should also be mentioned that Regulation (EU) 2024/1689 (the 'AI Act') encompasses rules on penalties, for instance in the event of non-compliance with the prohibition of specific AI practices that are referred to in Article 5 of the Act. The AI Act is currently being incorporated into Norwegian law.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

See the answer to question B1.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

Norway has signed the Council of Europe Framework Convention on AI and Human Rights, Democracy and the Rule of Law (CETS No. 225, 'CAI'), and is currently in the process of implementing the EU AI Act. The approach of the AI Act, based on risk-assessment and transparency, is a different measure to protect rights put at risk by the use of AI systems than adopting new criminal provisions. Apart from this, Norway has currently not identified a need for other measures. In its recent strategy on digitalisation, the Norwegian government expressed that it will assess the need to develop sector-specific regulation once the use of AI is more widespread. In that same strategy, the government also stated that Norway should assume an active role internationally in affecting the development of new legal rules on AI, particularly with respect to rules aiming to ensure ethical and safe use of AI.
With respect to the protection of copyright, Norway is in the process of implementing the directive (EU) 2019/790 on copyright and related rights in the digital single marked the provisions on text- and datamining in the near future. Other than that, there are no legal reforms concerning the protection of copyright in connection with the use of AI planed at this time.

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

There is currently no planned or ongoing legal reform concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes. Even so, the AI Act and Regulation (EU) 2022/2065 (Digital Services Act) might both contain different types of provisions that apply to deepfakes. Norway is currently in the process of incorporating both regulations into domestic law.
Production of deepfakes is, however, already covered by different general legal provisions. For instance, The Norwegian Copyright Act has a provision regulating the right to one's own image. The Penal Code has a provision regarding child sexual abuse material which covers both depictions of sexual abuse of children and depictions, which sexualises children. In the preparatory works, the legislator has stressed that the provision also covers depictions that are animated, manipulated, or otherwise artificially created. Moreover, some deepfakes that depict a natural person might be subject to the obligations under Regulation (EU) 2016/679, which is incorporated into Norwegian law.

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should

be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

Currently, Norway has not identified any other behaviours or activities involving AI that requires criminalisation, but it cannot be ruled out that a need for legal reform may arise in the future.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI? (This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

Initially, we would like to point out that it is not entirely clear to us how the wording 'a new type of offences' should be understood. That being said, Norway has not identified a need for new criminal provisions regarding dark AI, as defined above. As mentioned earlier, the provisions in the Penal Code are formulated in a technology-neutral way, meaning that they should, as a starting point, cover criminal offences where the offence has been committed by means of dark AI. However, it cannot be ruled out that a need for new provisions pertaining to dark AI might arise in the future.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

As mentioned above, it is not clear to us how the wording 'a new type of offences' should be understood. Whether violations of possible new provisions prohibiting production, placing on the market etc. of specific AI-systems should be criminalized or be subject to other types of penalties or responses, depends on the circumstances. In Norway criminal punishment is considered to be the society's strictest response to illegal acts. As a general rule, we find that there is no reason to resort to criminal punishment if sufficient compliance can be achieved through other sanctions or responses.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

Norway has currently not adopted specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems, and has not yet identified a need for such measures.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

At this time, Norway has not identified a need for the development of an international instrument on AI and Crimes. Norway has signed the CAI, and is currently in the process of implementing the AI Act from the EU. Norway has also signed the second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), and is considering signing the UN Convention 24 December 2024 against Cybercrime.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

- **Definitions**
- **procedural provisions,**
- **jurisdiction provisions**

- **extradition and mutual assistance issues**
- **problems with digital evidence**
- **collaboration of digital AI platforms with criminal prosecutions**
- **other issues**

As Norway has not yet identified the need for a new instrument on AI and crimes, we are not currently in a position to discuss the details of a prospective new instrument.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

See the answer to question D1.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

See the answer to question D1.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

See the answer to question D1.

SERBIA

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

No, the national criminal legislation of the Republic of Serbia does not currently contain provisions that explicitly address criminal liability or criminal offenses connected to artificial intelligence (AI). Similarly, there is no case law that establishes such liability.

However, under general criminal law principles, criminal responsibility may be attributed to natural or legal persons if the commission of a crime involves the use of AI systems. The Criminal Code provides for liability based on intent and negligence, depending on the nature of the offense. In such cases, responsibility would typically be attributed to a natural person (e.g., operator, programmer, user) or a legal entity in accordance with the Law on Liability of Legal Entities for Criminal Offenses.
Accordingly, general rules on criminal liability will apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

In the legal system of the Republic of Serbia, when AI systems are used as tools in the intentional commission of criminal offenses, general rules of criminal law apply. In such cases, criminal responsibility is attributed to the natural person who uses the AI system as an instrument to commit the offense, whether as a direct perpetrator, co-perpetrator, or instigator.
Article 112 of the Criminal Code of the Republic of Serbia (Definitions) provides that, for the purposes of this Code, paragraph (19) defines a computer program as a regulated set of instructions designed to control the operation of a computer and to solve a specific task by means of a computer.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

The use of AI systems is not expressly listed as an aggravating circumstance under Serbian law. However, the method of committing the offence, including the use of sophisticated or automated tools, may be taken into account by the court when determining the type and severity of the sentence pursuant to Article 54 of the Criminal Code.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

AI technologies are not explicitly regulated under Serbian criminal law. However, existing criminal provisions may apply depending on the context and method of execution. AI-based tools, including

deepfakes, autonomous systems, or synthetic media, may constitute means of perpetrating an offence, even though they are not separately addressed in the legislation. Examples include:

- Sexual deepfakes or online grooming of minors:
  - Article 185 – Showing, Procuring and Possessing Pornographic Material and Exploiting a Minor for Pornography
  - Article 185a – Inducing a Child to Attend Sexual Acts
  - Article 185b – Abuse of Computer Networks or other Technical Means of Communication for Committing Criminal Offences against Sexual Freedom of the Minor
  - Article 208 – Fraud
  - Article 301 – Computer fraud
  - Article 146 – Unlawful collection of personal data
- Use of autonomous drones to cause harm:
  - Article 113 and 114 – (Aggravated) murder
  - Article 278 – Causing general danger (e.g. by explosion, toxic materials, or other dangerous means)

While AI is not specifically regulated, these provisions may apply where AI technologies are used as tools for committing offences.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:

☒ sexual deepfakes

☒ online sexual grooming

☒ electoral processes

☒ use of autonomous drones to kill someone

☒ fraud of notorious importance

☐ other:

While not explicitly aggravating, AI use may increase the danger or complexity of the offense and be considered by courts accordingly.

5. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

As of today, there are no publicly available court decisions or criminal investigations in Serbia that explicitly concern crimes committed or facilitated by artificial intelligence systems. Nevertheless, AI-generated content—particularly deepfake recordings and manipulated videos or audio—has become a subject of increasing concern in academic discussions and public debate. Serbian legal scholars have underlined the potential misuse of deepfake technology for offences such as fraud, blackmail, or non-consensual dissemination of sexually explicit material.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

Yes. In 2025, the Ministry of Justice of the Republic of Serbia prepared a Draft Criminal Code introducing a new Article 145a, which criminalises the distribution, fabrication or manipulation of sexually explicit recordings, images or audio involving a person without their consent. Importantly, paragraph 2 of this provision explicitly covers situations where such content is created or altered by means of a computer system.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

The same initiative under Article 145a of the Draft Criminal Code addresses aggravating circumstances. In particular, it prescribes harsher penalties when the offence is committed using ICT or other technological means, when the material becomes available to a wider audience, or when the victim is a child. This demonstrates the legislator's recognition that AI and digital tools can significantly increase the harmful impact of such conduct.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

At this stage, no specific non-criminal legal or policy measures have been formally announced by the legislator to address rights at risk due to the use of AI systems. However, the topic is being followed within broader discussions on digital policy, data protection, and the ethical use of AI, particularly in the context of alignment with EU legal frameworks.

Regarding copyright, no draft legislation has been published or officially proposed that specifically addresses AI-related practices such as web scraping, data harvesting, or the use of protected content to train large language models. Nevertheless, the issue is gaining attention among regulatory and academic communities in Serbia, and may be considered in future amendments to the Law on Copyright and Related Rights, especially as Serbia continues its EU accession process and approximation to the EU Digital Services and AI regulatory frameworks.

5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

Please refer to the response provided under question 1, as the same legislative initiative (Article 145a of the Draft Criminal Code) is directly aimed at this type of conduct, particularly in paragraph 2.

6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

At present, there are no formal legislative initiatives or publicly announced plans to criminalise additional behaviours involving artificial intelligence beyond those already covered in the Draft Criminal Code (Article 145a). However, relevant authorities continue to monitor developments related to the use of AI in areas such as biometric surveillance, large-scale manipulation of public opinion, and automated dissemination of disinformation, particularly during electoral processes. These topics remain under consideration within expert and inter-ministerial discussions and could be addressed through future legal or policy measures depending on the evolving risk landscape.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

The potential for maliciously engineered AI systems to be used in cyberattacks or to endanger critical infrastructure and public safety is acknowledged. These concerns are being addressed within the framework of the national Draft Programme for Combating High-Tech Crime (2025–2030), which reflects Serbia's commitment to international cooperation under the Budapest Convention and its Second Additional Protocol.
While the issue of "dark AI" merits further legal and technical analysis, any potential response would be carefully considered within the existing structure of substantive criminal law, rather than through the immediate introduction of new standalone offences.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?
At present, Serbian criminal legislation does not contain a dedicated offence covering the placement or distribution of prohibited AI systems. The question of whether a new offence is required in this regard would be subject to expert review, taking into account the nature of the conduct, the degree of risk involved, and the extent to which such behaviour could already be prosecuted under general criminal law provisions, such as those concerning unauthorised possession or misuse of tools intended for criminal activity.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

The "negligence dilemma" resulting from autonomous actions of AI systems raises complex questions in both legal theory and practice. Serbian law currently bases criminal liability on individual culpability, with no specific framework for non-human autonomous agents. While no immediate reform is planned, the issue may warrant further academic, expert and inter-ministerial dialogue, particularly with regard to indirect liability, duty of care, and control over risk-generating technologies.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

Serbia supports ongoing international dialogue on the impact of AI on crime and criminal justice. As a party to the Budapest Convention and its Second Additional Protocol, Serbia recognises the importance of building on existing instruments. Any potential new international instrument would need to demonstrate clear added value and complementarity with existing frameworks, and its scope and content should be carefully evaluated before formulating a national position.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
☒ definitions
☒ procedural provisions,
☒ jurisdiction provisions
☒ extradition and mutual assistance issues
☒ problems with digital evidence
☒ collaboration of digital AI platforms with criminal prosecutions
☐ other issues

In the event that a new international instrument on AI and crime is developed, it should be approached with caution and built on existing legal frameworks, particularly the Budapest Convention and its additional protocols.
Such an instrument could serve a complementary and clarifying role, particularly in terms of:

- definitions relevant to the use or misuse of AI in the context of criminal conduct,
- procedural issues arising in the context of AI-generated or AI-related evidence,
- jurisdictional questions where AI systems operate transnationally,
- and potential challenges related to digital evidence and the cooperation of private sector AI platforms in criminal proceedings.

The question of extradition and mutual legal assistance may also require further analysis, particularly in relation to the attribution of responsibility and dual criminality principles in AI-facilitated crimes.

Any such instrument should be carefully scoped and designed to avoid duplication and preserve the integrity of the general principles of substantive and procedural criminal law.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

Definitions play a crucial role in ensuring legal clarity and effective international cooperation. In principle, alignment with the definitions set out in the EU AI Act could contribute to legal consistency, particularly for countries that are in the process of harmonising their legislation with the EU acquis.

However, any prospective international instrument should retain sufficient flexibility to accommodate the diverse legal systems of Council of Europe member States, including non-EU members. Definitions should be tailored to the specific context of criminal law and law enforcement, which may differ from those used in regulatory instruments such as the AI Act.

Accordingly, while alignment with the AI Act may serve as a useful starting point, the final definitions should be subject to careful legal review and adapted as necessary to reflect the objectives and scope of a criminal law convention.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

Procedural challenges related to digital evidence, including the authenticity, chain of custody, and admissibility of AI-generated or AI-manipulated content, which are highly relevant for fair trial guarantees and effective prosecution.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

A single global instrument on AI and criminal law could offer the advantage of uniform standards, enhanced legal certainty, and more effective international cooperation. It could help close jurisdictional gaps and ensure coordinated responses to transnational challenges arising from the malicious use of AI.

However, such an instrument would also face significant challenges, including divergent legal traditions, varying levels of technological development, and differences in national criminal justice systems. A one-size-fits-all approach could risk creating overly broad or rigid provisions that are difficult to implement in practice.

SLOVAKIA

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?

No, Slovak law and case law currently do not provide any specific regulation regarding criminal liability in relation to artificial intelligence (AI). AI is not recognised as a legal subject, but rather as a tool or instrument created and operated by humans. Liability always lies with a natural or legal person.

In the case of natural persons, liability requires fault (either intent or negligence). If a natural person uses an artificial intelligence system as a tool to commit a criminal offence, liability is derived solely from their conduct.

For legal persons, Act No. 91/2016 Coll. on the Criminal Liability of Legal Persons applies. This Act provides that a legal person is liable if a criminal offence was committed for its benefit or on its behalf by persons specified in the Act (e.g. statutory representatives, senior employees, or authorised agents).

At the EU level, the first comprehensive legal framework is the Artificial Intelligence Act (Regulation (EU) 2024/1689), adopted in June 2024, which entered into force on 1 August 2024, with full application from 2 August 2026 (certain provisions taking effect earlier in 2025 and 2027). As an EU regulation, it is directly applicable and takes precedence over national law.

Under Slovak criminal law, liability for offences involving AI is assessed under the general provisions of the Criminal Code. Conduct involving AI may fall particularly under cybercrime offences (Sections 247, 247a–247d CC), but also under other provisions depending on the object of the attack, such as extortion (§189), violation of rights (§376), stalking (§360a), spreading alarming messages (§361), or copyright infringement (§283).

AI cannot be held criminally liable under Slovak law. Responsibility always rests with the human (either a natural or legal person) who develops, deploys, or uses the AI system. The AI Act (EU) 2024/1689 will provide the first binding framework at the EU level, but national criminal law will continue to apply existing provisions, treating AI as a means of committing a crime rather than as its perpetrator.

If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

Given the answer to the first question, there are no general rules. However, the general principles of criminal liability fully apply. This means that responsibility is always attributed to a natural or legal person who intentionally or negligently uses AI as an instrument to commit a crime.

In practice, the key criterion is the subjective element of the offence (mens rea). Courts would assess whether the human actor acted with direct intent, indirect intent, or negligence when employing AI as a tool (for example, in cases of murder, manslaughter, theft, or other crimes). Thus, even where AI plays a decisive role in the execution of the offence, liability is attributed to the individual who operated, programmed, or deployed the system.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

Section 37 of the Criminal Code only provides a demonstrative list of aggravating circumstances for the perpetrator of a crime.

While the law explicitly mentions only certain circumstances, courts may also take into account other factors that justify a harsher penalty. The use of an AI system in the commission of a crime is not explicitly listed, but it does not prevent the court from considering it as an aggravating circumstance.

In practice, this means that if an AI system is employed in planning or carrying out a crime in a way that increases its seriousness or harmfulness, the court may reflect this in sentencing. The assessment depends on the specific circumstances of the offence, the degree of intent or negligence of the offender, and the role the AI system played. This interpretation follows from the open character of Section 37, which allows courts to flexibly take into account new or specific circumstances not expressly mentioned in the law but relevant to the gravity of the crime.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

No, Slovak criminal law, including Act No. 300/2005 Coll. (the Criminal Code) and Act No. 91/2016 Coll. on the Criminal Liability of Legal Persons, does not contain provisions specifically regulating AI technologies such as deepfakes, autonomous drones, or AI-enabled online fraud. Liability is always attributed to the individual who commits the offence or uses the AI system, not to the technology itself, in accordance with the general principles of criminal law.

A deepfake is defined as image, audio, or video content created or manipulated by AI to resemble existing persons, objects, places, or events in a way that falsely appears authentic. The Prosecutor's Office of the Slovak Republic has identified high-risk uses of AI, including the creation and dissemination of deepfake content for purposes such as extortion, defamation, manipulation of public opinion, or falsification of evidence. It has also flagged the use of AI for real-time remote biometric identification in public spaces outside a clearly defined legal framework—except in cases involving serious crimes listed in Annex II of the AI Act, such as terrorism, human trafficking, child sexual exploitation, murder, abduction, rape, trafficking in nuclear material, or participation in a criminal organisation.

The current lack of forensic experts specialised in AI, particularly in the fields of electrical engineering and criminalistics, complicates the assessment of the reliability of AI-generated evidence. Expert opinions remain essential for evaluating the admissibility of deepfake content or biometric data in criminal proceedings.

The Prosecutor's Office emphasises the necessity of human oversight over AI systems to ensure proper interpretation of AI outputs, moral reasoning, and the protection of fundamental rights. The future use of AI in criminal proceedings should be limited to supportive tools, with all decisions ultimately reflecting human judgment and autonomy.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:

☐ sexual deepfakes

☐ online sexual grooming

☐ electoral processes

☐ use of autonomous drones to kill someone

☐ fraud of notorious importance

☐ other:

With reference to the answer to the third question, the assessment always depends on the specific circumstances of the offence, the intent or negligence of the perpetrator, and the role played by the AI system in the commission of the crime. This approach enables courts to flexibly

consider emerging technologies and novel forms of criminal conduct that are not explicitly mentioned in the law but are relevant to the seriousness of the offence.

Although the use of AI systems is not expressly listed as an aggravating circumstance under Slovak law, the demonstrative nature of Section 37 of the Criminal Code allows courts to take such factors into account when determining a harsher sentence. Depending on the specific circumstances, this may include cases involving sexual deepfakes, online grooming, election-related offences, the use of autonomous drones to commit homicide, large-scale fraud, or other AI-assisted criminal acts.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

Currently, there are no recorded cases of crimes directly committed or facilitated by AI systems in Slovakia.

However, case law establishes boundaries and legal frameworks for the use of technologies that may affect fundamental rights and freedoms. Relevant jurisprudence includes S. and Marper v. the United Kingdom (2008) and Podchasov v. Russia (2024), both of which underscore that the collection and retention of biometric or genetic data must be balanced against the right to privacy under Article 8 of the European Convention on Human Rights (ECHR). In Gaughran (2020), the European Court of Human Rights emphasized that the use of facial recognition technologies requires a careful assessment of necessity and proportionality.

The Constitutional Court of the Slovak Republic (PL. ÚS 25/2019) has stressed the importance of transparency, individual safeguards, and collective oversight in automated decision-making processes. Similarly, the Court of Justice of the European Union (CJEU) in C-80/23 (2024) highlighted the need to prove the absolute necessity of collecting biometric and genetic data.

Based on prosecutorial practice, several potential high-risk uses of AI technologies warrant close attention. These include:

the creation and dissemination of deepfake content (e.g. for extortion, defamation, manipulation of public opinion, or falsification of evidence);

real-time remote biometric identification in public spaces conducted outside a clearly defined legal framework;

the use of autonomous drones or robotic systems that cause physical harm or death;

the use of generative AI to manipulate evidence or spread disinformation.

The lack of AI-specialized forensic experts continues to complicate the assessment of the reliability of such evidence. As a result, expert opinions remain crucial in criminal proceedings involving AI-generated content or biometric data.

The prosecutors in Slovakia consistently emphasizes the necessity of human oversight over AI systems to ensure correct interpretation of AI-generated outputs, appropriate moral judgment, and the effective protection of fundamental rights. The future use of AI in criminal proceedings should remain limited to supportive tools, with all final decisions resting entirely on human judgment and autonomy.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

As part of the Legislative Tasks Plan of the Government of the Slovak Republic for 2025, the following task is included:

Proposal of a law regulating institutional conditions, the competence of authorities, and the rights and obligations of entities in connection with the use of artificial intelligence systems.

Responsible institutions:

Ministry of Investment, Regional Development and Informatization of the Slovak Republic

Office for Personal Data Protection of the Slovak Republic

The objective of the proposed legislation is to implement certain provisions of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (the Artificial Intelligence Act) (OJ EU L, 2024/1689, 12.7.2024).

The need for implementation applies only to certain parts of the Regulation—primarily the designation of competent national authorities responsible for the enforcement of Regulation (EU) 2024/1689 and the introduction of penalties for its violations.

Regulation (EU) 2024/1689 will apply in its entirety from 2 August 2026, with some provisions becoming applicable earlier—on 2 February 2025, 2 August 2025, and 2 August 2027. For provisions effective as of 2 August 2025, it is necessary at the national level to introduce legislation ensuring institutional preparedness, in particular the designation of competent authorities [notification bodies, conformity assessment bodies, and supervisory authorities – see Chapter I, Articles 28 and 29, and Chapter VII]. It is also necessary to implement the penalties (Chapter VII and Chapter XII).

In June 2025, the Office for Personal Data Protection of the Slovak Republic submitted two draft legal texts for interministerial review. The review process is currently ongoing. The materials are available at the following links:

LP/2025/305 – Draft Act on Ensuring the Protection of Natural Persons in the Processing of Personal Data and on Amendments and Supplements to Certain Acts

LP/2025/306 – Draft Act on the Protection of Natural Persons in the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection, or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data.

As part of LP/2025/305, a new criminal offence is also proposed:

Section 378

Violation of Personality Rights through Digital Forgery

(1) Whoever violates another person’s right to personality protection by unlawfully providing, publishing, or making available to a third party media content created or modified using computer software that gives the impression of a faithful representation of that person’s personal characteristics and thereby causes serious harm to that person’s rights shall be punished by imprisonment of up to two years.

(2) The offender shall be punished by imprisonment of six months to three years if the act under paragraph 1 is committed:

a) publicly,

b) against a protected person,

c) causing substantial harm,

d) with the intent to gain substantial benefit for oneself or another, or

e) in a particularly serious manner.

(3) The offender shall be punished by imprisonment of six months to five years if the act under paragraph 1 is committed:

a) causing damage of a large extent, or

b) with the intent to gain benefit of a large extent for oneself or another.

(4) The act under paragraph 1 shall not be considered a criminal offence if committed for the purpose of scientific, research, educational, or artistic activity, reporting on current or historical events, or for other similar purposes, provided that the media content clearly indicates that it was created for such purposes

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

N/A

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

Slovakia currently addresses the protection of fundamental rights and freedoms affected by the use of AI systems primarily through ethical, regulatory, and institutional measures, rather than through amendments to criminal law. A key reference is the European Parliament resolution of 3 May 2022, which emphasizes that the use of AI by law enforcement authorities must respect fundamental rights, be subject to democratic oversight, and ensure transparency, human supervision, and high standards of information security.
To implement this framework, Slovakia established the Standing Commission for Ethics and Regulation of Artificial Intelligence (CERAI) at the Ministry of Investments, Regional Development and Informatization. CERAI is an independent advisory body composed of experts from academia, public administration, and the private sector. It provides guidance on the ethical, social, and legal aspects of AI, supports the responsible deployment of AI in public administration, and develops methodological materials for education and research.
In addition, the government created the role of Government Plenipotentiary for Artificial Intelligence, tasked with coordinating regulatory and ethical aspects of AI to indirectly safeguard individual rights. AI policy is integrated into the Slovak Digital Transformation Strategy 2030, which promotes the concept of digital humanism, striking a balance between technological advancement and the protection of human dignity, rights, and freedoms.
Professional practice confirms that AI can assist in routine legal tasks; however, its use must not compromise the core functions of the justice system or infringe upon fundamental rights, including data protection, information security, and the confidentiality of lawyer-client communications. Academic and professional platforms, such as AIslovakIA and the Center for Artificial Intelligence (CUI), also play a key role in promoting ethical standards and the development of professional expertise.
Slovakia addresses AI-related risks primarily through soft regulatory instruments, ethical frameworks, methodological guidance, and institutional coordination. This approach allows for flexible adaptation to technological developments while maintaining an appropriate balance between innovation and the protection of fundamental rights.

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?
5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?
6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

Based on the current legal framework and prosecutorial practice, Slovak authorities have identified certain AI-related behaviours that may warrant future criminalisation. While the AI Act provides a comprehensive EU-level legal framework for the use of artificial intelligence, including within law enforcement, national legislation currently lacks detailed provisions for the practical application of AI in criminal proceedings—particularly in the areas of evidence collection and evaluation, technical and organisational infrastructure, and the availability of expert capacity.

AI-related conduct considered to present high-risk includes:

the creation and dissemination of deepfake content for the purposes of extortion, defamation, manipulation of public opinion, or falsification of evidence;

the unlawful use of real-time remote biometric identification outside a clearly defined legal framework; and

the use of generative AI to manipulate or fabricate evidence, which poses serious threats to the integrity of the justice system, the reliability of evidence, and legal certainty.

Slovakia currently lacks forensic experts specialising in AI, which complicates the evaluation of digital evidence in criminal cases. The explicit criminalisation of selected AI-related behaviours could have a preventive effect, provide greater legal clarity, and reinforce the requirement of human oversight to safeguard fundamental rights, fairness, and equality before the law.

The future use of AI in criminal proceedings must remain strictly supportive and auxiliary. All legal decisions should continue to be the result of human judgment and an expression of human autonomy, underpinned by ethical standards, transparency, and targeted professional training for judicial and prosecutorial authorities.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

There is a growing need to consider the introduction of a new criminal offence targeting so-called “dark AI”—AI systems specifically developed for malicious or harmful purposes, such as hacking, cyberattacks, endangering critical infrastructure, generating deepfake content for criminal use, or assisting in the commission of serious crimes.

Current Slovak legislation does not address such conduct as a separate offence. AI continues to be regarded solely as a tool, with criminal liability attributed to the natural or legal person deploying or using the system.

However, practical experience indicates that the misuse of AI for harmful purposes poses significant risks to public safety, the administration of justice, and the protection of fundamental rights. The introduction of a dedicated criminal offence could establish clear liability for the development, distribution, or deployment of AI systems intentionally designed to facilitate serious criminal activity. This would complement the existing Penal Code, which is currently focused exclusively on human perpetrators.

Such regulation should be tightly integrated with broader AI governance, ensuring alignment with the principles of trustworthiness, ethical use, and transparency. It must also preserve the requirement for human oversight as a fundamental safeguard in criminal law decision-making.

This approach would strengthen preventive mechanisms, reduce the potential for the malicious use of AI, and enhance the protection of public safety and the public interest.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

N/A

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

In the context of a proposed international convention on artificial intelligence and criminal offences, it is essential to first establish solid foundations in substantive criminal law before any meaningful harmonisation of procedural rules can take place. AI systems should be clearly defined and limited to supportive tools for law enforcement purposes, with all legal decisions remaining strictly under human authority. This is necessary to uphold fundamental guarantees such as fair trial rights, legal certainty, and judicial independence.

Once these substantive principles are in place, procedural rules can be meaningfully developed to govern the use of AI in criminal proceedings, for example, in the search, analysis, and evaluation of evidence. These rules should balance the potential benefits of AI, such as speed, pattern recognition, and consistency, with the associated risks, including algorithmic opacity, dependence on data quality, and ethical and human rights concerns.

The convention should also include clear provisions on digital evidence, particularly with regard to deepfake content and remote biometric data. Key safeguards should include transparency, auditability, and mandatory expert assessment of AI-generated or AI-processed evidence.

Provisions on cross-border cooperation, including rules on jurisdiction, extradition, and mutual legal assistance should logically follow once shared substantive principles have been agreed. This would facilitate effective international collaboration in criminal matters, without compromising the primacy of human decision-making in the justice process.

In summary, clarifying and harmonising substantive criminal law standards is the primary step. These foundational principles must underpin any procedural, technical, or ethical rules. Other instruments, such as those relating to electronic evidence or cross-border cooperation are necessarily secondary and should remain flexible and adaptive to ensure coherence with core legal values.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

Yes

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

If legal theory and potential global legislators were to conclude that the direct criminal liability of AI systems represents the optimal approach, the most effective solution would likely be the adoption of a dedicated international legal instrument, analogous to existing frameworks on corporate criminal liability.

Such an instrument would establish the conditions under which AI systems could be held criminally liable, including:

adapted definitions of culpability appropriate to autonomous or semi-autonomous decision-making,

a coherent framework for applicable sanctions, and

a clear enumeration of offences that AI systems could commit, either independently or in collaboration with human actors.

This kind of comprehensive legal framework would enhance legal certainty, consistency of application, and accountability, while enabling courts and law enforcement authorities to effectively balance the competing interests of public safety, protection of fundamental rights, and technological innovation.

SLOVENIA

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?

No. There are no specific rules on criminal liability if crimes involve artificial intelligence (hereinafter: AI). Our Criminal Code (KZ-1) also does not encompass any AI-specific criminal offences.

If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Yes. If crimes would be committed or facilitated by AI, general rules on criminal liability from the Criminal Code (KZ-1) and the Liability of Legal Persons for Criminal Offences Act (ZOPOKD) would apply. Namely, Slovenia's legal framework also holds legal persons criminally liable for offences committed in their name on their behalf or for their benefit.
Illegal act involving AI would be assessed under the existing catalogue of criminal offences from the Criminal Code (KZ-1).

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

As noted above, Slovenian Criminal Code (KZ-1) does not entail AI – specific criminal offences nor does it have special forms of standard criminal offences (e.g. theft, murder, manslaughter) when AI is used as a tool for committing them. Only voluntary human act can be subject to criminal liability. Under the Criminal Code of Slovenia (KZ-1), individuals are held criminally liable when they commit an act that constitutes a criminal offence with guilt and there are no grounds for excluding criminal liability. This basic rule would apply also in cases when AI system is used as a tool for committing established criminal offences.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

The use of AI system is not considered as a specific aggravating circumstance in the Slovenian Criminal Code (KZ-1). However, our provision on aggravating and mitigating circumstances (below) is quite open and general, so theoretically the use of AI system could represent an aggravating circumstance, depending on the specific circumstances of the particular case and subject to judicial discretion.
Article 49, paragraph 2 of the Criminal Code (KZ-1): “In determining the sentence, the court shall consider all the circumstances that influence the grading of the sentence (mitigating and aggravating circumstances), in particular: the degree of the perpetrator's guilt; the motives for which the act was committed; the intensity of the danger or injury caused to the protected legal value; the circumstances in which the act was committed; the perpetrator's past life; his or her personal and financial circumstances; his or her conduct after committing the act, especially whether he or she provided compensation for the damage caused by the criminal offence; and other circumstances relating to the perpetrator's personality and to the expected effect of the punishment on the perpetrator’s future life in the social environment.”

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

As noted above, Slovenian Criminal Code (KZ-1) does not explicitly address the use of specific AI technologies such as deepfakes, autonomous drones, or AI-driven fraud. However, such modus operandi could fall under different criminal offences from the Criminal Code, depending on the circumstances of a particular case.
For example, Article 143(6) criminalizes public disclosure of recordings or messages with sexual content without the consent of the depicted person, if such disclosure seriously affects their privacy. Article 176 in addition addresses the production, distribution, or possession of pornographic material involving minors, including their realistic depictions, with severe penalties.
Article 173a criminalizes child grooming of a minor under 15 years of age through information and communication technologies. Depending on the specific circumstances of a case, the commission of such an offence using AI may fall within the scope of this provision.
In the Criminal Code of Slovenia (KZ-1) the criminal offences of murder (Article 116), manslaughter (Article 115) and fraud crimes (Articles 211, 228-231) are technology neutral so generally (and of course depending on the circumstances of a particular case) they would apply regardless of the specific technology used.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:

As mentioned above (see answer under question 2) the use of AI system is not considered as a specific aggravating circumstance in the Slovenian Criminal Code (KZ-1).
6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

N/A

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

Currently no such reforms are foreseen.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

Currently no such reforms are foreseen. We do not see why such amendments would be necessary. In our view the use of AI should not always and automatically be considered as an aggravating circumstance but depending on the circumstances of a particular case. And in our view our legislation already provides sufficient level of flexibility when determining aggravating and mitigating circumstances.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

Slovenia is bound by the EU`s AI Act. One of its aims is to protect rights put at risk by the AI systems. We are currently making efforts for implementing this comprehensive Act.
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?
With respect to criminal law protection, no modifications to the existing offences protecting copyright are currently foreseen.

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

As above, with regards to the criminal law protection no such reforms are currently foreseen.

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

Dark AI systems can cause widespread and significant damage, often with transboundary effect. Therefore, we would encourage discussion on the possible added value of regulating the most dangerous and critical dark AI systems in a new criminal instrument. However, the deficiencies in the current approaches and the added value of such new instrument should be clearly demonstrated. We would need to have a clear picture on the state of affair in the field (e.g. what forms of dark AI systems are more often used for criminal purposes, what effects can they produce, what sort of development can we expect in the future etc.). We should also avoid overlapping with the existing legal framework, including Cybercrime Convention.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

There should be no conflict with the EU´s AI Act. The AI Act already provides sanctions for the infringement of the provisions on the prohibited AI systems. They are administrative in nature. Any deliberations on potential criminalization should take into account the proportionality (the risks of such activity, without actually using the AI system to commit a specific offence) and ultima ratio nature of criminal law.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

At the moment we are not in a position to provide a general comment. A question that arises is whether we can really adopt a uniform approach to address the negligence dilemma on the European level. We are open to discussions and to pursue this avenue if it would prove to be meritorious.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

As above under point 1. We are open to discussing this option as well as alternatives. An added value in creating a new instrument in the field of criminal law should be demonstrated.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

Premature to provide views on the possible structure of the instrument.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

We are of the view that the possible instrument as a whole should be aligned with the AI Act. There should be no divergencies as the AI Act is applicable to 27 Member States of the Council of Europe.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

Possible new instrument on AI and Crimes should in our view address basic challenges in the area of criminal law, including substantive (specific AI related criminal offences, possibly also specific general principles such as criminal responsibility for negligence), procedural aspects (e.g. safeguarding the right of defence – equality of arms, capacity to understand how evidence was obtained and analysed, efficient capacity to counter the results of investigations conducted using AI, etc., and other procedural rights when AI tools are used by law enforcement and judiciary), and judicial cooperation mechanisms specific for AI-related crimes, together with capacity building and technical assistance elements.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

Crimes related to AI are often transnational in nature. Therefore, a global instrument providing a harmonised legislative framework would be important in addressing them more effectively, especially by facilitating international cooperation. As we do not yet have any internationally legally binding instrument in the area of AI and criminal law, such a global instrument would undoubtedly establish new worldwide standards.

SWEDEN

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Swedish national legislation and Supreme Court case law does not specifically address criminal liability or crimes connected to artificial intelligence. However national legislation is often technology neutral, which means that criminal liability in many cases can be imposed when AI technology is used to commit crimes.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

Several general rules regarding criminal liability and sentencing can possibly be applied when AI systems are used as tools for the intentional commission of criminal offences.

Chapter 1 section 2 of the Swedish Criminal Code (Brottsbalken) states that unless otherwise specifically provided, an act is only considered an offence when committed intentionally. There are three forms of intent in Swedish criminal law. “Avsiktsuppsåt” (when the perpetrator actively desires the outcome to occur), “insiktsuppsåt” (when the perpetrator is fully aware of the circumstances and the outcome of his/her action) and “likgiltighetsuppsåt” (when the perpetrator is aware of a risk that his/her action might cause an outcome, but he/she is indifferent to whether that outcome is realized). “Likgiltighetsuppsåt” is considered the lowest level of intent.

Furthermore, criminal liability requires a certain degree of unacceptable risk-taking and proximate cause between the perpetrator’s action and the outcome/injury.

When it comes to sentencing the use of AI systems could possibly be considered an aggravating circumstance (see below). However, there are no rules in the Swedish sentencing system that specifically address the use of AI.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

Chapter 29, Section 1 of the Swedish Criminal Code states that, when deciding on a sentence, courts should consider the interest of uniform application of the law, that penalties are determined within the framework of the applicable scale of penalties according to the penalty value of the offence or of the combined offences. When assessing penalty value, consideration should be given to the damage, violation or danger involved in the act, what the accused realised or ought to have realised in this respect, and their intentions or motives. Particular consideration should be given to whether the act involved a serious attack on someone’s life or health or personal security. Aggravating circumstances that the courts should particularly take into consideration when assessing penalty value, are listed in Chapter 29, Section 2. The use of AI systems is not specifically addressed in that section but could possibly fall within the scoop of one of the listed provisions. For instance, whether the offence was part of criminal activities conducted in an

organised form or systematically, or whether the offence was preceded by particular planning, are some of the aggravating circumstances listed in Chapter 29, Section 2.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

The crime "child pornography offence" is technology neutral. It is further described below (see question B4). The same applies to the sexual offences in the Swedish Criminal Code, even though it is not possible to commit all the different crimes with the use of AI technologies. For example, the crime "sexual molestation" includes sending a so called "dick-pic" to another person. It is not relevant whether the picture is a real picture or AI generated. It is also criminalised to, by improper means, induce a child to undertake or submit to intercourse or a similar sexual act. Under some circumstances, the induction might be implemented using AI. The crime "contact with a child for sexual purposes" (i.e. grooming) can also be committed by using, for example, a deepfake when grooming a child.

Other crimes, such as "fraud" (Chapter 9, Section 1 of the Swedish Criminal Code), "breach of data security" (Chapter 4, Section 9 c), and "improper interference with voting" (Chapter 17, Section 8) can be committed with the use of AI technologies.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:

☐ sexual deepfakes

☐ online sexual grooming

☐ electoral processes

☐ use of autonomous drones to kill someone

☐ fraud of notorious importance

☐ other:

See above (question A3).

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

In a recent case, a young man was convicted for sexual molestation for having manipulated two images of two different young women with the use of AI and then sending the pictures to one of the women. He used real photographs of the young women's faces but altered them to make the pictures look like nude pictures. (Court of Appeal for Western Sweden, case no B 2880-25, 5 May 2025.)

There are also reports on the increasing findings of AI-generated child sexual abuse material. The Swedish regulation makes no difference between real or fake pornographic images (see question B4 below).

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

In 2018 a government appointed committee published a report with constitutional proposals for the introduction of automated driving of vehicles on public roads, including proposals regarding criminal liability (SOU 2018:16). In 2021 the Swedish Government published a report regarding self-driving cars, supplementing and adjusting some of the proposals in SOU 2018:16 (Ds 2021:28)

related to self-driving cars and criminal liability. The proposals are being processed within the Swedish Government Offices.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

When a crime is committed, facilitated, enhanced, or aided by the use of AI systems these circumstances can be regarded as aggravating according to existing legislation (see above, question A3).
In July 2023 one-person inquiry was appointed by the Swedish Government with the mission to review penalty scales and reform the sentencing system. The inquiry published its final report (SOU 2025:66) in May 2025. The report includes proposals to ensure that penalties are set in a nuanced and differentiated way, with greater account taken of aggravating circumstances. The proposals are being processed within the Swedish Government Offices.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

The legislator could address the new challenges of protecting rights at risk from AI systems through measures other than adopting new criminal laws.
The AI Commission's roadmap proposes measures such as strengthening AI and cybersecurity research, improving public access to AI knowledge, and ensuring secure data governance in the public sector.
The Commission was appointed by the Swedish government in late 2023 and completed its work in November 2024. The recommendations are being analysed within the Government Offices and implementation to support a safe and rights-respecting AI development in Sweden has commenced. According to the AI Commission's roadmap, several strategic actions are proposed:
- Strengthening AI and cybersecurity research – The roadmap emphasizes the need for consolidated research efforts under a national actor, such as KTH via Cybercampus Sweden. This would enhance understanding of AI-related threats and support proactive risk mitigation.
- Improving access to knowledge and competence – Initiatives like the AI Workshop aim to equip individuals and organizations with the tools and understanding needed to navigate and protect themselves from AI-related risks.
- Establishing robust data governance in the public sector – The Commission recommends mandatory modern digital information management across public sector entities. This includes secure and interoperable data sharing that respects privacy, enabling cross-sectoral digitalization and building resilient systems that can withstand AI-driven threats.

At EU level the AI Act introduces two requirements related to copyright (Article 53(1)(c) and (d)), entering into force on 2 August 2025. The first requires general purpose AI (GPAI) providers to put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with a so called opt-out (a reservation of rights expressed by a rightsholder pursuant to Article 4(3) of Directive (EU) 2019/790). The second provision requires GPAI providers to draw up and make public a sufficiently detailed summary of the content used for training.

A government inquiry has been appointed to draft legislation enabling prosecutors to seize or otherwise secure immaterial properties, such as Internet domain names, with a view to future confiscation. (Dir. 2024:122.) Potentially, a seizure (or similar measure) of this kind could be utilized to target crimes committed with the use of AI.

A government inquiry has also been appointed to assess the need for and conditions of a prohibition on private individuals receiving IPTV provided without authorization from relevant

rightsholders and propose how such a prohibition should be designed. If necessary, the inquiry may propose additional measures to counteract the distribution. (Dir. 2025:5). Although the questions do not specifically concern AI, the proposals may cover violations carried out with the help of AI.

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

There are already several existing regulations in Swedish criminal law addressing this issue. Some examples are:

- The crime “Defamation” (Chapter 5, Section 1 of the Swedish Criminal Code) can, under certain circumstances, be applicable to the dissemination of certain sexual images, both real and manipulated. In a 1994 Supreme Court Case (NJA 1994 p. 637), an editor in chief for a Swedish newspaper was found guilty of defamation by publishing an article which included a photomontage where images of faces of Swedish celebrities had been combined with pornographic images, and speculative captions to the images.
- A person who intrudes into the private life of another person by disseminating, inter alia, an image of or information about a person’s sexual life or an image of a person’s wholly or partially naked body is, if the dissemination is liable to result in serious damage to the person whom the image or information concerns, guilty of the crime “Unlawful breach of privacy” (Chapter 4, Section 6 c of the Swedish Criminal Code). In order for the dissemination to be criminal, the material which has been disseminated should be true and correct. However, the fact that the material in question has been manipulated does not rule out criminal responsibility.
- The crime “Child pornography offence” (Chapter 16, Section 10 a of the Swedish Criminal Code) already makes no distinction between real or fake images. In other words, a deepfake or an AI-generated image depicting a fictional child would be considered child pornography material (provided that the image is considered “pornographic”). However, whether or not a real child is depicted may affect the seriousness of the crime. The crime covers inter alia depicting, dissemination and possession of child pornography material.

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

It cannot be ruled out that certain behaviour or activities involving artificial intelligence should be criminalised in the future. However, Swedish criminal law legislation is often technology neutral which means that criminal liability in many cases can be imposed when AI technology is used to commit crimes. We have not identified an immediate need for new types of criminal offences related to AI. As mentioned above, proposals regarding self-driving cars and criminal liability, are being processed within the Swedish Government Offices (see question B1).

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

Answer to question C1-4: We have not identified an immediate need for new types of criminal offences related to AI or an immediate need for a new international instrument which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems. In any case, these issues must be analysed further. If an international instrument is created, it should be a recommendation and not a binding instrument.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

Question 1-3 are raised too early. The need for definitions, procedural and jurisdiction provisions etc., depends on which specific areas of criminal law being addressed in the international instrument.
When it comes to question 4, a single global instrument addressing AI and criminal law, would likely contribute to harmonizing regulations in different counties. On the other hand, with such a broad approach it might be hard to find consensus on more concrete issues. Individual pieces of legislation (or a list of recommendations) in specific areas would probably better address concrete issues related to AI and criminal law.

SWITZERLAND

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

(1) Switzerland does not have a specific legislation that addresses criminal liability or crimes connected to artificial intelligence.
(2) Criminal responsibility is generally attributed to a natural or legal person and is based on the standards of criminal intent or negligence. Swiss criminal law is not based on the concept of strict liability.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

General criminal rules remain relevant even if AI systems are used as tools for the commission of criminal offences. The Swiss Criminal Code is generally technology neutral and remains applicable regardless of the technological methods used by the perpetrators. If, for example, the perpetrator uses deepfake technology to commit an offence against honour or privacy or to obtain a financial advantage by means of deception, the respective criminal offences are applicable.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

Switzerland does not per se consider AI systems as an aggravating circumstance. But it can be assessed within the discretion in determining the penalty according to existing laws. If AI systems or technologies are particularly sophisticated in certain constellations or if the quality of a deception increases, the perpetrators may well be found to have acted with particular malice or intent to deceive when sentencing in individual cases.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

Swiss criminal law does not address specific AI technologies for committing crimes. As stated above under question 2, Swiss criminal law is generally technology neutral. It would hence encompass crimes, in which AI technology is being used, under the traditional provisions such as fraud, sexual harassment etc.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone

☐ **fraud of notorious importance**
☐ **other:**

See answer to question 3.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

Generally, the use of AI is increasing, both regarding its use by criminals and by law enforcement and prosecution authorities.
On the offense side:
• Facilitation and baiting/phishing: AI can be used both to find victims (en masse or in a targeted manner depending on the crime, for example through social media analysis) and to improve bait (fake emails and/or web pages designed to mislead victims using LLM such as ChatGPT).
• Execution of crimes: AI is used to automate attacks, expand the circle of recipients, or improve or simply change malware codes so that they evade antivirus software.
• Yes, in Switzerland, there are cases (not in the sense of case law) in which AI plays a role. Within the scope of cantonal powers, there are - for example - cases that include deepfakes (e.g., nudify technologies among adolescents). On the federal level, the use of AI in the development of malware, such as increasingly sophisticated ransomware, is on the rise (writing or improving malware code, or the computer architecture used for attacks or to recover ransom money).
On the investigative side:
• AI is also being tested and used to develop software in the area of police and criminal prosecution: for example, in the field of child pornography, AI can be used to automate the viewing of photographs and videos in order to identify evidence, determine whether they belong to a known series or represent a new case of abuse.
• Also, in the field of evidence gathering, AI software can be used to scan the various terabytes seized from perpetrators in search of relevant material, saving valuable time.
• In addition, in the area of cyber fraud, particularly romance scams, tests are being conducted in collaboration with academia and the private sector to identify cases and manage relations with the alleged perpetrators.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

The Swiss Confederation is working to regulate AI in Switzerland. Switzerland signed the Council of Europe's AI Convention (CAI) and wants to ratify it. In this context, the responsible departments are analysing the necessary legal measures on the national level, particularly in relation to transparency, data protection, non-discrimination and supervision. Criminal liability and crimes are not a primary focus of this work. Nevertheless, the adoption of horizontal measures in this regard could also affect aspects in relation to (criminal) liability and crimes related to IA. The work is still in its early stages, and it is not yet possible to provide more concrete details on the legislative measures envisaged.
Furthermore, there were recent regulatory developments in regard to automatic driving (see 13. Dezember 2024, Bundesrat ermöglicht automatisiertes Fahren).

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

See the answer to the previous question.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

In connection with the developments mentioned above (see the answer to question B.1), civil or other laws as well as legally non-binding measures such as industry solutions and voluntary commitment declarations will also be important. Furthermore, sector-specific activities will be continued. If a need for regulation is identified in a certain legal field, such developments might be solely approached in that field or frameworks directly (e.g., in the context of civil law or law on secondary penalties (such as copyright laws) and not necessarily in the context of core criminal law).
Currently, reform efforts are being considered in the field of copyright laws as some members of Parliament raised the concern to step up intellectual property protection in the face of AI. There seems to be a general consensus in Switzerland, that copyright is relevant when AI-systems are being trained or applied and that the interplay between the creative sector and the AI sector needs clarifying rules. However, these developments are not yet at a stage where more detailed information can be provided on how and which areas would be concretely adapted.

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

General criminal law also remains relevant for the development of applications for the production, the use, or the dissemination of certain (sexual or hacking) material. The production and distribution of such applications that facilitate the production, the use or dissemination of (sexual) deepfakes may hence already constitute a violation of certain relevant criminal legal provisions, independently of whether AI is being used or not. The legislative work currently underway in connection with the ratification of the Council of Europe's AI Convention may also have an impact in relation to (criminal) liability and crimes related to AI.

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

Activities involving AI continue to be subject to political discussions. However, there are currently no specific legislative plans in regard to substantive criminal law. As mentioned above under question B.3, certain regulatory developments might continue sector-specific.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

In principle, any hacking or other cyberattack would fall under the Swiss hacking provision in Art. 143bis CrimPC if a person obtains unauthorised access by means of data transmission equipment to a data processing system that has been specially secured to prevent his access.
Furthermore, AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks would be covered by existing provisions that address the production and marketing of equipment for the unauthorised decoding of encoded services (Art. 150bis CrimPC) as well as the making accessible of passwords, programs or other data that are intended to be used to unauthorisedly access a data processing system (Art. 143bis CrimPC).

Also, the manufacturing, importing, marketing, advertising, offering or otherwise making accessible of programs for the purpose of damaging data is covered. Therefore, there does not seem to be a general legal gap in this regard.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

See answer to question 1 above. There is at least no general legal gap as to the putting into service, the production, importation, or provision to third parties of prohibited systems or programs according to national legislation.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

The general concepts of intent and negligence remain relevant for any natural or legal person using, or possibly also producing AI systems-based products.
Since an AI system is not a criminal legal entity and cannot itself be prosecuted under criminal law, the responsibility in connection with criminal damage caused by AI systems would generally lie with a person (such as the user, operator, owner, or manufacturer).
As challenges may rather arise in the assessing and locating of the responsibility in an individual case by judicial authorities, there does not necessarily seem to be a need to address the “negligence dilemma” by legislatory action.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

The Budapest Convention on Cybercrime might already cover issues on substantive criminal law such as illegal access to a computer system (under which AI systems would fall too), illegal interception or interference with data or systems, even if this is done or facilitated through AI systems. AI systems are usually also computer systems that work with data.
Also, the Budapest Convention contains procedural provisions, covers international cooperation (extradition and mutual assistance), as well as the collection of evidence that is relevant for potentially any crime.
Therefore, it would need to be critically evaluated in what concrete areas a Convention on AI and Crimes might provide an additional value to the existing international conventions that may already be relevant for certain constellations.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

If a new Council of Europe legal framework should be sought, it might make primarily sense to align it with the definitions (e.g., the definition of an AI system) of the Council of Europe AI

Convention (CAI), as another Council of Europe instrument should be consistent with its previous ones.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

Any new regulation would have to be proven necessary and carefully examined, as each of the above-mentioned areas already has a framework and clear approaches in place that, while surely affected by the challenges associated with AI, do not seem to exclude them from the scope of application per se.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

AI technologies are relevant for many different areas. A single global instrument on AI and criminal law could potentially not be specific or detailed enough to adequately regulate the concrete needs of every relevant field. Sectorial approaches might be closer at the exact issues at hand (e.g., traffic road law or medical law context). There would have to be good reasons why general principles offer added value to the general principles that already exist.
Furthermore, introducing provisions about behaviour that is already covered by existing law, could mislead to the conclusion that the behaviour in question is currently permitted or unproblematic, which in many constellations would not be the case.

TÜRKİYE

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);

Although there is no national legislation that specifically addresses the criminal liability or crimes connected to artificial intelligence, general rules of criminal liability are applicable to instances that involves artificial intelligence. Also, as per article 90 of the Constitution of the Republic of Türkiye indicates “International agreements duly put into effect have the force of law. No appeal to the Constitutional Court shall be made with regard to these agreements, on the grounds that they are unconstitutional. In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail.”
Furthermore, Law No. 5651 on the Regulation of Publications Made on the Internet and Combating Crimes Committed Through Such Publications, Turkish Penal Code No. 5237, and the Personal Data Protection Law No. 6698, along with other pertinent laws can also be taken into consideration in this context.
https://www.anayasa.gov.tr/media/7258/anayasa_eng.pdf
https://mbkaya.com/turkish-internet-law/ (unofficial translation)
https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law
https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)011-e

(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

For crimes committed, facilitated, enhanced, or aided by artificial intelligence, general criminal liability rules apply. However, the specifics of crimes may trigger the application of other special laws for example;
- Under Law No. 5651, natural or legal entities such as content providers, hosting providers, and access providers can be held legally and criminally liable for crimes committed online.
- Under Law No. 6698 on the Protection of Personal Data, natural or legal entities acting as data controllers for the processing of personal data are subject to legal and criminal liability, even for transactions conducted through automated means (e.g., artificial intelligence).
- Law No. 6698 is particularly important for its obligations of "explicit consent" and "data security." Under both laws, criminal liability is imposed on a natural person or their representative acting on behalf of a legal entity. Because an artificial intelligence system lacks legal personality, it is not yet directly criminally liable as a perpetrator.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

In our Criminal Law, the definition of artificial intelligence in relation to criminal liability was not made. However, if artificial intelligence is used as a means to commit an intentional offence, it is considered that the general rules regarding fault in Turkish Penal Code can be applied.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

Although artificial intelligence is not explicitly listed as an aggravating circumstance in our legislation; it is considered that the use of artificial intelligence could similarly be accepted as an aggravating circumstance, because the crimes committed by using information systems are considered as qualified versions (aggravating circumstances), as stipulated in the Article 158 of the Turkish Penal Code.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

While there is no specific criminal law in Türkiye directly targeting crimes committed using artificial intelligence technologies (e.g., deepfakes, autonomous drones, etc.), current legislation addresses crimes involving the use of IT systems under general provisions. Some examples are provided below:

• Turkish Penal Code Article 226 (Obscenity): The production of sexually explicit content/deepfakes targeting minors may be considered within the scope of this article.
• Turkish Penal Code Article 105: Online abuse acts may also be considered child sexual abuse.
• Turkish Penal Code Article 245: “If a device, computer program, password, or other security code is produced or created exclusively for the purpose of committing the crimes listed in this Chapter or other crimes committed through the use of information systems as a tool, the person who manufactures, imports, ships, transports, stores, accepts, sells, offers for sale, purchases, gives to others, or possesses them shall be punished with imprisonment of one to three years and a judicial fine of up to five thousand days.”
• For certain crimes, committing crimes using information systems is considered an aggravating factor. Furthermore, "Crimes in the Field of Information Technologies," regulated under Volume II, Chapter III, Part Ten of the Penal Code, can be linked to artificial intelligence.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other: …

The use of AI in cases involving sexual deep fakes, online sexual grooming, or killing someone with autonomous drones is not directly considered as an aggravating circumstance. However, as in the case of obscenity crime regulated in the Article 226 of Turkish Penal Code, the use of computer systems as a means to commit certain crimes against children is considered as an aggravating circumstance under our laws. Nevertheless, depending on the manner in which the crime was committed and whether the used artificial intelligence device is considered as a weapon, it may also be evaluated in terms of other crimes.

Besides that as per the Article 243 of the Preamble of the Turkish Penal Code, IT systems may include AI systems, and for certain crimes, committing crimes using information systems is considered an aggravating factor.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

There is no case law of the Court of Cassation directly related to this issue yet. However, some decisions rendered by the regional courts of justice addressed the use of AI in crimes. These decisions discussed whether it should be considered a qualified form of theft and fraud and whether it should be accepted as an aggravating factor.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?
2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?
3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?
Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?
4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

It is considered that such a legal framework would be beneficial.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

It is considered that such a legal framework would be beneficial. It is considered beneficial to define prohibited artificial intelligence in this regard, determine its scope and elements, and regulate its use or provision for use or sale as a criminal offence.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

It is considered that such a legal framework would be beneficial.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

- ✓ □ **definitions**
- ✓ □ **procedural provisions,**
- ✓ ☐ **jurisdiction provisions**
- ✓ ☐ **extradition and mutual assistance issues**
- ✓ ☐ **problems with digital evidence**
- ✓ ☐ **collaboration of digital AI platforms with criminal prosecutions**

☐ **other issues**

It is considered appropriate that, in addition to the elements mentioned above, the provisions relating to investigation and prosecution procedures should also be included within the content of the instrument.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

It is not possible to answer this question at this point, as the context and scope of the potential instrument is not definitive yet. Once the scope and context of the potential instrument are clarified, each definition should be discussed thoroughly. This has been the case during the process of drafting the CAI Convention. It was decided to leave the definitions to last, to first determine which terms needed a definition and to decide on the best possible definition of each term to be defined.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

Dark AI, deep fake, autonomous systems, the use of artificial intelligence platforms in the investigation and prosecution of crimes, extradition and mutual assistance issues, problems with digital evidence, collaboration of digital AI platforms with criminal prosecutions (It is understood that this question is posed for the purposes of the potential instrument on AI & criminal law.)

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

International cooperation is vital for cross-border digital crimes. Such an instrument could be helpful. It is also considered that it would be beneficial to prepare separate instruments for each sector.

UKRAINE

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?

If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal,
e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).

If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

Ukrainian national legislation does not regulate the specifics of criminal liability for crimes related to artificial intelligence (hereinafter referred to as AI).

Thus, according to Article 3 of the Criminal Code of Ukraine (hereinafter referred to as the CC of Ukraine), the legislation of Ukraine on criminal liability is constituted by the CC of Ukraine, which is based on the Constitution of Ukraine and generally recognized principles and norms of international law.
Part three of the aforementioned article also establishes that the criminal illegality of an act, as well as its punishability and other criminal law consequences, are determined solely by the CC of Ukraine. At the same time, the basis for criminal liability is the commission by a person of a socially dangerous act that constitutes a criminal offense under this Code.

According to Article 18 (Subject of a Criminal Offense) of the Criminal Code of Ukraine, the subject of a criminal offense is a sane natural person who committed a criminal offense at an age at which, according to this Code, criminal liability may arise.
The occupation, profession, or position of such a person is not decisive for the classification of a criminal offense, although, according to the content of a specific offense, they must be related to the use of electronic computers, systems, computer networks, and telecommunications networks.

Actions committed both intentionally and negligently, including in the form of criminal unlawful negligence, are punishable by criminal law. At the same time, Ukrainian criminal law does not provide for strict liability. In this context, it should be noted that civil liability for compensation for damage caused by a source of increased danger (including in the context of civil claims in criminal cases) can be considered an analogue of such an institution in Ukrainian national legislation.

A selective study of criminal cases decided by Ukrainian courts showed that artificial intelligence was used either as a means of committing a crime (judgment of the Dzerzhinsky District Court of Kharkiv dated January 29, 2025, in a case under Part 2 of Article 309 of the Criminal Code of Ukraine) or as a defense strategy for the defendant (judgment of the Dzerzhinsky District Court of Kryvyi Rih dated October 14, 2024, in the case under parts one and two of Article 111, part one of Article 263 of the Criminal Code of Ukraine), and was also mentioned in the context of the potential generation of the subject of the crime by artificial intelligence (judgment of the Pervomaisky City District Court of Mykolaiv Region dated March 12, 2025, in the case under part one of Article 301-1 of the Criminal Code of Ukraine) or evidence in the case (judgment of the Kherson City Court of Kherson Region dated June 17, 2025, in the case under part five of Article 111-1 of the Criminal Code of Ukraine).

In addition, Section XIV-1 of the Criminal Code of Ukraine defines an exhaustive list of criminal law measures applicable to legal entities. According to Article 67 (Circumstances Aggravating

Punishment) of the Criminal Code of Ukraine, the use of artificial intelligence systems is not included in the list of circumstances aggravating punishment.
Thus, these provisions do not contain provisions regarding the specifics of acts with additional qualifying characteristics committed using artificial intelligence.

In the CC of Ukraine, the use of computer equipment, electronic devices, information and telecommunications systems or technologies is a means of committing a number of criminal offenses provided for in: Part 4 of Article 190 (fraud committed through illegal operations using electronic computing equipment), Article 156-1 (sexual harassment of a child), Part 1 of Article 301-1 (accessing, acquiring, storing, importing, transporting or otherwise moving, manufacturing, selling and distributing child pornography), Article 301-2 (holding a sexual entertainment event involving a minor), Article 200 (illegal actions with transfer documents, payment cards and other means of access to bank accounts, electronic money, equipment for their manufacture), part 2 of Article 289 (illegal seizure of a vehicle committed using electronic devices to interfere with the operation of technical security equipment).
Also, in the Criminal Code of Ukraine, provisions on criminal offenses in the field of use of electronic computers, systems, and computer networks and telecommunications networks are highlighted in Section XVI of the Special Part of this Code.
This section contains, for example, Article 361-1 “Creation for the purpose of unlawful use, distribution, or sale of malicious software or technical means, as well as their distribution or sale.”

Hypothetically, it is possible to imagine that a malicious software tool was created using AI or a specifically created AI model (taking into account the purpose of its creation and the functions it performs) and is such a malicious software tool. Under such conditions, there are grounds for applying the general rules of qualification. However, there is no case law in accordance with the simulated situation.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

There are no specific provisions in the Criminal Code of Ukraine that directly regulate criminal liability for acts related to the use of artificial intelligence systems. In cases of crimes committed using artificial intelligence, the general provisions of the Criminal Code of Ukraine apply, taking into account the elements of the crime provided for by law, namely: the object, the objective side (including the act, consequences, causal link, method, place, time, tools, and means of committing the crime), the subject and subjective side (form of guilt, intent, negligence, motive, purpose).
An artificial intelligence system may be recognized as an instrument of crime in cases where it is used by a person to directly commit or facilitate the commission of a crime, provided that a causal link between its use and the occurrence of consequences is established.
Part two of Article 168, “Procedure for Temporary Seizure of Property,” of the Criminal Procedure Code of Ukraine stipulates that the temporary seizure of electronic information systems, computer systems or their parts, mobile communication terminals for the purpose of studying physical properties that are relevant to criminal proceedings shall be carried out only if they are directly specified in the court ruling.
The temporary seizure of electronic information systems, computer systems or their parts, mobile communication terminals is prohibited, except in cases where their provision, together with the information contained therein, is a necessary condition for conducting an expert examination, or if such objects were obtained as a result of a criminal offense or are a means or instrument of its commission, as well as if access to them is restricted by their owner, possessor, or holder, or is associated with overcoming a logical protection system.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

According to Ukrainian legislation, the use of AI is not considered an aggravating circumstance.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

According to Ukrainian legislation, there are no regulations governing the use of specific AI technologies in the committing of crimes.

Criminal offenses, as provided for, in particular, by Articles 156-1 “Solicitation of a child for sexual purposes,” 301 “Import, manufacture, sale, and distribution of pornographic items,” 301-1 "Access to child pornography, its acquisition, storage, import, transportation or other movement, manufacture, sale and distribution" of the Criminal Code of Ukraine, may potentially be associated with the use of artificial intelligence as a means and/or instrument for committing unlawful acts, although this feature may not be explicitly stated in the disposition of the relevant provision.

At the same time, regarding the use of autonomous drones to kill people: according to information posted on the official website of the Ukrainian Parliament, the Verkhovna Rada of Ukraine has registered a draft law of Ukraine “On Amendments to the Code of Ukraine on Administrative Offenses, the Criminal Code of Ukraine, and the Air Code of Ukraine regarding the strengthening of liability for offenses in the field of civil aviation after the termination or cancellation of martial law in Ukraine” (reg. No. 13600 of 05.08.2025) (hereinafter referred to as the draft law).
According to the explanatory note to the draft law, its purpose is to standardize the rules for flying unmanned aerial vehicles, their registration and accounting, standardize the functioning of the unmanned aviation system, and determine liability for offenses in the field of civil aviation.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:

The use of AI in the commission of a criminal offense is currently not listed in part one of Article 67 of the Criminal Code of Ukraine as an aggravating circumstance. At the same time, according to part three of this article, when imposing a sentence, the court cannot recognize as aggravating circumstances those not specified in part one of this article.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

The Unified State Register of Court Decisions contains a number of criminal proceedings in which artificial intelligence was involved in one way or another in the context of committing offenses or in the course of court proceedings. In particular:
• Financial fraud: in cases No. 757/31391/22-k, No. 757/35689/22-k, and No. 757/39004/25-k, the organizers of international financial pyramids convinced the victims that their investments were managed by artificial intelligence to ensure high returns, while in fact the funds were embezzled.
• Abuse of procedural rights: in case No. 991/4110/25, the applicant used ChatGPT to draft an appeal; the court considered this to be an abuse of procedural rights and contempt of court.
• Cybercrimes and attempts at justification: in case No. 161/5016/21, the convicted person claimed that child pornography was sent to the victim by “artificial intelligence” created by him, but the court found this version unproven.

• Court decision formed with the help of AI: in case No. 11- кп/824/1818/2025, the court of appeal found that the first instance verdict contained fragments generated by ChatGPT, which replaced the judges' discretion. This became the basis for overturning the verdict and scheduling a new trial.
• AI as newly discovered circumstances: in case No. 743/1378/13-k, the convicted person attempted to use artificial intelligence calculations based on satellite data and telephone connections to prove his innocence, but the court found this data to be legally insignificant.
• AI mining and training: in case No. 757/53166/21-k, the investigating judge refused to overturn the seizure of more than 3,400 game consoles, which, according to the investigation, were illegally imported and used for cryptocurrency mining and artificial intelligence training.
• Espionage in the field of AI: in case No. 757/21307/21-k, it was established that a foreign citizen collected and transmitted information related to scientific developments in the field of nanotechnology and artificial intelligence, which constituted state secrets, for further use by a foreign state.

Article 16 of the Code of Judicial Ethics, approved by Resolution XX of the regular congress of judges of Ukraine on September 18, 2024, establishes that the use of artificial intelligence technologies by judges is permissible if it does not affect the independence and impartiality of the judge, does not relate to the assessment of evidence and the decision-making process, and does not violate the requirements of the law.
In accordance with parts five and six of Article 13 of the Law of Ukraine “On the Judicial System and Status of Judges,” conclusions on the application of legal norms set forth in Supreme Court rulings are binding on all authorities that apply the regulatory legal act containing the relevant legal norm in their activities. Conclusions on the application of legal norms set forth in Supreme Court rulings are taken into account by other courts when applying such legal norms.
In particular, according to the position of the Supreme Court as part of the panel of judges of the Commercial Court of Cassation dated July 8, 2025, set forth in the ruling in case 925/496/24: "...the complainant's reference to the fact that the court of appeal unreasonably rejected the motion to examine electronic evidence, namely the responses of two artificial intelligences (GROK (developed by xAI) and ChatGPT (developed by OpenAI) to confirm the literal interpretation of subparagraph 6 of paragraph 23 of the Agreement, is rejected by the panel of judges, since artificial intelligence can be a useful and helpful informational tool in the field of justice, but cannot replace either the role of judges or the principles of relevance, admissibility, and reliability of evidence provided for in Chapter 5 of the Civil Procedure Code of Ukraine. Technology should only be used to support and strengthen the rule of law. Technology can only be used to support and assist courts and judges in the proper management and determination of proceedings. Decision-making must, explicitly or implicitly, be carried out only by judges. It cannot be delegated or performed with the help of technology. Judicial autonomy must be respected through the use of technology.
However, in the case under consideration, the participant uses artificial intelligence technology not as a means of promoting the proper administration of justice, but rather to challenge (question, appeal) the conclusions already made by the court. This is consistent with the legal position set out by the Supreme Court in its ruling of 08.02.2024 in case No. 925/200/22...".
At the same time, with the aim of introducing modern and effective models of management, information protection, increasing the level of digitization, and optimizing material resource costs in the High Anti-Corruption Court (hereinafter – HACC), by order of the HACC dated December 19, 2024 No. 56 “On Certain Issues of Using Artificial Intelligence Tools in the High Anti-Corruption Court” approved the Principles for Using Artificial Intelligence Tools in the High Anti-Corruption Court, which define the general provisions for the use of artificial intelligence tools by judges and staff in performing the tasks assigned to the HACC.
In accordance with paragraph 1 of Section II of the aforementioned order, the main purpose of using AI in the activities of HACC is to increase the efficiency and transparency of HACC's activities, as well as to establish the conditions and rules for the use of AI tools in the performance of official duties in order to improve the quality of work, reduce the amount of organizational and material resources spent, and finding ways to improve the efficiency of the HACC's work organization processes.
Thus, national practice already records various aspects of the use of artificial intelligence in criminal proceedings — from fraudulent schemes to procedural abuses and even espionage. This

indicates the need for clear regulatory regulation and an expert approach to the assessment of evidence related to AI technologies.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

Current legislative reform plans in Ukraine do not envisage specific measures regarding (criminal) liability and crimes related to AI.

The Concept for the Development of Artificial Intelligence in Ukraine was approved by Resolution No. 1556-p of the Cabinet of Ministers of Ukraine dated December 2, 2020, which defines the goals, principles, and objectives for the development of artificial intelligence technologies in Ukraine as one of the priority areas in the field of scientific and technological research. This Concept was developed in accordance with the Government's Priority Action Plan for 2020, approved by the Cabinet of Ministers of Ukraine on September 9, 2020, No. 1133-p.

At the same time, the Cabinet of Ministers of Ukraine approved a plan of measures for the implementation of the Concept for the Development of Artificial Intelligence in Ukraine for 2025-2026 by its Resolution No. 457-p of May 9, 2025.

The main measures of the Plan include the development and submission to the Cabinet of Ministers of Ukraine of a draft law on legal regulation in the field of AI development, ensuring the adoption of international standards in the field of artificial intelligence development as national standards, ensuring the use of artificial intelligence technologies in the field of defense, etc.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

In Ukraine, legal reforms concerning aggravating circumstances related to the use of artificial intelligence systems in the commission of crimes are not currently under consideration..

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

The Ministry of Digital Information of Ukraine developed the White Paper on AI Regulation, that based on the AI Regulation Roadmap. It laid the foundation for the bottom-up and gradual approach to AI regulation and alignment with the EU AI Act. The essence of the approach is to divide the path to mandatory regulation into two stages:
1. The preparatory stage (2-3 years, before the adoption of a law that is analogous to the EU AI Act) includes facilitation of self- and co-regulation among stakeholders and providing them tools for compliance.
2. The implementation stage of law that is analogous to the EU AI Act. By that moment, Ukraine is ensuring the state’s and the industry's capacity to regulate and comply accordingly.
According to the White Paper, Ukraine is currently implementing the first stage of approach, which includes such policy instruments and soft law tools as: Sandbox; adaptation of the Council of Europe HUDERIA methodology; support of signment of the Voluntary Code of Conduct between AI companies and establishment of self-regulatory organisations; publication of guidelines on AI for various sectors. Currently, guidelines have been published for: lawyers, developers, higher education institutions, civil servants, schools, intellectual property, media, and advertising. The guidelines help people from different sectors be aware of the responsible use of AI tools in their work.

Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

In Ukrainian copyright law, the term sui generis is used to define a special legal regime for objects that are not works in the traditional sense but require legal protection. According to the current Law of Ukraine “On Copyright and Related Rights,” such protection is provided for non-original objects created with the help of computer programs. This means that if an AI system creates certain content that is not original (i.e., does not contain human creative input), it can still be protected under this special regime. In practice, this provision applies to the following cases: Generated data and works created without human involvement.

4. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

No information currently available .

5. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

There is an objective need to introduce a separate criminal offense relating to so-called “dark” AI, i.e., AI systems specifically designed for malicious purposes. These include technologies designed to carry out cyberattacks, hacking, attacks on critical infrastructure, and other actions that pose significant risks to public and national security. Given the autonomous nature of such systems, it is extremely difficult to prove the guilt of a specific person, which requires special regulatory measures.

Separately, it is worth emphasizing the advisability of criminalizing the circulation of prohibited AI systems. This refers to the production, sale, import, transfer to third parties, or other forms of distribution of such technologies. At the same time, the list of prohibited systems must be clearly defined at the legislative level, taking into account both national and European security standards.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

The Criminal Code of Ukraine establishes liability under Article 361-1 (Creation for the purpose of unlawful use, distribution, or sale of harmful software or technical means, as well as their distribution or sale). The subject of this criminal offense is precisely harmful software and technical means designed for unauthorized interference with the operation of computers, automated systems, computer networks, or telecommunications networks.

In order to develop programs, the perpetrator of the crime may use any available information. Therefore, it is not advisable to regulate the source of knowledge by law, given that the decisive factor in this case is intent – the creation of a criminal program from elements and digital platforms based on AI or information about the algorithms of information systems and programming languages.

The problem arises when developers artificially level the restrictive mechanisms in AI, which directly give the attacker a fundamentally new, high-quality tool—AI, which, thanks to the use of its capabilities, develops malicious software on demand.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

Yes, we see a need for such a criminal offence to address the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties of AI systems prohibited under national or European legislation.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

Resolving the so-called “negligence dilemma” is an important aspect that arises in connection with autonomous AI actions. To this end, it is advisable to legislate the presumption of control over the operation of such systems by their developers or operators. This approach will avoid legal gaps in holding accountable persons who directly or indirectly created the conditions for the commission of offenses.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

The use of AI certainly requires legal regulation. However, specific legislative measures should be taken after identifying existing and potential threats associated with the use of AI in criminal activities and comparing these threats with the existing legal instruments for responding to them. If such an analysis reveals gaps in legislative regulation, they need to be addressed.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?

- ✓ **definitions**
- ✓ **procedural provisions,**
- ✓ **jurisdiction provisions**
- ✓ **extradition and mutual assistance issues**
- ✓ **problems with digital evidence**
- ✓ **collaboration of digital AI platforms with criminal prosecutions**
- ☐ **other issues**

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

Yes, we agree that the definitions should align with those in the AI Act.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

One of the most important issues requiring urgent consideration and resolution is the formulation and implementation of provisions in the current criminal legislation concerning the commission of criminal offenses involving the use of artificial intelligence, as well as the assessment by courts of the relevant circumstances of criminal proceedings.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

In our view, a single global instrument would allow for the unification of approaches among Council of Europe member States at the level of guiding principles, while also providing a structured methodology for assessing the risks and impact of AI. At the same time, individual legislative acts in specific areas would ensure sufficient flexibility and responsiveness to national particularities. The establishment of common European standards in this field would be of particular added value, as such standards could significantly facilitate future cooperation mechanisms, notably in the areas of extradition as well as the recognition and enforcement of judgments.

UNITED KINGDOM

Foreword from the United Kingdom

With regards to the answers of the United Kingdom below, it is important to note that criminal law is a devolved matter to be determined by the devolved governments of Scotland and Northern Ireland within those jurisdictions. As such, the criminal law of England and Wales, Scotland and Northern Ireland are addressed separately. Please find answers from Scotland at the end of this questionnaire.
It is also important to note that AI is a cross-cutting topic and some matters regarding the regulation of technology more broadly are reserved for the UK Government, as are topics of national security and measures relating to terrorism. On such matters, the devolved legislatures of Wales, Scotland and Northern Ireland will not have competency to legislate. Insofar as those matters are concerned, the UK's response shall refer to the UK government in that reserved capacity.

A: Existing Frameworks

1. Does your national legislation and/or case law specifically address criminal liability or crimes connected to artificial intelligence?
If so, could you please:
(1) provide, if available, the relevant texts (in English or in French);
(2) indicate whether criminal responsibility is attributed to a specific person (natural or legal, e.g., driver, producer, programmer, fleet supervisor, tele-operator, etc.) and what standard it is based on (i.e., strict liability, negligence, intent).
If not, will general rules apply in situations where crimes are committed, facilitated, enhanced, or aided by artificial intelligence?

UK: England and Wales

Criminal law in England and Wales is generally flexible and broad enough to encompass the use of AI in the commission of criminal offences and therefore there is no specific legislation that addresses the broader concept of criminal liability for crimes committed with the use of AI systems. However, criminal law in England and Wales does include some specific provisions which cover specific uses of AI to cause harm and commit criminal acts – although these do not always refer exclusively to the use of AI systems, such uses which may be covered include:

1. Non-consensual intimate image abuse

- The Sexual Offences Act 2003, as amended by the Data (Use of Access) Act 2025, includes an offence of intentionally creating a non-consensual purported intimate image of an adult without consent or reasonable belief in consent, and an offence of requesting the creation of a purported intimate image of an adult without consent or reasonable belief in consent. Neither of these offences are yet in force.
- It is an offence under the Sexual Offences Act 2003 for a person to intentionally share or threaten to share a photograph or film without consent or reasonable belief in consent, including photographs or films which were made or altered by computer graphics – which may or may not include AI.

2. Child sexual abuse material

- AI-generated child sexual abuse material (CSAM) is illegal in the UK. The creation and sharing of CSAM which is AI-generated is captured by offences under the Protection of Children Act 1978 and the Coroners and Justice Act 2009. However, neither Act specifically refers to AI, and these offences instead apply to "pseudo-photographs" (which are images, however made, which appear to be a photograph) or prohibited images which needn't be photorealistic.
- The UK Government is also introducing new offences in England and Wales related to child sexual abuse image-generators under the Crime and Policing Bill. The Crime and Policing Bill will also update existing law under section 69 of the Serious Crime Act 2015 to ensure the definition of 'paedophile manuals' includes instructions to create AI-generated child sexual abuse material.

In answer to the final question under Question A1, general criminal law provisions will apply to criminal conduct not specifically addressed by specific offences or specific legislation.

2. What general rules are applied in your law when AI systems (as defined in Article 2 of the CAI, ETS No. 225) are used as tools for the intentional commission of criminal offences (such as murder, manslaughter, or theft)?

UK: England and Wales

Where an offence in England and Wales can be carried out using a tool, including AI, the use of that tool will be considered part of the conduct element of the offence, and is not generally considered a separate offence in its own right.
Similarly, the use of AI is irrelevant in the commission of an offence, so long as every element of an offence is present on the facts of the case – such offences can be committed with the use of AI systems or without. For example, the offence of theft in England and Wales requires the appropriation of property belonging to another, with the intention to permanently deprive the other of it. The law does not require that theft is done in a particular way nor by the use of specific tools or systems.
As a further example, it is an offence to make, distribute, show or publish indecent photographs of children under the Protection of Children Act 1978. This includes “pseudo-photographs” which are images, however made, which appear to be a photograph. This definition includes images generated by AI.
Offences relating to the possession of articles for use in relation to particular crimes (such as fraud) may also apply where the tool in question is an AI system made or adapted for a criminal purpose. For example, the offence of “going equipped for stealing” in the Theft Act 1968 is so broadly drafted that an AI tool which enables theft may fall within its definition depending on the facts of the case. Similarly, section 6 of the Fraud Act 2006 creates an offence of possession of articles for use in fraud. “Articles” is defined in a way which captures any program or data held in electronic form, so would capture the possession of AI tools specifically adapted for use in committing fraud.
Encouraging or assisting others to commit crime by providing AI tools may also be captured by existing general offences in some circumstances.

3. According to your domestic law and/or case law, can the use of AI systems be considered an aggravating circumstance?

UK: England and Wales
There is currently no specific aggravating factor for the use of AI in the commission of an offence. Judges in England and Wales, in their capacity as an independent judiciary, are free to consider any relevant facts in a case an aggravating factor – which may include considering the use of AI in the commission of the offence of which they have been convicted.
Whether the use of an AI in the commission of an offence might be considered an aggravating factor will depend upon the particular facts of each case.

4. Does your law address the use of specific AI technologies for committing crimes, e.g., the use of deepfakes in certain contexts (such as sexual deepfakes, online sexual grooming, or during electoral processes), the use of autonomous drones to kill someone, or specific forms of fraud?

UK: England and Wales
Although the UK Government has introduced measures to address AI-specific harms, such legislation is broadly worded with the intention of ensuring it is applicable regardless of the specific technology used, including the use of AI.
Please refer to our response to Q.A1 for more information on existing offences involving the use of AI, such as those offences included in the Sexual Offences Act 2003.
The Online Safety Act 2023 is also now in effect. The Act covers some generative AI tools, chatbots and platforms such as those which offer user-to-user services, those that enable the search of more than one website, and those that can generate pornographic material.

5. Is the use of AI considered an aggravating circumstance, particularly in cases involving:
☐ sexual deepfakes
☐ online sexual grooming
☐ electoral processes
☐ use of autonomous drones to kill someone
☐ fraud of notorious importance
☐ other:

UK: England and Wales
Please refer to our answer to Question A3.

6. Are there any examples of national case law or investigative practice (e.g., criminal investigations, prosecutorial assessments) involving crimes committed or facilitated by artificial intelligence? If yes, please summarise the case(s) or describe the issues, if possible.

UK: England and Wales

There was the high-profile case of Jaswant Chail in 2023 that demonstrated the role chatbots can have in radicalising individuals considering violent action. Chail was given a nine-year sentence for gaining access to Windsor Castle with a loaded crossbow, intent on killing the late Queen Elizabeth II – actions he was encouraged to undertake by an AI chatbot he had developed.
Chail was charged with treason and plead guilty to making threats to kill and being in possession of an offensive weapon. No charge was made in relation to his “conspiracy” to commit murder with the chatbot he had developed, as conspiracy must be between two legal persons, and an AI chatbot is not considered a legal person in England and Wales.
The circumstances surrounding the use of this AI system were applied by the courts during sentencing in determining Chail’s mental state, his motivations for committing the offence, and his culpability for the crimes for which he was found guilty.

B. Future plans

1. Does the legislator in your country plan legal reforms regarding (criminal) liability and crimes related to AI?

UK: England and Wales

The UK Government is clear on its ambition to bring forward legislation specific to the topic of AI, to realise the enormous benefits and opportunities of this technology while mitigating its most pressing risks and harms.
While the criminal law of England and Wales is broadly capable of capturing the use of AI systems in the commission of a criminal offence, we are continuing to review our existing legislative frameworks to ensure the UK is able to realise AI’s transformational potential whilst safeguarding against potential risks.
The Crime and Policing Bill is currently in Parliament, seeking to criminalise AI models which have been made or adapted to create AI generated child sexual abuse material – please refer to our answer to Q.A1 for more information. It will also amend the existing ‘paedophile manuals’ offence under s.69 of the Serious Crime Act 2015, which currently criminalises the possession of advice or guidance about abusing children sexually, to include guidance pertaining to the creation of AI child sexual abuse images.
The AI landscape is complex and constantly evolving; the UK will continue to refine its AI legislation proposals, which will incentivise innovation and investment.

2. Does the legislator in your country plan legal reforms concerning aggravating circumstances when a crime is committed, facilitated, enhanced, or aided by the use of AI systems?

UK: England and Wales

When deciding what sentence to impose, the courts take into account the circumstances of the offence and any aggravating and mitigating factors, in line with any relevant sentencing guidelines issued by the Sentencing Council for England and Wales. Courts are required to follow sentencing guidelines unless it is not in the interests of justice to do so.
The UK has considered this topic and currently has no plans to introduce any specific statutory aggravating factor for the use of AI in criminal offending in England and Wales.

3. Would your legislator address the new challenges of effectively protecting rights put at risk by the use of AI systems through measures other than adopting new criminal laws? If so, how?

UK: England and Wales

The UK Government is currently considering a wide range of measures, including safeguards for security risks arising from the use of AI.
The UK Parliament's Joint Committee on Human Rights has launched a new enquiry to examine how human rights can be protected in the age of AI. The inquiry will involve the committee examining the threats and opportunities AI offers for human rights in the UK and consider whether the existing legal and regulatory frameworks are fit for purpose.
We are continuing to review our existing legislative frameworks and non-legislative policy options.

4. Does the legislator in your country plan legal reforms concerning the protection of copyright in connection with the use of AI (e.g., due to web scraping, web harvesting, or data extraction from websites to train large language models)?

UK: England and Wales

The UK Government is considering potential changes to copyright as it applies to AI. The Government recently published a consultation covering a range of issues and potential changes and received a wide range of responses from stakeholders across the creative industries, technology sectors and academia. We are now carefully reviewing that evidence and establishing stakeholder working groups to inform the development of policy on copyright and AI.

5. Does the legislator in your country plan legal reforms concerning the development of applications that facilitate the production of (sexual) deepfakes, or the use or dissemination of (sexual) deepfakes?

UK: England and Wales

The UK Government is seeking to criminalise AI models which have been made or adapted to create AI generated child sexual abuse material (including deepfake technology) through the Crime and Policing Bill. This Bill is being considered by Parliament as part of the UK's legislative process.
The UK Government also recently passed the Data (Use and Access) Act 2025 which includes an offence of intentionally creating a non-consensual purported intimate image of an adult without consent or reasonable belief in consent, and an offence of requesting the creation of a purported intimate image of an adult without consent or reasonable belief in consent. Neither of these offences are yet in force.

6. Based on your national context and legal developments, are there any other behaviours or activities involving artificial intelligence that your authorities consider should

be criminalised in the future? If so, please describe the conduct and, if possible, explain the rationale.

UK: England and Wales

The AI landscape is complex and constantly evolving and the UK is continuing to review its existing legislative frameworks in England and Wales.
We are currently considering various areas of crime and are examining how to ensure our criminal law is future-proofed for AI, including where the risks and harms may lie in future.

C. Scoping the need for a new instrument

1. Do you see a need for a new type of offence related to dark AI?
(This refers to AI systems specifically engineered for malicious purposes, such as hacking, cracking, or other cyberattacks, as well as AI designed to target critical infrastructure, create serious public security risks, or facilitate the commission of any crime.)

UK: England and Wales

With regards to new kinds of offending and AI-enabled harm, the UK Government recognises the impact that AI misuse can have on public safety and national security. Existing AI systems can enable malicious actors to radically and quickly upscale their activities and we know this already poses significant risks to areas like fraud, Violence Against Women and Girls, and terror-related activity.
We are continuing to review the existing legislative frameworks in England and Wales to ensure we are able to safeguard against such offending.

2. Do you see a need for a new type of offence to criminalise the placing on the market, putting into service, production, acquisition for personal use, importation, or provision to third parties - in any form - of an AI system that is prohibited under national or European legislation?

UK: England and Wales

Please refer to the written response to Question C1.
The UK notes that this question refers to “national or European legislation” and therefore implies reliance on the EU AI Act, which does not apply to the UK. The UK would opt for a common definition of AI systems in this context based on definitions by the OECD or the Council of Europe’s Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.

3. Do you see a need to adopt specific measures to address the "negligence dilemma" arising from the autonomous actions of AI systems?

UK: England and Wales

The core concepts underpinning the criminal law in England and Wales are capable of being fulfilled when AI tools play a part in the commission of an offence, including in the circumstances defined in the “negligence dilemma”.
The UK Government is also considering how to account for the autonomous actions of AI systems.

4. Do you see a need for the creation of an international instrument (Convention on AI and Crimes) similar to the Budapest Convention on Cybercrime, which would define and criminalise acts that can be committed, facilitated, enhanced, or aided through AI systems?

UK: England and Wales

The UK does not currently see the need for an international instrument on criminal liability and the use of artificial intelligence.
An international instrument on AI and criminal liability would likely be unnecessary and difficult to implement in a way which is effective in practice. The core concepts underpinning the criminal law in England and Wales are capable of being fulfilled when AI tools play a part in the commission of an offence.
The most advanced AI systems pose distinct opportunities and risks. These systems and the companies that create them transcend international borders, and we continue to see striking technological breakthroughs in what they can do.
The UK may consider it beneficial to establish greater cooperation on the investigation and prosecution of AI-enabled offending where such offending reaches across borders. The nature and extent of such practical cooperation would be a matter for further discussion.
The UK is currently considering its domestic legislation and regulatory frameworks, but we are committed to working closely with international partners as our approach must fit within a broader global approach to AI security.

D. Content of a prospective new instrument, if developed

1. In your view, which of the following elements could a prospective new international instrument (Convention on AI and Crimes) include?
□ **definitions**
□ **procedural provisions,**
☐ **jurisdiction provisions**
☐ **extradition and mutual assistance issues**
☐ **problems with digital evidence**
☐ **collaboration of digital AI platforms with criminal prosecutions**
☐ **other issues**

UK: England and Wales

The UK does not see a need for an international instrument on artificial intelligence and criminal liability such as a “Convention on AI and Crimes”. Please refer to our written answer to Question C4 above.

2. Do you agree that the definitions should align with those in the AI Act? Please give details.

UK: England and Wales

The UK would opt for definitions as defined by the OECD to ensure broader international application and alignment with the terminology adopted by the OECD or the Council of Europe’s Framework Convention on Artificial Intelligence.
Any alignment on definitions would need to be considered on a case-by-case basis and would need to prioritise alignment on futureproof definitions of AI technologies and risks.

3. Which of the above issues (if any) do you consider the most urgent to address in relation to AI and criminal law?

UK: England and Wales

The UK does not see a need for an international instrument on artificial intelligence and criminal liability such as a “Convention on AI and Crimes”. Please refer to our written answer to Question C4 above.
The UK may consider it beneficial to establish greater cooperation on the investigation and prosecution of AI-enabled offending where such offending reaches across borders. The nature and extent of such practical cooperation would be a matter for further discussion.

4. What would be, in your view, the advantages or disadvantages of a single global instrument addressing AI and criminal law, or individual pieces of legislation in specific areas?

UK: England and Wales

We are committed to working closely with international partners on our approach to AI security and keeping people in the UK safe. A single global instrument for technology that is evolving at such a fast pace may quickly become irrelevant and it may be more beneficial to tackle commonly agreed issues with bespoke processes, legislative or otherwise.
The recent UN Convention on Cybercrime was adopted by the General Assembly in December 2024 and is likely to be open for signature in October. Whilst not specifically focused on AI, this and other conventions, such as the Council of Europe Lanzarote Convention (CSEA), already cover crimes facilitated by AI and a further instrument may cause additional complexity, leading to an adversely crowded regulatory landscape.
Finally, we understand that many member States are at different stages of considering their own domestic regulatory frameworks for AI; some already have regimes that apply to AI-enabled criminal offending or AI more broadly and the UK would not recommend seeking an international regulatory framework where States may still be reviewing and/or amending their domestic law on this topic.

Annexed information from Scotland

UK: Scotland

While there is ongoing work as part of the Crime and Policing Bill at the Westminster Parliament which could impact Scots law, the Scottish Government has no live plans to specifically consider AI and criminal liability. In general, however, any consideration of future international legal instrument would need to be carefully looked at to take the distinct nature of Scottish law and devolved justice policy in the UK into account.
We are not aware of any specific legislation or case law that specifically engages with AI in Scotland. That is not to say that offences could not be committed through the use of AI tools, whether text/image generation or operation based.
In general, crimes in Scotland are outcome-focused, meaning the method or means of committing the crime isn't necessarily relevant or determinative. There are specific crimes where the method forms part of the underlying actus reus but committing a murder by autonomous drone would simply be a murder. There may be other crimes attached (under legislation related to aviation, terrorism etc) but there is no specific legislation on AI.
Use of AI wouldn't be an aggravation in itself in Scotland.
The use of deepfakes isn't itself criminalised. Altering images or producing deepfake pornographic material is not a specific offence and the production of such material in itself, would probably not amount to a criminal offence in Scotland. However, the distribution, publication or sale etc. of such material, where it appears to depict a person who has not consented to such a depiction may amount to a criminal offence. Depending on the facts and circumstances, this may be capable of being charged under offences including section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 (non-consensual sharing of intimate images), section 38 of the Criminal Justice and Licensing (Scotland) Act 2010 (threatening or abusive behaviour) or section 127 of the Communications Act 2003 (misuse of a public electronic communications network). However, the Scottish Government's and COPFS data only details numbers of convictions and charges under these acts, and not detailed information on the specific conduct which resulted in the charge or conviction. [from Written question and answer: S6W-00472 | Scottish Parliament Website]

"Art and part" liability in Scottish law is important to note here. This operates under the Common Law more broadly and S293 of the Criminal Procedure (Scotland) Act 1995 explains its operation for statutory crimes:

293 Statutory offences: art and part and aiding and abetting.

1. A person may be convicted of, and punished for, a contravention of any enactment, notwithstanding that he was guilty of such contravention as art and part only.

2. Without prejudice to subsection (1) above or to any express provision in any enactment having the like effect to this subsection, any person who aids, abets, counsels, procures or incites any other person to commit an offence against the provisions of any enactment shall be guilty of an offence and shall be liable on conviction, unless the enactment otherwise requires, to the same punishment as might be imposed on conviction of the first-mentioned offence.

This could mean the creator of an AI agent (if sufficiently independent) is held fully liable for that agent's acts given their role in the agent's creation, including responsibility for programming etc. Deliberately creating such an agent might also, depending on the circumstances, amount to culpable and reckless conduct.