



Strasbourg, 30 April 2026

CDPC-AICL(2026)07

COUNCIL OF EUROPE COMMITTEE ON CRIME PROBLEMS (CDPC)

**Working Group on Artificial Intelligence and Criminal Law
(CDPC-AICL)**

Recommendation of the Committee of Ministers to member States on Criminal Law Responses to Deepfakes ZERO DRAFT

Prepared by Expert Magistrate Alfonso Peralta Gutiérrez; revised and supplemented
by the CDPC Secretariat

Criminal Law Secretariat

DGI-CDPC@coe.int / www.coe.int/cdpc

PREAMBLE

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Recalling that the Council of Europe's aim is to achieve greater unity among its member States, particularly through common actions in promoting and safeguarding human rights, the rule of law and democratic governance;

Recognising that artificial intelligence technologies, including deepfake systems, can be used in ways that pose significant threats to those objectives;

Reaffirming the obligations of member States to secure to everyone within their jurisdictions the rights and freedoms under the European Convention on Human Rights (ETS No. 5, the Convention) and its Protocols, in particular the right to respect for private life (Article 8), freedom of expression (Article 10), and the right to a fair trial (Article 6);

Recalling that the European Court of Human Rights has consistently held that member States have positive obligations under Article 8 of the Convention to adopt adequate legal frameworks - including, where necessary, criminal law measures - to protect individuals against serious interferences with their private life and personal integrity perpetrated by private actors, and that the gravity of harm caused by non-consensual deepfake content may engage such positive obligations;

Mindful of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), the first binding international treaty on artificial intelligence governance, which requires Parties to adopt measures preventing AI systems from undermining democratic institutions and processes;

Having regard to the Convention on Cybercrime (ETS No. 185) and its Protocols, which provide the foundational international framework for addressing technology-facilitated criminal conduct, and emphasising the importance of ensuring coherence with that framework;

Bearing in mind the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention, CETS No. 201) and the importance of ensuring that child protection standards are fully maintained in the context of AI-generated content;

Recalling the Committee of Ministers' Recommendation on Accountability for Technology-Facilitated Violence against Women and Girls, and the need for coherent responses addressing the specific risks faced by women and girls in the use and misuse of AI and deepfake technologies;

Acknowledging that deepfake technologies - by enabling the realistic synthesis or manipulation of a person's image, voice or likeness - can facilitate a range of serious criminal offences, including non-consensual sexually explicit content, fraud, impersonation and identity theft, as well as the creation of child sexual abuse material;

Recognising that deepfake content depicting identifiable persons in a sexual or degrading manner without their consent constitutes a serious violation of human dignity, the right to private life and personal integrity, and may cause severe and lasting harm to any victim regardless of their gender, age or other personal characteristics;

Noting that criminal misuse of deepfake technologies is not limited to any single category of offence, but extends across diverse areas including property crimes, identity misuse and the exploitation of minors, and that national legal frameworks may present gaps in their coverage of such conduct;

Acknowledging the cross-border nature of deepfake-related offences, which often involve creators, disseminators and victims located in different jurisdictions, making international cooperation essential for effective criminal justice responses;

Recognising that any criminal law response to deepfake technologies must be carefully calibrated to avoid undue restrictions on freedom of expression, including the protection of artistic, satirical, journalistic and research activities, in accordance with Article 10 of the Convention and the relevant case law of the European Court of Human Rights;

Emphasising the principles of legality, legal certainty, necessity and proportionality as fundamental constraints on the exercise of criminal law powers, and noting that technological neutrality should guide the interpretation and application of criminal offence provisions where appropriate;

Noting the results of the questionnaire conducted among member States of the CDPC-AICL Working Group, which revealed broad convergence regarding the need to address non-consensual sexual deepfakes and child sexual abuse material in criminal law, and wider - though more nuanced - support for action in areas including fraud, impersonation, grooming and procedural integrity;

Recognising that deepfake-related offences, in particular those of a sexual nature, cause harm that is not limited to the moment of creation or first dissemination, but persists and compounds as the content continues to circulate online, often beyond the victim's ability to control or remove it, and that this ongoing victimisation constitutes a distinctive feature of such offences that criminal law and procedural frameworks must take into account;

Reaffirming that victims of deepfake-related criminal offences are entitled to effective access to justice, to appropriate support services, and to remedies that include not only criminal sanctions against perpetrators but also practical mechanisms for the prompt removal or blocking of unlawful content, and that the design of criminal law responses should place the rights and interests of victims at its centre;

Noting that the rapid evolution of deepfake technologies - which are becoming increasingly accessible, affordable and difficult to detect - creates a growing risk that existing criminal law frameworks will be outpaced by the capabilities of malicious actors, and that a Council of Europe Recommendation in this field, given the Organisation's broad membership of 46 member States and its established expertise in criminal law standard-setting, provides a timely and appropriate means of inspiring coherent legislative responses at the national level and encouraging further normative action by other international organisations and regional bodies;

Convinced that a Recommendation of the Committee of Ministers provides a flexible and timely means of guiding member States in developing coherent national criminal law responses to the malicious use of deepfake technologies, while leaving room for further binding standards should future developments so require,

RECOMMENDS that the governments of member States be guided, in their national criminal law policies and legislation, by the principles and measures set out in this Recommendation.

I. PURPOSE AND SCOPE

Purpose

1. This Recommendation aims to provide guidance to member States on addressing, within their criminal law frameworks, the malicious use of deepfake technologies. It seeks to encourage coherent national legislative responses while respecting the diversity of legal traditions across the Council of Europe.
2. Specifically, this Recommendation is intended to:
 - promote common normative principles for addressing deepfake-related conduct within criminal law frameworks;
 - encourage member States to review and, where necessary, strengthen their criminal law provisions to ensure adequate coverage of deepfake-facilitated offences;
 - address procedural and evidentiary challenges arising from the use of AI-generated content in criminal proceedings;
 - promote effective international co-operation in the investigation and prosecution of cross-border deepfake-related offences; and
 - support prevention, awareness and capacity-building efforts.

Scope

1. This Recommendation covers the intentional creation, dissemination or use of AI-generated or AI-manipulated synthetic content - including images, audio, video or other media - where such conduct constitutes or facilitates criminal offences against identifiable persons or protected interests. The specific scope of the Recommendation should cover, as a minimum:
 - Non-Consensual Sexual Deepfakes;
 - Digital child sexual abuse material (DCSAM);
 - Use of Deepfakes in Child Grooming and Exploitation;
 - Fraud, Impersonation and Identity Misuse;
 - *[Etc.]*
2. *[In keeping with the guidance provided by the Finnish delegation at the 5th CDPC-AICL meeting,]* the scope should be understood as focused and purposeful. Member States are encouraged to apply the principles of this Recommendation in a manner proportionate to the specific harms addressed.
3. This Recommendation does not cover:
 - legitimate artistic, satirical, journalistic, educational or research uses of synthetic media, subject to national law and the safeguards of Article 10 of the European Convention on Human Rights *[delegations may wish to consider whether additional categories of legitimate use should be explicitly excluded from the scope of this Recommendation]*;
 - issues of civil or administrative liability arising from AI use, which fall under separate legal frameworks;
 - the use of AI by member States' armed forces or in the context of international humanitarian law;

- the criminal liability of AI systems as such, which is excluded on the basis that criminal liability under this Recommendation is grounded in the intent or culpable negligence of natural or legal persons.
- 4. This Recommendation is without prejudice to existing Council of Europe instruments, in particular the Convention on Cybercrime (ETS No. 185) and its Protocols, and the Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

II. DEFINITIONS

For the purposes of this Recommendation, the following definitions apply:

“Deepfake” or “digital forgery” means AI-generated or AI-manipulated image, audio, video or other synthetic content that depicts or represents an existing person, object, place, entity or event in a manner that would falsely appear to a reasonable observer to be authentic or truthful *[delegations are invited to consider whether the reference to “a reasonable observer” is the appropriate standard, or whether an alternative formulation would better reflect the technical realities of deepfake detection]*.

“AI-generated content” means content produced autonomously by an artificial intelligence system without being directly derived from pre-existing real content.

“AI-manipulated content” means content derived from pre-existing real material that has been substantially altered using an artificial intelligence system so as to misrepresent the original.

“Identifiable person” means any natural person who can be recognised, directly or indirectly, from the synthetic content, whether by their face, voice, name, identifying characteristics or any other means.

“Digital child sexual abuse material” (DCSAM) means AI-generated or AI-manipulated content that visually depicts a minor engaged in sexually explicit conduct, or that depicts the sexual organs of a minor for primarily sexual purposes, regardless of whether any real child was involved in its creation. *Drafting should ensure full compatibility with the definitions in the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse.]*

These definitions should be applied in a technologically neutral manner and interpreted so as to remain applicable as technology evolves. Careful drafting at the national level should ensure compatibility with existing definitions under the Cybercrime Convention and the Lanzarote Convention.

III. GENERAL PRINCIPLES

Member States should be guided by the following principles when formulating or reviewing their criminal law responses to deepfake-related conduct:

Respect for human rights and fundamental freedoms

All legislative and enforcement measures adopted in response to deepfake-related conduct must be fully compatible with the European Convention on Human Rights and other applicable international human rights instruments. Particular attention should be paid to the right to a private life (Article 8 ECHR), freedom of expression (Article 10 ECHR), and the right to a fair trial (Article 6 ECHR).

In particular, any criminal law measure that engages freedom of expression must satisfy the three-part test established by the European Court of Human Rights under Article 10 §2 of the Convention: it must be prescribed by law with sufficient precision; it must pursue a legitimate aim; and it must be necessary in a democratic society, meaning that it must respond to a pressing social need and be proportionate to the legitimate aim pursued.

Legality, legal certainty and foreseeability

Criminal offences related to deepfake conduct must be defined in clear and precise terms, accessible to the public, so that individuals can reasonably foresee the legal consequences of their actions. Vague or overly broad formulations should be avoided.

Necessity and proportionality

The use of criminal law to address deepfake-related conduct should be limited to cases where it is necessary and proportionate to achieve a legitimate aim. Civil, administrative or regulatory measures may in many cases provide a more appropriate response, and criminal law should not be relied upon as the default instrument.

Technological neutrality

Where appropriate, criminal law provisions should be formulated in a technologically neutral manner, so as to remain effective as deepfake technologies evolve, and to avoid the rapid obsolescence of legislative measures tied to specific technical methods.

Coherence with existing international instruments

Member States should ensure that national measures adopted pursuant to this Recommendation are consistent with their existing obligations under Council of Europe and other international instruments, including the Cybercrime Convention and the Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse. Duplication or conflict with those frameworks should be avoided.

Protection of victims

The rights and interests of victims of deepfake-related offences should be a central consideration in the design of legislative and enforcement responses. This includes access to justice, effective remedies, support services and content removal mechanisms.

IV. SUBSTANTIVE CRIMINAL LAW

This section *[is the primary focus of this Recommendation, reflecting the preference expressed by the Czech delegation at the 5th CDPC-AICL meeting. It]* addresses the areas in which member States should consider strengthening or clarifying their substantive criminal law frameworks in order to adequately respond to the criminal dimensions of deepfake technologies. The guidance is organised by categories of harm and reflects the levels of support expressed by member States in the questionnaire. For each area, the Recommendation sets out guidance on the conduct to be addressed, the mental element required, aggravating circumstances, and sanctions.

1. Non-consensual Sexual Deepfakes

[Given the strong convergence among member States, this area warrants the most specific and detailed guidance.]

The European Court of Human Rights has recognised, in its case law under Article 8 of the Convention, that member States are required to ensure effective protection of individuals against

acts that seriously violate their sexual integrity and personal autonomy, even where such acts are committed by private persons without the use of physical force. Member States should take into account this jurisprudence when reviewing the adequacy of their criminal law responses to non-consensual sexual deepfakes.

a. Conduct to be criminalised

1. Member States should ensure that their criminal law covers, as distinct and specific offences or as adequately covered conduct under existing provisions, the following acts when committed intentionally and without the consent of the person depicted:
 - the production or creation of sexually explicit synthetic content depicting an identifiable person, irrespective of whether the content is subsequently disseminated;
 - the dissemination, sharing, distribution or publication of such content through any means, including online platforms and private messaging services;
 - the possession of such content with intent to distribute or share;
 - the threatening to produce or disseminate such content, where used to coerce, intimidate or extort the victim.
2. For the purposes of this Recommendation, “consent” to the original recording or creation of content does not constitute consent to its sexual transformation, synthetic reproduction or dissemination in a sexually explicit form *[to be discussed: whether a specific definition of consent should be included, or whether reference to national law is sufficient]*.

b. Mental element

1. The offences referred to in paragraph 1 should require proof of intentional conduct. Member States may also provide that reckless disregard as to whether consent was given constitutes a sufficient mental element for the offence of dissemination.
2. Member States should ensure that honest and reasonable belief in consent may constitute a defence, subject to the requirement that the accused took reasonable steps to ascertain consent.

c. Aggravating circumstances

1. Member States should establish aggravated forms of the offences referred to in paragraph 1, carrying increased penalties, where one or more of the following circumstances are present:
 - the victim is a minor, a person with a disability or a member of a particularly vulnerable group;
 - the offence is committed by a person in a position of trust, authority or influence over the victim, including within the context of an intimate or family relationship;
 - the offence is committed for financial gain, whether directly or through coercion or extortion of the victim;
 - the content is disseminated to a large number of persons or published on publicly accessible platforms;
 - the offence is committed as part of an organised criminal enterprise;
 - the offence causes severe psychological, professional or social harm to the victim.

d. Sanctions

1. Member States should ensure that the offences referred to in this section are punishable by effective, proportionate and dissuasive criminal sanctions, taking into account the severity of the harm caused.
2. In addition to custodial and financial sanctions, member States should consider providing for ancillary measures, including:
 - orders for the prompt removal or blocking of the unlawful content;
 - prohibition orders restricting the convicted person's use of digital technologies or online platforms;
 - confiscation of instruments and proceeds of the offence;
 - obligations of reparation or compensation to the victim.

2. Digital child sexual abuse material (DCSAM)**a. Conduct to be criminalised**

1. Member States should ensure that their criminal law expressly covers the production, acquisition, possession and dissemination of digital child sexual abuse material as defined in Section II. The AI-generated or synthetic nature of the material – and the absence of a real child victim in the production process – should not constitute a ground for exemption from criminal liability.
2. Member States should also consider criminalising the generation of content that, while not explicitly sexual, is clearly intended to sexualise or exploit the image of a minor, in accordance with the principles of legality and proportionality.

b. Mental element and defences

1. Offences relating to DCSAM should require intentional conduct. Member States may provide that knowingly accessing such material, even without downloading or storing it, constitutes a criminal offence.
2. Member States should ensure that their law does not provide defences based solely on the synthetic origin of the material. Any defence of artistic or educational purpose should be subject to strict scrutiny and should not apply where the primary purpose of the material is sexual.

c. Coherence with the Lanzarote Convention

All measures adopted pursuant to this section should be drafted and applied in full coherence with the obligations of the Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse. Member States are encouraged to consult the Recommendations of the Committee of the Parties to that Convention when reviewing their national law.

3. Use of Deepfakes in Child Grooming and Exploitation

1. Member States should assess whether their existing offences adequately cover the use of synthetic identity impersonation or AI-generated content in the context of child grooming, online solicitation or child sexual exploitation, including:
 - the use of deepfake audio or video to impersonate a peer, trusted adult or authority figure in order to gain the trust of a child;

- the use of AI-generated personas in online environments for the purpose of establishing contact with children with a view to their sexual exploitation;
 - the sharing of AI-generated sexual content with a child as part of a grooming process.
2. Where such conduct is not already covered by existing grooming or exploitation offences, member States should consider introducing specific provisions or clarifications. Legislative responses should emphasise coherence with the Lanzarote Convention.

4. Fraud, Impersonation and Identity Misuse

Deepfake technologies increasingly enable sophisticated fraud and identity-based offences, including voice cloning, face-swapping and the creation of fictitious personas. Member States should take the following measures:

a. Review of existing provisions

1. Member States should review whether existing fraud, deception and impersonation offences provide adequate coverage for deepfake-facilitated conduct, including cases where a person's voice, image or likeness is synthetically reproduced without consent in order to deceive a third party into taking an action that causes financial or other harm.
2. Where existing provisions are formulated in technologically neutral terms, member States should consider issuing prosecutorial or judicial guidance to confirm their applicability to deepfake-facilitated conduct, rather than creating new offences.

b. Specific clarifications or offences

Where existing provisions do not adequately cover deepfake-facilitated conduct, member States should consider:

- establishing AI-facilitated identity misuse – such as voice cloning or face-swapping for deceptive purposes – as an aggravating circumstance of existing fraud or impersonation offences;
- introducing specific offences covering the unauthorised synthetic reproduction of a person's voice, image or likeness for deceptive or harmful purposes, where not already covered by existing law;
- ensuring that the criminal law covers the use of deepfakes to deceive identity verification systems, including biometric authentication where applicable *[delegations may wish to consider whether this provision is sufficiently precise, or whether further guidance on the types of systems covered would be helpful]*.

c. Sanctions

Offences in this category should be punishable by effective, proportionate and dissuasive sanctions. Member States should ensure that confiscation of proceeds of AI-facilitated fraud is available as an ancillary measure.

5. Attempt and Participation

1. Member States should ensure that attempt to commit the offences referred to in sections 1 and 2 above is criminalised, where the offence is sufficiently serious.
2. Member States should ensure that aiding, abetting, inciting or otherwise facilitating the commission of deepfake-related offences is also criminal, including:

- providing deepfake generation tools or services knowing they will be used to commit an offence;
- hosting, distributing or sharing deepfake content knowing it constitutes criminal conduct.

6. General Aggravating Circumstance

Member States should consider establishing the use of AI systems or deepfake technologies to facilitate, conceal or amplify the commission of a criminal offence as a general aggravating circumstance under national criminal law. This would allow courts to take into account the enhanced capacity for harm, increased scale or reduced detectability enabled by such technologies when determining sentences across a wide range of offences, beyond those specifically addressed in this Recommendation.

7. Criminal Liability of Legal Persons

1. Member States should ensure that legal persons – including companies involved in the provision, deployment or distribution of AI systems – can be held liable, whether criminally, civilly or administratively, where the criminal use of deepfakes is attributable to them by reason of a lack of supervision or control by a person in a position of authority within the legal person.
2. Such liability should not preclude the concurrent criminal liability of the natural persons responsible.
3. Providers, deployers and operators of AI systems should not be held liable for content generated by users through the misuse of their systems, where:
 - they had no effective knowledge of the unlawful nature of the content; or
 - upon acquiring such knowledge, they acted promptly and diligently to remove or disable access to the content.
4. Member States should adopt measures to require AI providers and platform operators to establish effective mechanisms for the reporting and removal of deepfake content that constitutes criminal conduct, and to co-operate promptly with competent judicial and law enforcement authorities.

V. PROCEDURAL AND EVIDENTIARY ISSUES

Member States should review their procedural and evidentiary rules to ensure that criminal proceedings involving deepfake content can be conducted effectively and fairly.

1. Assessment of Digital Evidence

1. Member States should ensure that their procedural frameworks provide guidance on the assessment of the authenticity and reliability of AI-generated or AI-manipulated content tendered as evidence in criminal proceedings.
2. Courts, prosecutors and investigating authorities should be assisted in determining:
 - whether content tendered as evidence has been altered, generated or manipulated by an AI system;
 - the reliability and limitations of AI-based forensic tools used to detect deepfakes;

- the disclosure obligations of parties who introduce AI-generated content in proceedings.
- 3. Member States should consider establishing or strengthening procedural rules that require parties to disclose, at the earliest practicable stage, where content presented as evidence may have been generated or manipulated using AI systems *[to be discussed: whether such disclosure obligations should apply equally to prosecution and defence, and at what stage of proceedings they should take effect]*.
- 4. Member States should ensure that procedural rules governing the use of AI-generated or AI-manipulated content as evidence are consistent with the guarantees of Article 6 of the Convention, as interpreted by the European Court of Human Rights. In particular, defendants must have a genuine and effective opportunity to challenge the authenticity and reliability of digital evidence adduced against them, in accordance with the principle of equality of arms and the right to an adversarial hearing.

2. Capacity-Building

1. Member States should invest in specialist training for judges, prosecutors, investigating judges and law enforcement officers in relation to:
 - the technical functioning and capabilities of deepfake technologies;
 - methods and tools for forensic detection of AI-generated content;
 - the evidentiary assessment of synthetic media in criminal proceedings.
2. Member States should also promote digital and AI literacy among the general public, and particularly among children, young people and other vulnerable groups, in order to enhance the ability of individuals to identify and critically evaluate synthetic content.
3. Member States should co-operate with universities, research institutions and relevant international organisations to develop and disseminate expertise in this rapidly evolving field.

VI. JURISDICTION AND INTERNATIONAL CO-OPERATION

1. Jurisdiction

1. Member States should review their jurisdictional frameworks to ensure that they can effectively assert criminal jurisdiction over deepfake-related offences with a cross-border dimension. In particular, member States should consider establishing jurisdiction where:
 - the offence is committed on their territory, regardless of the nationality of the perpetrator or the victim;
 - the perpetrator is a national of the member State concerned;
 - the victim is a national of or habitual resident in the member State concerned, at least in relation to the most serious offences.
2. Where more than one State has jurisdiction over an alleged offence, the States concerned should co-operate to determine the most appropriate forum for prosecution.

2. International Co-operation

Member States should promote effective international co-operation in the investigation and prosecution of deepfake-related offences, in accordance with applicable international instruments, particularly the Convention on Cybercrime (ETS No. 185) and its Protocols.

To this end, member States should:

- consider recognising serious deepfake-related offences as extraditable offences, in accordance with applicable international instruments;
- make use of existing mutual legal assistance mechanisms to facilitate the swift exchange of evidence in deepfake-related investigations, including digital evidence held by service providers in other jurisdictions;
- encourage the use of existing frameworks in a manner that facilitates effective cooperation, and consider accepting requests for assistance where the conduct concerned would be criminal under the law of the requested State even if defined differently;
- promote direct co-operation between prosecutorial and law enforcement authorities in different States, including through established networks of contact points.

VII. PREVENTION AND AWARENESS

1. Member States are encouraged to develop or support public awareness campaigns to inform the general population about the existence, nature and potential harms of deepfake technologies, and about the legal consequences of their malicious use.
2. Member States are encouraged to promote responsible deployment of AI systems capable of generating synthetic media, including through:
 - the promotion of technical standards and good practices for the labelling and disclosure of AI-generated or AI-manipulated content;
 - engagement with AI providers, online platforms and other relevant stakeholders to implement effective content moderation practices and to facilitate the rapid removal of harmful deepfake content;
 - support for research and development of technologies capable of detecting AI-generated or manipulated content.
3. Member States are encouraged to engage with the private sector, civil society and educational institutions to foster a culture of responsible AI use and to build societal resilience against the harms associated with deepfake technologies.
4. Member States should ensure that victims of deepfake-related offences have access to appropriate support services, legal assistance and effective remedies, including mechanisms for the prompt removal or blocking of unlawful synthetic content.
5. Member States are encouraged to support the development and use of technical tools for the detection and identification of synthetic content, where appropriate.

VIII. MONITORING AND FUTURE REVIEW

1. Member States are invited to report to the Committee of Ministers, through the CDPC, on measures taken to implement this Recommendation, including legislative changes, policy initiatives and operational developments.
2. The CDPC should periodically review the implementation of this Recommendation and assess its effectiveness in light of technological developments in the field of AI and deepfake technologies, taking into account relevant case law and national practices.
3. The CDPC should monitor relevant developments at the national and international levels and consider whether further, and potentially binding, normative standards may

be required [*delegations are invited to indicate their views on the appropriate timeline and form of any future review exercise*] as the technology and its misuse evolve.

4. In conducting its review, the CDPC should draw upon the expertise of relevant Council of Europe bodies, including the Committee of the Parties to the Lanzarote Convention, the Cybercrime Convention Committee (T-CY), and the Steering Committee for New and Emerging Digital Technologies (CDNET), as well as civil society and expert communities.

APPENDIX – EXPLANATORY NOTES

These explanatory notes are intended to assist member States in interpreting and implementing this Recommendation. They do not form part of the Recommendation itself.

On Section I (Purpose and Scope)

The scope of this Recommendation is deliberately focused on conduct that intentionally causes harm through the creation or dissemination of deepfake content. It reflects the preference expressed by the Finnish delegation at the 5th CDPC-AICL meeting for a cautious and proportionate approach. Member States retain full discretion to adopt broader national measures where they consider this appropriate.

On Section II (Definitions)

The definitions in this section are intended as a working framework for the purposes of this Recommendation. They draw on the definition in Article 3(60) of the EU AI Act and on prior work within the CDPC. States are encouraged to adopt definitions that are compatible with those in the Cybercrime Convention and the Lanzarote Convention.

On Section IV – General approach

Section IV is deliberately the most developed part of this Recommendation, reflecting the preference expressed by the Czech delegation for a focus on substantive criminal law. The structure – organised by category of harm, with sub-sections on conduct, mental element, aggravating circumstances and sanctions – is intended to give member States concrete and actionable guidance while stopping short of prescribing specific offence formulations, which remain a matter of national law.

On Section IV.1 (Non-consensual Sexual Deepfakes)

This area attracted the strongest convergence among member States. The Recommendation encourages criminalisation of both production and dissemination, reflecting the reality that harm can occur at either stage. The concept of ‘consent’ in this context should be understood broadly: consent to the original recording or creation of content does not constitute consent to its sexual transformation, synthetic reproduction or dissemination in sexually explicit form. The inclusion of threatening to produce or disseminate such content addresses the increasingly common practice of ‘deepfake extortion’.

On Section IV.2 (DCSAM)

The term ‘digital child sexual abuse material’ (DCSAM) is used deliberately to signal that AI-generated content depicting minors in a sexual manner is to be treated as seriously as material produced through the real-world abuse of children. The note that the absence of a real child victim does not constitute a ground for exemption from liability reflects the growing consensus – consistent with the Lanzarote Convention framework – that the harm caused by the

normalisation and circulation of such material is independent of whether a real child was directly exploited in its creation.

On Section IV.4 (Fraud, Impersonation and Identity Misuse)

Member States are encouraged to consider whether existing fraud and impersonation offences are sufficiently technology-neutral to apply to AI-facilitated conduct. In many jurisdictions, existing provisions will apply without amendment; in others, specific clarification or supplementary offences may be needed. The reference to biometric authentication systems is intended to address the growing use of deepfakes to bypass identity verification in financial and administrative contexts.

On Section IV.7 (Criminal Liability of Legal Persons)

The framework for liability of legal persons set out in this Recommendation is modelled on the approach taken in the Cybercrime Convention and related instruments. The ‘safe harbour’ provisions in paragraphs 3 and 4 are intended to ensure that liability attaches to those who knowingly facilitate criminal conduct, and not to those who act promptly and in good faith to address harmful content upon becoming aware of it.

On freedom of expression safeguards

This Recommendation consistently preserves the protection of legitimate speech, including satire, parody, artistic expression and journalism. Member States should ensure that criminal law provisions do not have a chilling effect on these constitutionally and conventionally protected activities. The case law of the European Court of Human Rights on Article 10 ECHR should be taken into account in drafting and applying national measures.