XXI INTERNATIONAL CONGRESS OF PENAL LAW ON ARTIFICIAL INTELLIGENCE AND CRIMINAL JUSTICE

SECTION II: PENAL LAW AND CRIMINALIZATION IN THE FACE OF THE CHALLENGES OF AI

Resolution (draft), final version approved by the Colloquium in Bucharest, 14th–16th of June 2023

Preamble

Considering that

- Artificial Intelligence, one of the last advancements of the digital revolution, has already reached a significant level of development in this third decade of the 21st century and is already widely used in many sectors of society;

- although there is no absolute agreement on the definition of this technology, there is an implicit consensus that it includes a multitude of computerized systems that, through the gathering, the processing, and the analysis of data in their context, are capable of acting autonomously and/or assisting in decisions to achieve specific objectives;

- the transformative potential of this technology is impacting multiple fields and social spheres, bringing important benefits and opportunities;

- Artificial Intelligence also poses risks and harms to individual and collective interests.

Observing that

- multiple decisions traditionally adopted or informed by humans are beginning to be automated through the use of these technologies, affecting different areas and interests;

- in areas such as autonomous vehicles, health services, financial markets, media, and other sectors, the use of this technology is unstoppable and a future without it seems inevitable;

- the promise of AI being both efficient and objective is leading to the development of these technologies without assessing its real necessity or considering the risks that it may create.

Bearing in mind that

- recent developments in large language models and other AI systems such as machine learning and deep learning have highlighted the need for regulation, including security protocols, to control the evolution of these technologies in terms of their effects and risks;

- the development of AI systems, particularly the training of its algorithms, requires the use and accumulation of data and large amounts of information, which is a risk that must be considered in itself;

Highlighting

- the growing concern about the harm malicious or negligent uses of AI can cause in areas where AI is already beginning to have a strong presence;

- that there are many countries in which the use of AI systems has caused harm to relevant interests such as life, health, and privacy, among others;

Acknowledging

- that the emergence of new criminal acts as well as new interests worthy of criminal protection will lead states to adapt criminal laws related to AI;

- the need to analyze whether states' legal response to the challenges of AI is sufficient or it needs to be reformed and adapted, either through specific modifications or through the creation of new forms of criminalization;

Taking into account

- the Recommendation of the Council on Artificial Intelligence adopted by the OCD on 22 May 2019; the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts presented by the European Commission on 21 April 2021; the European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)); the Ethics Guidelines for trustworthy AI presented by the High-Level Expert Group set by the European Commission on 8 April 2019; and Recommendation CM/Rec (2020) 1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies);

- the debates and resolutions of previous International Criminal Law Congresses, in particular the resolutions of the XIV Congress on Criminal law and modern bio-medical techniques and the legal and practical problems posed by the difference between criminal law and administrative penal law; the resolutions of the XIX International

Congress of Penal Law – Information Society and Penal Law; and the draft resolutions of the XXI International Congress of Penal Law on Section I (Criminal Law – general part) and Section 3 (AI and the administration of criminal justice);

The participants of Section II of the Colloquium in Bucharest, 14–16 June 2023, have adopted the following:

RESOLUTIONS

I. AI regulation and enforcement

1. With the development and expansion of AI, harms and risks to individual and collective interests have arisen and are likely to increase. This poses the need for an adequate regulation of the production and implementation of AI systems and of its use. The response to these challenges shall consider different perspectives and all available regulatory tools, whether they are public or private, taking into account the different nature and functionality of each.

2. The global impact of AI requires an international response to effectively protect the individual and collective interests at stake. States should take into account international standards in national regulation and enforcement.

3. As happened with other technological and socio-economical innovations, for instance the Internet or new developments in gene editing and neuroscience, the irruption of AI makes it necessary to review general aspects of the criminal justice system and, in particular, the catalog of existing offenses in criminal laws to ascertain if states' regulations are suitable to the challenges posed by the use of this technology.

4. The debates regarding the transformation of criminal law in response to the impact of AI and the role that the criminal law system might play in relation to these new technologies shall not be isolated from the international ethical discussions taking place on the development of AI, nor can they overlook discussions regarding AI regulation in other branches of the legal system. Considering this broad picture, legislators shall reflect on the specific role that criminal law plays to avoid harms caused by the use of AI.

5. Legislators will have to reform existing offenses when AI modifies the risk to existing interests or creates new means of perpetration that are not covered by existing legislation. Moreover, new offenses shall be introduced when the development of this technology leads to the emergence of new individual and collective interests worthy of protection not covered by existing legislation.

II. Criminalization and the protection of interests related to AI

6. The development of AI may give rise to new interests worthy of protection. Additionally, AI systems can affect the dimension and relevance of interests that are not currently considered worthy of protection by criminal law. When criminal laws do not provide an adequate response to protect these interests, new criminal offenses shall be enacted that proportionally punish conduct harmful to such interests. This shall only be done when there are no means less harmful than criminal law to effectively protect such interests.

7. When the transformation of AI leads to the emergence of new interests which are essentially similar to others traditionally considered worthy of protection, new criminal offenses shall not be introduced. Instead, it is preferrable to adapt the interpretation of existing offenses, as long as strict respect for the principle of legality allows.

8. Legislators will have to decide whether the development of this technology gives rise to the need for specific criminal protection of individual or collective interests related to AI technology itself. While it is still too early to determine whether such a need will arise, this could be the case for the data on which the algorithms are based; the functionality of AI systems themselves, in some cases; collective interests related to the safety and reliability of their design and application; or even interests associated with robots.

9. Some AI systems, such as those used in critical infrastructures, are essential to assure already protected interests. To the extent the Budapest convention contemplates the criminalization of attacks on computer systems and AI may be considered as such, the enactment of new offenses might not be necessary. In order not to raise interpretative doubts, it might be advisable to reform some criminal offenses to introduce AI systems as types of computer systems.

10. If it is not proven that there are some other interests at stake and considering the current level of development of these technologies, AI and robotic systems do not deserve different protection, in relation to their economic or functional value, from other computer systems.

III. Grounds of legitimization and techniques of criminalization

11. Criminal law shall not play a leading role in the regulation of AI. In view of its nature as a particularly coercive enforcement instrument, it must intervene as the last resort and be limited to the repression of the most serious and harmful acts.

12. Legislators shall not introduce new offenses based solely on the fact that AI was employed. Many criminal offenses can be committed using AI systems as a means of carrying out the sanctioned conduct. It is only when acts committed with AI systems acquire a different meaning in terms of harmfulness or risk that it will be necessary to enact new criminal offenses.

13. The automation of data-driven decision-making processes AI entails resituates the key moment of human agency to phases of design and implementation of algorithms far removed from the harm. The liability of individuals and legal persons involved should therefore preferably be focused on these phases. This shall be done considering existing legal duties established in other branches of the legal system.

14. Criminal law systems are designed to have a deterrent effect on likely offenders, preventing them from engaging in criminal actions. If the key moment in terms of risk in relation to AI is the moment of the design and implementation, the enactment of offenses that aim to deter conducts at such moments shall be considered. This can be done by anticipating protection with endangerment offenses that punish failure to fulfil certain duties in relation to specific interests worthy of protection. Also, and similarly to what is established for the criminal liability of legal persons, specific regulatory obligations related to the design and implementation of AI systems could be established, infringement of which may give rise to criminal liability.

15. Endangerment offenses related to the design and implementation of AI systems that cause risks shall be enacted when the sanctioned actions pose a considerable threat to the protected interests. Additionally, the legal consequence attached to these offenses shall be proportional to the level of risk caused and the interest at stake. Due to the complexity of the design of AI systems and the different approaches to regulating these tools, endangerment offenses shall not be enacted before considering the developments in self-regulation or administrative regulations on control and security of AI in each legal system. These regulations shall serve to identify relevant risky acts that might be worthy of criminal prosecution.

16. New offenses might be introduced to punish the abuse and transformation of existing lawful AI systems when, by changing the design or the purpose of the AI, new risks arise.

17. In those legal systems where negligent action is only punished when expressly provided for (*numerus clausus*), reform of criminal laws might be required. The complex design of AI and the participation of multiple parties in the AI lifecycle means that in most cases it will be extremely difficult to prove awareness at the time of design that a harmful result was going to occur. Negligence offenses based on the infringement of standards of due diligence could be then enacted if the protection of the affected interests make it necessary.

18. Since AI systems are dynamic and their performance depends on the introduction or collection of data that modify its outcomes, risk management processes established on other branches of the legal system might operate throughout the entire AI lifecycle. Thus,

criminal laws may address, if necessary, infringements of rules related to the lack of appropriate monitoring and oversight of AI systems, duties that might affect different subjects involved in the whole lifecycle of AI.

19. Since AI technology and its applications are scalable, criminal justice systems might adapt to adjust the proportionality of penalties to the severity of the harm that AI can cause. Nevertheless, legislators shall not enact aggravated circumstances only because an offense was committed using AI. Only if existing aggravated circumstances can't encompass the severity of the damages caused by the use of AI, attending also at the relevance of the affected interest, new forms of aggravation shall be considered. This shall always be done complying with the principle of proportionality.

IV. Criminalization and the protection of specific interests from the risks created by AI.

20. Since criminal laws do not usually provide for specific means for the commission of crimes against life and health, it does not seem necessary to reform these offenses in order to protect such interests when AI system have been used as a mean of commission. Nor does it seem necessary to modify the system of liability graduation. Nevertheless, in specific areas, such as autonomous driving, criminal law will have to be attentive to the changing regulatory landscape, that will be the basis to assert what is considered an "allowed risk" for the determination of liability.

21. If autonomous driving becomes widespread, road safety offenses could undergo significant changes, including new offences related to new risky behaviors for life and road safety other than those currently focused on human driving.

22. In the same way that the revolution on gene editing led to the appearance of offenses sanctioning genetic manipulation with the capacity for mass destruction, technological evolution may make it necessary, in the near future, to criminalize the creation, development and use of AI tools with a high destructive capacity, such us some autonomous weapons, drones or robots that could be enormously harmful specially if human control is lost.

23. AI systems collect and rely on large amounts of information to perform its tasks, creating new threats to classical interests. Given this development of AI technology, a review of offenses linked to privacy and other personal interests is necessary, and a revision of the understanding of privacy as a solely individual good, considering a collective dimension of this interest, should be taken into account.

24. The criminalization of acts involving the unlawful gathering of personal data should not only be linked to the protection of interests such as privacy. The use of AI in cyberspace may open the door to mass data collection for the commission of cybercrimes that harm interests such as property. States should review whether it is necessary to

enact criminal offenses to sanction the unlawful massive collection of data, and similar preparatory acts to serious crimes, whenever it causes concrete risk to those interests and only if there is not another less coercive legal tool available.

25. The accessibility of images and personal data in cyberspace linked to the potential of generative AI to transform images, video, and audio can endanger interests such as reputation and honor or sexual freedom. It is necessary to review whether current criminal laws allow the punishment of conducts harmful to human dignity, reputation, and sexual freedom such as the distribution of Deep Fakes, including those with sexual content, or of child pornography.

26. Generative AIs, such as large language models and similar tools, can facilitate deception, threats, and coercion, affecting different phases of the formation of will, endangering interests worthy of protection. Nevertheless, it does not seem appropriate to introduce new criminal offenses, since current criminal laws encompass the more harmful acts and other means of controlling this type of tools should be used to prevent less risky conduct.

27. The popularization of algorithms for risk management in such areas as healthcare, employee recruitment, justice, credit and loans, and many others has revealed the existence of discriminatory biases in some decisions taken by AI systems. Beyond the criminal offenses that can already punish some particularly serious discriminatory decisions, other branches of the legal system such as civil or administrative law are more appropriate for avoiding the problem of algorithmic discrimination.

28. The use of AI in cyberspace may facilitate and enhance existing attacks against property and other interests worthy of protection. However, given the regulation of cyber fraud and other cybercrimes against property, it will not be necessary, at least in the short term, to adapt these offences to accommodate crimes perpetrated using AI systems.

29. Some of the criminal laws which punish the production, sale, procurement for use, import, distribution, or otherwise making available of devices designed or adapted primarily for the purpose of committing offenses enacted in accordance with articles 2 through 5 of the Budapest Convention can already punish the creation, development, and sale of AI systems designed or adapted for those criminal purposes. Thus, if AI is considered a device, including a computer program, in accordance with Art. 6 of the Budapest Convention, the introduction of new offences that anticipate the criminal response is not necessary in this field.

30. In the socio-economic and financial sphere, the proliferation of algorithmic decision-making systems and the use of AI for trading is already being reported. The risk that malicious or negligent use of AI systems could seriously affect the markets is clear, but the interests at stake could be better protected through preventive regulatory measures of an economic, administrative, and commercial nature, rather than through criminal offences other than those already in place to punish insider trading and similar conduct.

When AI systems are used for manipulating markets, criminal law should be revised to give a proportional response.

31. Concern about the impact of disinformation, first in the aftermath of some electoral processes and then with the infodemic during the Covid-19 crisis, has led many states to create criminal offenses to punish this conduct. The fact that AI can increase its impact either by automating its dissemination or by using sophisticated video-, audio-, image-, and text-manipulation technologies may sustain this trend. Criminalizing disinformation will only be justified for the protection of fundamental interests of democratic societies and if this criminalization does not jeopardize freedom of expression.