Questionnaire - Section II

Offences in the Criminal Code

Prof. Fernando Miró

A. Defining the Scope of the Questionnaire

The development and popularization of the technologies encompassed within Artificial Intelligence (AI) will impact criminal justice in many ways in the coming years. One of the main effects will be the emergence of new criminal behaviours as well as new interests worthy of protection by the criminal justice system and, as a consequence, criminal laws will need to be adapted. This questionnaire aims to identify the challenges that criminal law faces and will face regarding the need to reform different crime types. AI is in continuous development and we still do not know when and how it will evolve, although we do know in which direction. Thus, without disregarding more remote yet plausible advancements, the analysis focuses on technologies that already exist or that seem closer to new advances, since it is considered that current and upcoming developments already pose immediate challenges that are of sufficient importance for the criminal justice system.

Given the general objective is to determine the current state of research on the potential impact of AI on the criminal regulation of crime types in the different countries, the questionnaire has two specific objectives: first, to identify the main characteristics of existing AI systems that may make them both threats to old and new interests worthy of criminal law protection, as well as those characteristics that may also make them values in need of protection. The second is to compare these threats with the regulation of specific crimes in the different criminal codes, in order to analyse whether the legal response is sufficient or whether it requires amendments and adaptations through both specific modifications and the creation of new crimes that protect new interests or punish conducts that are now harmful or dangerous. In addition, the questionnaire seeks to determine the role of criminal law in punishing harmful or dangerous conducts and in protecting interests in relation to other legal areas and even to other systems of formal or social regulation. Finally, the questionnaire also addresses the new actors in AI crimes and in particular legal persons, since the question of which crimes should give rise to criminal liability of legal persons will depend on the identification of risks in relation to particular interests. Therefore, a specific document is proposed to analyse the prevention of corporate crime and AI, which would be carried out from this second section.

B. Conceptual and criminological framework

Despite the widespread use of the term AI, there is no absolute consensus on its definition. Perhaps this is because it is agreed that this technology is in continuous development and that it aims to make a machine behave in a way that is comparable to "intelligent" human activity. The most accepted definition is minimal and includes any "systems that display intelligent behaviour by analysing their environment and taking action — with some degree of autonomy — to achieve specific goals.". This definition includes: a) weak or narrow AI, computer systems that allow automatic learning to carry out a specific task;

b) average or general AI, which do not yet exist and which would have the capacity to understand to carry out any task; c) and strong AI, or Super Artificial Intelligence (SAI), which includes those systems that exceed the capacities of human beings. While it is obvious that much of the changes in the criminal justice system will be caused by more advanced AI technologies, it is also obvious that current AI poses sufficient challenges and threats to be the focus of the present analysis. Taking this into consideration when we have designed the questionnaire we have taken a more wide definition given by the High-Level Expert Group of the European Commission. In this sense, "Artificial Intelligence" (AI) systems are understood as "software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions".

Given the objective is to determine whether current criminal law can adequately respond to the new interests and threats related to the development of AI, it is important to go beyond a phenomenological perspective and adopt a more axiological approach that identifies the risks that are different in this technology from those in human or corporate actions without AI. It will be these different risks that can lead to the amendment of our substantive criminal law. What does AI contribute that human action and the existing instrumental mastery of machines does not? This questionnaire aims to identify this from the respondents' responses; however, it already takes into account two essential elements that may have a particular impact on the need to change the criminal justice system. On the one hand, the efficiency and scalability of AI, which will significantly affect the potential harm of this technology by potentially increasing both the success rate and the harm rate depending on the purpose of the designer, producer, or end user. This may contrast with the way criminal codes currently consider greater offensiveness when delimiting punitive deserts. On the other hand, the potential ability of AI machines to "act autonomously", or at least to have non-contingent control, which is related to the issue of attributing liability based on control and knowledge of the acts and results. This may lead to it being necessary to rethink the creation of new crimes based on risk and negligence.

C. The challenge of adapting substantive criminal law to the development of AI

The questionnaire, which focuses on current or imminent phenomena and on the characteristics of technology that may shape new interests and new risks, will mainly enquire about the following three issues. Firstly, the adaptation of current criminal justice systems to the emergence of new conducts worthy of a criminal law response, as well as new interests worthy of protection. Secondly, the role of criminal law in the current and future response to the new risks in relation to other branches of the legal system. Thirdly, special attention will be paid to some areas where, due to current experience or a special relationship with technology, the risks associated with AI may be even greater. To develop these last two aspects it is essential to first differentiate between: a) on the one hand, analysis of the suitability of national criminal codes for "traditional" crimes

perpetrated using AI; and b) on the other hand, reviewing whether the existing criminal justice systems adequately protect the new interests and values that are related to AI itself or to what it will generate and that socially will be (and may already be) considered worthy of protection, or whether the systems will require amendments and the incorporation of further protected interests. In order to achieve the objectives detailed above, the questionnaire is based on open questions. In this regard, it is essential that each of the national rapporteurs try to answer each of the questions as comprehensively and specifically as possible. It is also desirable that they use as many references, links or specifics as they consider necessary.

D. Questionnaire

I. Foreword

AI is already a reality in many social areas and its evolution and increasing growth will soon make it a preeminent technology that is both valuable and risky. Above all, we are interested in identifying existing agreements and debates surrounding this technology and its impact. In this regard, please **indicate briefly**:

1. Whether there is a public debate in your country related to the benefits and risks that will be associated with the increasing use of AI systems in security matters or in the criminal justice system, and/or a nationally strategy for the development of AI (even if there is a public organisation or institution specifically in charge) Please indicate the implications of these discussions, if any, from the perspective of all stakeholders (public authorities, legislators, legal practitioners and citizens).
2. Whether cases of crimes involving AI have already reached the media and the courts, and whether this is frequent or not. Please indicate and describe the cases and, if there is any, the resolution number, and provide a brief summary.

II. General Remarks about law, criminal law and AI in each country

As opposed to current human actions in which machines or computer programming are also used, AI technologies imply significant changes in processes and results (which we are only beginning to intuit) in terms of efficiency, scalability and automatization. Considering this, and also that substantive criminal law is usually secondary, it is of interest to know whether there are specific regulations for AI or for areas in which the technology is already a reality or is about to become one. Please answer, in accordance with your expert opinion, the following questions.

Accordingly, please briefly answer the following questions:

3. Are there any general regulations of artificial intelligence in your country and, if so, what is their scope? If so, please, specify in which legal text this regulation is provided for. If there is no specific national regulation, does your country adopt international strategies and regulations, e.g. from the European Union? Please, also indicate to what extent this regulation is applied or implemented. If none of the aforementioned is available, what would be your proposal?

4. Are there any regulations on the use of AI in specific areas such as those indicated below (If there is another area that is not specified in the list below, please indicate it)? If so, please indicate what kind of regulations are, describe them briefly. If not, are there any legislative projects? Also, if there is no regulation at all in terms of binding law, please indicate if you are aware of any non-binding regulation (e.g. protocols or codes of conduct from public or private initiatives). If none of the aforementioned is available, what would be your proposal?
    4.1. Drone technology
    4.2. Facial recognition technologies
    4.3. Speech recognition and speech assistance technologies
    4.4. Biometric analysis technology
    4.5. Autonomous driving and flying car technologies
    4.6. Others that you consider of interest
5. Have there been cases in your country where an artificial intelligence system has been involved and where legal goods have been affected and which have also led to a debate on the adequacy of criminal law to respond to it? Do you consider that your legislation in general is adequate enough to respond to these cases?
6. Has the need to criminalise any conducts related to the use of AI or to adequately protect any of the interests derived from its development been raised in the public or political forum?
7. Do you believe that the special part of your criminal code and your criminal law system is adequate to respond to the harmful impacts that my occur from the use of AI? Likewise, do you think that the special part of your criminal law is adequate to protect interests that may require protection in relation to AI?
8. Do you consider that the way in which the criminal code in your country adjusts liability on the basis of the damage caused, may be outdated given the level of potential damage of some actions carried out with AI? For example, the use of AI for the perpetration of crimes such as hate crimes may carry a greater risk because of the scalability and affect many more subjects than a person who carries out this crime himself. Should your country's criminal code take this into account? If so, do you believe that a complete overhaul of the system for determining liability is necessary or would specific modifications suffice? If in your opinion, specific modifications would be sufficient, please indicate how these should be made. For example, through an introduction of an aggravating circumstance in the general part of the criminal code or should an aggravated modality be included in each crime in view of the damage caused by AI system?
9. Do you think that it will be necessary, in general, to incorporate new offences related to the design and control of certain AI systems given the enormous risk that some of them may present for different protected interests? If so, please indicate in which areas and also whether the way your criminal justice system includes and regulates offences would be appropriate and whether there are any areas of criminal intervention that should be taken as models (e.g. criminal regulation of genetic manipulation offences)?
10. Regarding legal persons, if your country's criminal system uses a “numerus clausus” system of criminal liability of legal persons (provided for only some crimes in the special part), for what type of crimes do you consider that legal persons should be held liable for the crimes committed within them and through

the use of artificial intelligence systems? If your criminal system uses a system other than “numerus clausus”, please also indicate the type of offences for which legal persons should be held liable for the commission of offences through the use of AI.

11. And, in relation to criminal organisations whose activity and objective is the commission of criminal acts and the use of artificial intelligence systems for this purpose, what areas of crime do you think deserve special attention for the case of criminal organisations? What type of regulation does your criminal code have on criminal organisations? Do you think that the special part of your country's criminal code would respond adequately to the risk posed by these organisations using artificial intelligence systems to carry out their criminal activities? Has there been any case of this type in your country? If so, please indicate.

III. AI in the commission of "traditional" crimes and the suitability of the Criminal Code

You will now be asked a set of specific questions about the criminal code and the risks posed by the use of AI to each of the protected interests. Please be as specific and comprehensive as possible, detailing criminal offenses and laws regulating conducts and linking all information you believe to be useful.

3.I. Crimes against life and health and AI

12. Are you aware of any cases, either because it has been judicially processed or because it has been made public through the media, in which people's lives or health have been injured or endangered due to a malicious or deficient use of AI? Could you tell us which cases and what type(s) of crime could be punished and, if not they cannot be punished, why not?
13. Do crimes against life and health as regulated in your country allow for criminal sanctions against those responsible for the creation of machines capable of killing or injuring on the basis of subjective responsibility? Could the designers, producers and the sellers of the AI systems also be held responsible according to your legislation?
14. Do you believe that the model of grading liability on the basis of harm caused in crimes against life and health would adequately respond to the potential harm of actions against these interests produced by AI technology? If not, do you think it would be necessary to establish some kind of aggravation and in which crimes and how would you do it?
15. Has the need to expressly regulate the creation of AI machines or systems, such as military robots, killer drones or similar, as a criminal offence been raised in your country? If so, how has such regulation been considered and, in particular, how have been crime concurrence rules established? If not, do you think it should be done and how would you regulate the rules on concurrence offences?
16. Have you considered in your country any type of modification of road safety regulations or the criminal code related to autonomous driving and the configuration of intelligent decision algorithms and the ethical conflicts to which they are subject?
17. Is there any type of recommendation regarding the use or limitation of AI in the genetic field that may require a change in the criminal regulation?

3.II. Personal legal goods (privacy aside)

18. Do you know of any cases, in particular in your country, in which due to a malicious or deficient use of an AI or Algorithm, freedom in any of its aspects (including sexual freedom) or the dignity of people could have been affected? Could you tell us which one or two of these cases and the types of criminal penalties they could be punished with and, if not, why not?
19. As crimes against freedom, sexual freedom and moral integrity are regulated in your country, does the penal code allow for criminal sanctions against those responsible for the creation of machines capable of harming such interests (with conduct such as cyber-bullying or similar)? Could the designers, producers and the sellers of the AI systems also be held responsible according to your legislation?
20. Do you consider that the model of graduation of liability based on the harm caused in crimes against freedom, sexual freedom and moral integrity would respond adequately to the potential harm of actions against these interests produced by means of AI technology? If not, do you think it would be necessary to establish some kind of aggravation and in what crimes and how would you do it?
21. In relation to the possible discrimination that a person may suffer because of some type of algorithmic discrimination that determines and prevents someone from having access to the same working, economic, social or any other conditions on the basis of a pre-established condition, do you think that the criminal regulation in your country would provide an adequate response to these situations or that, on the contrary, this should be regulated by means of some special offence and, in that case, how should it be distinguished from the potential infringement of other administrative or employment provisions?
22. In relation to the possible creation of deep fakes of supplanting someone's image, voice and other personal characters and their use in videos of a sexual nature, what would be the means of sanctioning such conduct, if any, in your criminal system? And do you think that this is appropriate or that the relationship between privacy, self-image and sexual freedom should be reconsidered in these cases?
23. Do you think there is a risk of over-regulation in this area and that areas such as criminal law and others of specific military legislation, road safety, or other areas of risk will end up overlapping? If so, how do you think these legal areas should be differentiated?

3.III. The criminal protection of privacy and intimacy in the context of AI

One of the areas in which the development of AI can pose a threat to individuals is in relation to their privacy and intimacy, since this technology requires large amounts of information in order to work better and perform its tasks. With this in mind:

24. Have there already been cases in your country where the use of AI algorithms or technology has been carried out at the expense of some form of unauthorised or improper access to personal data?
25. Has the specific data protection or privacy legislation in your country been amended or is it planned to be amended in relation to the use of AI technologies

or where it refers to aspects related to these technologies such as the creation of specific user profiles?

26. In accordance with the crimes against privacy provided for in your country's regulations, does the criminal code allow for criminal sanctions for acts that, due to the creation, development and use of AI systems, may seriously affect the privacy and intimacy of individuals?
27. Do you consider that the system for attributing different levels of liability based on the harm caused in privacy crimes would adequately respond to the potential harm of acts against these interests produced by AI technology? If not, do you think it would be necessary to establish some form of aggravation and in which crimes and how would you do it?

3. IV. Criminal protection of property and cyber-crime in the face of AI

One of the areas where AI is being used most is in business. Furthermore, if there is an area for the malicious use of AI, it is cyberspace, where the use of algorithms for the identification of profiles vulnerable to different Internet frauds, and widespread infection of bots for economic extortion, or for ransomware attacks is already a reality. Many criminal systems often link preparatory fraud behaviour (malware infections, illegal computer access, phishing) in specific criminal laws or in chapters other than those on protection of property. In this regard, please answer the following questions:

28. In your country, have there been any actual cases of fraud, extortion or any similar property crimes mediated by the use of AI? Indicate whether these have occurred specifically in cyberspace or also in economic traffic outside it.
29. In accordance with the crimes against property provided for in your country's regulations, does the Criminal Code allow criminal sanctioning of behaviours that, due to the use of AI systems, in cyberspace or in the physical space, may seriously affect these interests?
30. Are cyberfraud as well as the essential preparatory acts to cyberfraud, such as identity theft or identity fraud, malware infections that replace illicit computer access or computer damage (to data and systems) and other conducts covered by the Budapest Convention, punishable in your country? Please indicate which acts, in which laws or chapters of the criminal code, and specify the main jurisprudence in relation to these offences.
31. Do you consider that the system for attributing different levels of liability based on the harm caused in property crimes would adequately respond to the potential harm of acts against these interests produced by means of AI technology? If not, do you think it would be necessary to establish some form of aggravation and in which crimes and how would you do it?

3.V. Market, economic crimes and impact of AI

Artificial intelligence is increasingly present in the financial and commercial sector, facilitating and improving predictive capabilities, customer service, compliance or cybersecurity tasks. Along with these advantages, there are certain risks related to the acquisition, use, management, distribution and access to data and undesired results in the markets.

32. Have there already been any cases in your country where AI has harmed trade, altered prices, manipulated advertising by creating users and false reports or any other crime related to the market and the consumer?
33. In accordance with crimes against the market and consumers provided for in your country's regulations, does the criminal code allow criminal sanctions for behaviours that may seriously affect these interests? And do you think it is necessary to create specific crimes related to the use of AI that aims to alter the market taking into account the potential harm of this type of act?
34. Do you consider that the system for attributing different levels of liability based on the harm caused in crimes against the market and consumers would respond adequately to the potential harm of acts against these interests produced by AI technology? If not, do you think it would be necessary to establish some form of aggravation and in which crimes and how would you do it?

3.VI. Falsification, Intellectual and Industrial Property

There are currently different AI technologies capable of replicating biometric parameters with great accuracy, reproducing images, voices or even objects, with capacities superior to humans and other types of technologies. This is why AI can become a useful technology for falsifying documents, signatures or biometric parameters. Furthermore, AI poses certain risks in relation to the use, management, distribution and access to data and protected works that could facilitate industrial espionage. Finally, certain bots and search algorithms can be used to distribute or locate and download protected works in cyberspace.

35. Have there been any cases in your country of falsification or plagiarism using AI and also of theft, distribution or illegal downloading of intellectual or industrial property? Please indicate whether this has occurred specifically in cyberspace or also outside it.
36. In accordance with the legal provisions for crimes of falsification, plagiarism and illegal reproduction or any other form of economic exploitation without the authorization of the holders of the corresponding intellectual or industrial property rights, does the criminal code allow these conducts to be sanctioned provided that the AI has been used or certain aspects such as serious harm to certain interests are taken into account? If certain aspects are taken into account, could you specify what they are?
37. Do you consider that the system for attributing different levels of liability based on the harm caused by intellectual property crime or falsifications would respond adequately to the potential harm of acts against the interests protected by these crimes when carried out by means of AI technology? If not, do you think it would be necessary to establish some form of aggravation or mitigation and in which crimes and how would you do it?

3.VII Weapons and drug possession and trafficking, organized crime and terrorism

Drones and other unmanned vehicles are a clear example of the risks posed by the dual use of AI, as they can also be used for illegal activities such as drug or weapons trafficking and may even allow attacks to be carried out remotely by depositing dangerous substances

such as explosives. All of the above ensures greater security for the criminal and lowers the psychological barrier posed by the perpetration of crimes such as terrorism. We also find a clear dual use of social bots, which can be used to advertise and sell legal or illegal products.

38. Have there been any cases in your country where drugs or weapons have been trafficked through the use of drones or other unmanned vehicles, or have they been used to commit terrorist acts? Have there been any cases in your country where drugs, weapons or other illegal substances have been sold and trafficked through the use of social bots?
39. In accordance with the legal provisions for crimes of possession of and trafficking in weapons and drugs, crimes of terrorism and organized crime in your country, does the criminal code allow for criminal sanctions for conduct that may seriously harm such interests?
40. Do you consider that the system for attributing different levels of liability based on the harm caused in crimes of possession of and trafficking in arms and drugs or terrorism would respond adequately to the potential harm of acts against these interests produced by means of AI technology? If not, do you think it would be necessary to establish some form of aggravation and in which crimes and how would you do it?

3.VIII Money laundering and financing of terrorism

The relationship between crypto-currency and criminal activity is now well documented. Its non-state distributed nature, characterised by the absence of a central entity that creates, manages or controls virtual, cross-border and pseudo-anonymized crypto-currencies, and by the absence of a point of contact that knows the origin and destination of the transfer, makes it difficult to identify the actors involved in the transactions, as well as the early identification of suspicious behaviour. Therefore, crypto-currency is an efficient payment method in illegal markets, facilitating crimes such as money laundering and the financing of terrorism.

41. Have there been any cases of money laundering or financing of terrorism through the use of crypto-currency, or of using IA technology for money laundering or financing terrorism, in your country?
42. Does your country's legislation respond to the risks posed by these technologies in relation to money laundering and financing of terrorism?

IV.I. AI as an interest worthy of protection and also as an object to be attacked

It is obvious that AI technology is already something worthy of protection, and although it is software or embodied in machines and objects that are already valuable, its decision-making power is what gives it value and what it essentially might need to be. We intend to identify whether the current law (in particular criminal law, but since this is secondary also other primary legal areas) adequately protects the interests related to the development of AI technology, from current weak AI to potential and future general AI. We must also pay attention to AI not as objects of protection but as objects to be attacked, in particular those attacks on AI that as well as harming the economic or functional interests related to

them can be dangerous for other different assets. To this end, please briefly answer the following questions:

43. Do you consider that the criminal code has the appropriate crime types to respond to the interests that should be protected regarding AI technology and its functionality?
44. In particular, and regarding the possible legal protection of machine learning algorithms and other similar weak AI, is there any specific regulation of intellectual property, industrial property or relating to unfair competition which protects the economic interests of the owners and developers of these tools and, if not, is there any legal discussion regarding the legal system of protection? And, finally, is any of this reflected in the criminal code?
45. Do you think that in the case of robots the criminal justice system should establish some specific protection that would take into account the different interests related to these AI and that, in the event that at some point they could have a certain degree of autonomy, their protection that exclusively focusses on their functions should be reconsidered and transferred to the ownership in some other way?
46. Taking into account that AI can be developed for benign purposes but used maliciously and that it can even be hacked to change its learning and its own functionality, do you consider that the criminal code has the appropriate criminal types to sanction attacks to the integrity and functionality of AI algorithms or that specific types should be included to protect the risks of an unauthorized attack, with multiple possible results derived from it, to the AI itself?

IV.II New interests being put under risk

The development of AI has resulted in new risks related to traditional crimes as well as other threats to existing interests that have not yet required protection. The most obvious example is the threat that the phenomenon of misinformation, closely related to AI technology, has posed to democracy. This has led to the possibility of specific regulation in the criminal field. However, the possibility of autonomous protection of digital identity and security, skewed towards the protection of property or privacy, is also being considered in the context of the harmful possibilities offered by this technology and even that of other new interests that may arise.

47. In your country, have you been involved in the debate about fake news and misinformation and have you come across striking cases of this deviant behaviour that have been controversial because they could harm political debate, the image of public persons or companies or some other interest worthy of protection?
48. By means of which specific offences could conducts encompassed in the phenomenon of the fake news be sanctioned? In your country, have any potential legal reforms, particularly of the criminal code been considered to sanction disinformation or fake news? Do you think that it would be possible to sanction these conducts? And, what conflicts with freedoms such as the freedom of expression could arise and what particularities does your legal system have in this respect?

49. What other interests do you think would require special protection against the risks posed by AI and taking into account the regulations in your criminal code?

List of topics for special reports (Section II)

1. The protection of privacy on AI era through Criminal law

2. Cybercrimes committed with AI and Penal Codes response

3. Disinformation, Fake News and Deep Fakes committed by AI

4. The importance of AI for financial crimes