Questionnaire - Section I (Criminal Law - general part)

Traditional Criminal Law Categories and AI: Crisis or Palingenesis?

Prof. Lorenzo Picotti

Objectives and scope

The advent of Artificial Intelligence (AI) technology and autonomous or artificial agents (AA) - ranging from self-driving cars, weapon systems, to robots and to medical diagnosis software -, support and replace many human activities and represent a real benefit for the society[1]. Nevertheless, the autonomy of AI systems and AA increases day by day and their behaviors may be unpredictable to the designers, programmers, producers and users. In the future, AI systems may even play an increasing role in the perpetration of criminal acts[2]. AI systems can be the "instrument" to commit crimes. Further, AI systems, due to their degree of autonomy and intelligence, could become the "subject" of a crime. In the 21st century, criminal law is required to provide the appropriate reactions to prevent and punish crimes committed by, through or against AI systems. This questionnaire addresses the question of whether and how the traditional criminal law categories and criminal liability modes can be applied to crimes related to AI systems and/or whether a *palingenesis* of the traditional criminal law at national and international level is needed.

The main objectives of this questionnaire are:

i. to determine whether the AA have or could have a (separate) legal personhood and agency and can be held liable in their own capacity;

ii. to determine whether and under which conditions human agents designing, programming, producing or using AI systems can be held accountable for decision and actions of artificial agents;

iii. to examine whether and how existing liability models are adequate to cope with the AI crime

iv. to determine whether the development of AI systems may lead to the enactment of new laws in the area of criminal law.

The questionnaire is addressed to the *rapporteurs nationaux* who are requested to provide the *rapporteur général* with an accurate and concise overview of the functioning of their legal systems with regard to the listed issues. The *rapporteur général* provides the *rapporteur nationaux* with a list of questions in order to grant a uniform analysis of each national legal system. The *rapporteurs nationaux* are requested to answer all the questions taking into account the domestic legal legislation, the relevant case law and the current relevant IT legislation and regulation as well. Priority should be given to all normative (national and supranational) sources, followed by regulatory sources and soft

[1] For the present purpose, the term "Artificial Agent" (AA: used interchangeably with "intelligent agent", "rational agent" or "autonomous agent") or "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», as defined by the High-Level Expert Group of the European Commission.

[2] See King T.C., Aggarwal N., Taddeo M., Floridi L., *Artificial Intelligence Crime: An Interdisciplinary Analisis of Foreseeable Threats and Solutions*, Sci Eng Ethics, 26, 89-120 (2020).

law. In addition, the *rapporteurs* should refer to decisions of the courts/case law and, finally, to the most accredited legal literature. First, the *rapporteurs* should provide an objective description of the legal framework, taking into account the abovementioned sources. Opinions, evaluations or suggestions, in a *de jure condendo* perspective as well, should be provided only upon request or in the final section, devoted to comments and suggestions.

Questions *(When answering the questions, you may tick more than one box)*

A) Definition and legal qualification of Artificial Intelligence system (AI system)

1) Is there a legal definition of AI system in your domestic law?

a) If so, could you please:

(1) quote it (in English and/or in your language)

(2) indicate the areas of law (e.g. criminal law, civil law, administrative law, labour law, etc.) it refers to

(3) indicate whether it is limited to a specific sector (e.g. smart contract legislation, automated decision-making: but please to refer to section III for the use of AI in criminal justice)

(4) clarify whether it refers to “products”, “services” and/or “agents”

(5) indicate whether it includes the concept of *Machine Learning*

(6) highlight whether any role is given to human intervention or control (e.g. is there any difference between autonomous and multi-agent AI systems and human-assisted AI system?)

b) If not, could you please indicate whether:

(1) there is a definition in the case-law

(2) it is possible to infer this definition from other legal sources

(3) your national lawmaker plans a legal reform to define this concept. If so, please provide a short description

(4) there is a definition elaborated by the scholars (e.g. in the field of criminal law, civil law, administrative law, labor law)

2) Is there a different legal definition of *Machine Learning* in your domestic law?

a) If so, could you please:

(1) quote it (in English and/or in your language)

(2) clarify the areas of law (e.g. criminal law, civil law, administrative law, labour law, etc.) it refers to

(3) indicate whether it includes the concept of AI

b) If not, could you please indicate whether:

(1) there is a definition in the case-law

(2) it is possible to infer this definition from other legal sources or soft law

3) Does your domestic law confer legal personhood or legal capacity to the AI systems?

a) If so, could you please:

(1) indicate what form of personhood is granted in specific areas of the legal system (e.g. criminal law, civil law, administrative law, labour law, tax law, etc.) and provide the legal references
(2) specify whether an AI system has autonomous or limited legal personhood, possibly under which conditions or in which sectors
(3) indicate whether the AI system is equalized to an artificial agent

b) If not, could you please indicate:
(1) whether the lawmaker in your country has planned/plans legal reforms to confer legal personhood upon AI systems
(2) whether scholars suggested to confer legal personhood or legal capacity upon AI systems

4) In regulating AI applications, which is the preferred approach? Is it a general one, applicable to all kinds of AI applications, or a sectoral one (e.g. applicable only to specific sectors, such as drones, facial recognition, autonomous driving, etc.)?

5) In which areas are complete automated and autonomous decision-making processes carried out by AI systems forbidden? If available, please refer to new proposals.

The following questions concern the general aspects of the offences related to the AI systems in your country (e.g. production, acquisition, distribution, dissemination, transmission, making available, offering, possession of AI systems; illegal acts committed against AI systems). More detailed questions on the mentioned offences will be discussed in the Section II of the Congress (Criminal Law – special part).

B) Existing criminal offences and criminalization

In your answer, please refer to legal reforms or law proposals, if available, and provide information on the criminal-policy strategy, the political and academic debate on the emerging legal goods and the most critical issues related to the AI system.

1) Have traditional offences and/or cybercrimes already been applied to illegal act committed by, through or against an AI system?

a) If so, could you please specify what offences have been applied, providing case law references and a brief description of them?

b) If not, could you please:
(1) indicate whether there are legal reforms or law proposals at issue
(2) indicate whether according to the legal literature there are offences already applicable to illegal acts involving AI system (if so, please specify)

2) Has your domestic law introduced new offences related to designing, programming, developing, producing, functioning or making use of AI systems?

3) Has your domestic law introduced new criminal offences concerning acts committed through or against an AI system?

a) If so, could you please:

   (1) quote them (in English and/or in your language)

   (2) indicate where they are regulated (e.g. special part of the Criminal Code, complementary legislation, etc.)

   (3) indicate the protected legal goods and/or fundamental rights

   (4) indicate whether and when the AI system can be considered the “subject” of the crime

   (5) indicate when the AI system can be considered the “object” of crime

   (6) indicate when the AI system can be considered the “instrument” of crime

   (7) highlight whether they are crimes of mere conduct, commission and omission offences, consummate offence, crimes with intent, etc.

   (8) specify who can be considered the possible perpetrator and/or victim of the new AI offences (e.g. producers/programmers/system engineers/developers/designers etc.)

   (9) indicate whether individual criminal liability requires a specific mental element and whether it involves also recklessness and/or negligence

   (10) could the legal persons be held liable for AI crimes committed by any person acting individually or having a leading position within the legal person? In this case, please describe the related imputation system

   (11) indicate whether there is any defence excluding the criminal responsibility of the perpetrator or of the legal person in order to avoid the risk of over-criminalization if the AI systems are produced, used or put on the market for legal purposes, e.g. for scientific or research reason

b) If not, could you please indicate:

   (1) whether the lawmaker in your country has planned/plans legal reforms to introduce new criminal offences related to AI systems (please quote them, in English and/or in your language)

   (2) whether reports or legal literature suggest the introduction of new criminal offences linked to AI systems (please provide also bibliographic references)

4) Does your domestic law provide for positive obligations for persons and/or legal person designing, developing, producing, testing, selling or distributing AI systems

a) If so, could you please indicate:

   (1) whether they are related to algorithmic transparency for patent and/or cybersecurity purposes

   (2) whether they imply a duty to control, possibly providing some examples

   (3) whether they lead to a form of strict liability

5) Does your domestic law provide for specific legal obligations for users of AI systems?

b) If so, could you please indicate:

   (1) whether they are surveillance or control obligations

   (2) whether these obligations lead to a form of strict liability

C) Applicability of Traditional Criminal Law Categories

1) According to your domestic law and/or jurisprudence, is the AI system considered as a "computer system" as defined by Article 1, lett. a) of Cybercrime Convention and/or Article 2, lett. a) of Directive EU/2013/40?

2) In your national system, are there other definitions applicable to AI systems despite not expressly referring to them?

3) Have the existing offences (see B 1.a) already been applied to illegal acts related or connected to AI systems (e.g. designing, programming, developing, producing, making use of an AI system)? If so, which traditional criminal law categories (e.g. action, omission, causation requirement, mental element, direct liability, etc.) have been applied or extended to these cases?

4) Are there specific problems with respect to the principle of legality?

5) Is analogy admissible? Has it been used in order to criminalize illegal acts related to AI systems?

a) If so, please provide, if available, examples describing paradigmatic cases and give a brief description of the criminal conducts (*actus reus*) and other elements of crime

6) Are the provisions concerning attempted crime applicable to AI-related crimes? Are there already cases of AI-related crimes qualified as attempted crimes?

7) Is it possible to apply existent rulings of joint-perpetration and participation in the commission of the crime to AI related crimes? Who can be considered a joint-perpetrator or participant in the commission of the crime (please refer to both human and artificial agents)? Is the "perpetration-by-another" liability model applicable?

8) Could legal persons be held criminally liable for AI-related crimes committed for their benefit in your domestic law? If so, please give some examples

9) Are forms of secondary liability applicable to AI-related crimes?

10) Is the wording of existing offences (in particular, computer crimes and cybercrimes) capable of including illegal acts committed through or against an AI system?

a) If so, briefly explain the technical-legal wording of the applicable offence(s) and make reference, if available, to some concrete cases

b) If not, briefly explain why the existing offences cannot be applied

11) Please clarify whether, for the purpose of criminal liability, the state of mind (e.g. *dolus*) on the part of the human agent who designed/programmed/developed/produced/circulated/marketed/used the AI system shall include the exact and concrete modus operandi of the AI system in committing the offence

12) Assuming that the crime is caused by the autonomous "conduct" of the AI system, could the person who designed/programmed/developed/produced/sold/used of the AI system be held criminally liable if he had knowledge of its autonomous learning and decision-making capacity?

a) If so, could you please indicate what the subjective prerequisite for criminality is (specific intent, general intent, direct intent, *dolus eventualis*, negligence, etc.). Could you provide some examples?

13) Are there in your domestic legal system cases of criminal liability for negligent or reckless conducts which can be applied when a crime or an illegal result is caused by conduct consisting in programming, producing or making use of an AI system?

a) If so, please point out the differences between negligent/reckless conducts carried out by designers/programmers/producers/sellers and by users or persons with a specific duty of care
Please provide examples describing paradigmatic cases, giving a brief description of criminal conducts (actus reus) of offences deemed to be applicable, and please specify if there are cases of corporate criminal liability as well.

b) Which legal (e.g. criminal, civil) relevance may "defects" or "flaws" in programming, producing or updating an AI system have? Have unforeseen or unforeseeable deviations in the AI decision-making process any legal relevance?

c) Are there in your domestic legal system any positive obligations (*Garantestellung)* the violation of which could be the ground for criminalizing not having avoided an illegal outcome resulting from the functioning of the AI?

d) Which is the standard of care required from the human agent in developing/programming/producing/selling an AI system?

e) Are there forms of strict liability (secondary liability or indirect infringement) for harm produced by AI systems?

D) Case law

1) Are there judgments or decisions concerning criminal conducts committed by means of, or to the detriment of, an AI systems?

a) If so, please briefly explain the cases
b) If not, please indicate the possible reasons for the lack of judgments (e.g. no complaints by the victims, limited employment of AI systems, etc.).

2) Are there judgments concerning AI systems, relevant for possible criminal consequences?

a) If so, please give some references

E) Adaptation of Traditional Criminal Law Categories and academic debate

1) With regard to cases involving AI systems in your country, does the case law or the academic debate point out legal issues concerning the traditional categories of the general part of the criminal law?

a) If so, among the following categories, which are those mostly discussed?

(1) *Actus reus*

i. Legal and traditional qualification of the autonomous or independent AI systems agency as "conduct" of the crime
ii. Legal and traditional qualification of the autonomous or independent AI systems agency in relation to the human conduct
iii. Influence of the autonomous AI systems agency on the chain of causation

(2) *Causality*

i. Interruptions of the chain of causation between the AI systems agency and the crime due to errors in programming/producing/maintaining/updating/using
ii. Use of risk-based legal criteria for the objective charge of the crime to the human agent
iii. Interruptions of the chain of causation between the human agent's conduct and the crime due to any anomaly or unpredictability of the output produced by the AI system (e.g. so-called black box problem)

(3) *Principle of culpability* (nullum crimen sine culpa) *and mens rea*

i. Compliance with the principle of culpability when the output causing the harm generated by the intelligent machine is neither wanted nor predictable by the human agent
ii. Compliance with the principle of culpability when an AI system is intentionally used by a human agent as a tool but the AI system carried out an offence different from the one wanted by the human agent

(4) *Criminal participation and attempted crimes*

i. Could a human agent be liable for participation in a crime committed or for an harmful result caused by an AI systems or AA? Also for a crime different from the one intended by some of the participants, because of the autonomous and unpredictable functioning of the artificial agent
ii. End of the preparatory phase and starting of the phase of execution: which acts performed by an AI system or by AA can be considered as attempted crime?

(5) *Liability of legal persons*

i. Necessary adjustments of the legal principles on criminal liability of legal persons when they are involved in AI-related crimes

ii. Necessary adjustments of policies and preventive measures within private organizations in order to guarantee a correct and regular use of AI systems

2) Which possible solutions have been elaborated to address the questions posed by the unpredictability of the functioning of intelligent systems, especially when the AI system functioning causes an illegal result?

Please, only answer if you need to add something to the answers given in the previous questions.

3) Did the legislator or the academic community propose a possible form of criminal liability or a direct sanctioning of AI systems or AA?
If so, could you please report which form/mode of liability is proposed? (e.g. *direct liability, command responsibility, perpetrator-by-another, natural probable consequence*)

Please describe any proposal made in literature, highlighting the following aspects:

a) Elements qualifying the "conduct" of the artificial agent as "conscious and voluntary" (in compliance with the voluntary act requirement)

b) Forms of culpability attributed to AI systems justifying their legal punishment or sanctioning

c) Possible extension of the traditional categories of intent and negligence or their equivalents

d) Liability for participation in a crime or for attempted crime committed with the use of AI systems or AA

e) Forms of objective liability/strict liability for AI systems

f) Types of sanction (criminal punishments or others) to punish AI systems

g) Measures aiming at avoiding the lack of responsibility of human agents who develop/program/produce/sell AI systems

F) Alternatives to criminalization and non-criminal sources

1) Does domestic law use civil and/or administrative sanctions (e.g. payment of damages, closing of enterprise, etc.) in order to fight abuses of AI systems or harm caused by them?

a) If so, what is their relationship with criminal punishments?

2) Is there any form of compulsory civil insurance for damages resulting from the use of an AI system?

3) Are there other technical means for combating harm and/or abuses of AI systems? (e.g. re-programming of the AI system software; destruction of the artificial agent; or similar)?

4) To what extent are users expected to protect themselves (e.g. through security measures in using AI systems; intervention obligations in case of danger, etc.)? What legal relevance could reasonable self-protection of users have in crimes related to AI systems? Could it be a defence for producers accused of an AI-related crime?

5) To what extent is the product liability legislation applicable to emerging AI employment? Is there a specific regulation for AI systems' testing phase? Alternatively, does the law require simulation obligations?

Please include in your answer any proposal under discussion that has not entered into force yet.

6) Are there rules or principles (privacy by design, by default, etc.) on cybersecurity and data protection relevant to criminal aspects related to the design/production/use/development of AI systems?

7) What is the role of the human agent? What degree of control over the AI system is granted or required?

8) Is there a standardization of technical rules for designers/programmers/developers/producers of AI systems (or is it in the process of being defined)?

a) If so, could you please indicate:
   (1) By which institutions or bodies?
   (2) Through which instruments?

G) Final evaluations and future developments

Please, use the box below for further suggestions and observations, concerning current trends on criminal policy strategy regarding AI-related crimes, lack of legislation, legal reforms, law proposals, reports and statistics on the incidence of AI-related crimes, case law, legal debate in your country, etc.

List of topics for special reports (Section I)

1. Positive obligations (Garantestellung) grounding the criminal responsibility for not having avoided an illegal result connected to the AI functioning

2. Legal relevance of unforeseen or unforeseeable deviations in the AI decision-making process

3. Criminal liability of legal persons for AI-related crimes committed for their benefit

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

Questionnaire - Section III

AI and Administration of Justice: Predictive Policing and Predictive Justice

Prof. Juliette Lelieur

Introduction

According to a well-established tradition of the AIDP, the third section of international congresses deals with procedural aspects, that is, how criminal law is enforced in various legal systems. Concerning the impact of artificial intelligence (AI) on the administration of justice more specifically, it is still limited in some jurisdictions but abundant in others. In general, the use of AI-based systems is growing in many parts of the world, particularly due to a strong business interest in marketing these new technologies. The industry is therefore encouraging public authorities to help test, monitor and improve these systems on a large scale, for instance through public-private partnerships. In return, it is promising impressive results, claiming that AI-based systems will improve security and reduce crime by making policing more effective (predictive policing) and will introduce neutrality and accuracy, thereby eliminating judicial subjectivity and inconsistent judicial decisions (predictive justice).

Technologies based on AI may be used at many different stages of the criminal process: to deter or prevent crime when possible, to investigate crimes and sentence offenders. AI-based systems may be used by **traditional law enforcement authorities** such as the police, investigation and judicial authorities, criminal courts, and the authorities carrying out sentences. In addition, **administrative authorities and regulators** that are authorized to impose punishment can use such systems to gain time and efficiency in elucidating complex breaches of law and to punish them when appropriate. This may concern for instance breaches of antitrust law or banking or financial market regulations, tax fraud or other large-scale fraud, non-compliance (for example with anti-bribery or anti-money laundering regulations), etc. National rapporteurs are therefore encouraged to adopt a **broad conception of criminal justice**. They are urged to analyse and assess the use of AI-based systems in any legal field in which issues of **preventing, deterring, and investigating criminal offences and similar breaches of law**, as well as of **sentencing natural or legal persons,** arise.

For the purposes of the 21st Congress of the AIDP, general rapporteurs have agreed on a **common definition of artificial intelligence** to facilitate discussion in all four sections of the Congress. It is therefore recommended that national rapporteurs refer to the definition provided by the High-Level Expert Group of the European Commission in 2019[3]:

[3] https://www.aepd.es/sites/default/files/2019-12/ai-definition.pdf

> Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans[4] 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.
>
> As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).

When talking about AI-based systems, the terms “predictive policing” and “predictive justice” refer their alleged ability to predict or forecast the future and thus enable law enforcement and judicial authorities to align their policing strategy and rulings with these predictions. In fact, however, AI techniques merely **calculate probabilities** and mostly rely on **risk assessment tools.** They do so by processing a tremendous amount of data using algorithms set according to various parameters to deliver a **mathematical result**.

In some cases, AI has not made any spectacular changes. For instance, one purpose of algorithm-based **predictive policing** is to determine the locations where and times of day (or night) when crimes are most likely to be committed. This does not fundamentally differ from the experienced police officer’s intuition about the probable behaviour of offenders, except that the calculation is made much more quickly and can therefore be applied on a broader scale. It is supposed to help increase police presence at the right place and time so they can prevent crime or catch the perpetrators in *flagrante delicto*. Predictive policing also aims to identify people, including potential victims in order to protect them. In addition, AI-based systems enable the police to target groups of individuals who might be responsible for a crime that has already been committed, for example by analysing digital social networks. Lastly, these systems aim to identify suspects so the police may question and possibly arrest them. Here, the new technology not only provides investigative assistance, it alerts the police as to whom to surveil and where, before any crime is committed. This breaks with the major rule of criminal procedure according to which law enforcement authorities must base their investigation on a suspicion (and not vice-versa). The consequences in terms of investigative measures are meaningful, especially regarding civil liberties and human rights.

[4] Humans design AI systems directly, but they may also use AI techniques to optimise their design.

The term **predictive justice** covers different practices. Historically speaking, risk assessment tools were used first – at least in the United States – to assess the risk of recidivism of offenders. Updated to incorporate AI-based technology, these tools help judges decide on release, probation, parole, and supervision. Their primary purpose is to predict human behaviour, just as risk assessment tools do for predictive policing. However, they also suggest how cases should be decided, which shows that AI-based systems are able to provide assistance with the application of law.

More generally, a new generation of AI-based systems has been developed to calculate the probability of particular outcomes. These systems are already widely used in various legal disciplines, such as insurance law and several other branches of civil law. **Legal Tech** (technology at the service of law) is progressively making inroads into the area of criminal justice. Theoretically speaking, AI-based systems can be used to guide judicial decision making (whether to prosecute, order an alternative measure, or dismiss a case), or to calculate the amount of a deposit or fine or the length of pre-trial custody, for example. These systems thus tend to assist judicial authorities and judges in exercising the power to prosecute, judge or sentence a person – and may partly replace them in the future. This is a very disconcerting perspective for at least two reasons. First, from an epistemological point of view, it implies that the outcome of a case is not the result of the centuries' long tradition of legal reasoning but of a mathematical calculation. Second, there is a risk that judges will hide behind the algorithm and surreptitiously delegate the power to decide on other people's lives to software.

Furthermore, as some national rapporteurs might be able to illustrate on the basis of their country's experience, start-ups may either provide legal advice to lawyers' offices as subcontractors or directly offer AI-calculated outcomes to parties to criminal proceedings. Using rapid, AI-based calculations may become more and more popular, especially for settlement negotiations (and possibly, one day, plea bargaining). Again, the potential consequences are manifold. Not only does Legal Tech challenge well-established legal professions, it could also be the source of disparity between litigants: while the rich will be able to afford lawyers, the poor may have to be satisfied with software-produced "legal" advice or dispute resolution.

Artificial intelligence also affects a further component of criminal justice: the overarching **law of evidence**. It is not surprising that AI-based systems contribute to the collection of evidence. Forensic and law firms use them for complex criminal business law cases in the context of so-called internal investigations in order to sift through an enormous quantity of documents and e-mails to extract evidence of the crime and thus help the defendant, usually a legal person, to cooperate with the prosecution services by self-reporting charges against itself. AI may also assist social workers or judicial authorities with, for instance, the collection of relevant information for character reports about the suspect. In addition, AI-based systems produce evidence themselves, through techniques like facial and voice recognition. The question whether "AI evidence" is reliable and trustworthy in a criminal trial is obviously decisive. Moreover, which categories of evidence will such information fall into under national law: testimony – from a machine – or technical expert evidence? Will it be necessary to create new categories or concepts for implementing ad-hoc rules on the admissibility of evidence? It is moreover unclear whether information provided by AI-based systems used by non-investigative authorities may serve as evidence in criminal proceedings. An appropriate example is the drowsiness detection and distraction warning system embedded in an automated vehicle, which monitors human behaviour (e.g. evaluates the driver's ability to retake control of the vehicle where necessary) to enhance safety. Under what conditions – guaranteeing due process – may judicial authorities use the information given by the software robot as a charge against a particular driver? Finally, if we indulge in a bit of science fiction, judges in the future might rely on AI-based systems for an assessment of the evidence based on a calculation of the probability that the defendant is guilty. This would seriously challenge the presumption of innocence. If, for example, an AI-based system processing evidence concludes that there is a 97% probability that a suspect committed the crime, will the criminal court still follow the *in dubio pro reo* principle and acquit, and will an acquittal under such circumstances be perceived as just?

Layout of the questionnaire:

I. Predictive policing
II. Predictive justice
III. Evidence law

The **objectives of the national reports** based on this questionnaire are the following:

- Provide an insight into whether, how and for what purposes AI-based systems are used in national criminal justice systems (national practice with respect to AI-based-systems)
- Describe legal rules, case law and soft law related to the use of AI-based systems by law enforcement authorities (normative framework for using AI-based systems)
- Discuss the aptitude of currently applicable national rules to meet the challenges AI-based systems pose to the general principles of constitutional law and rules of criminal procedure (fairness, due process, presumption of innocence, rights of defence, right to non-discrimination, right to privacy, admissibility of evidence, etc.)
- Describe the current schools of thought among national legal commentators concerning the impact of AI in criminal justice systems

As national reports may be published in the RIDP *(Revue internationale de droit pénal – International Review of Penal Law),* national rapporteurs should not merely answer one question after another. They should instead provide the AIDP with a **self-standing report** where answers to the questionnaire are presented in a **fluent, articulate text**. National reports should be approximately 30 pages long.

When questions or parts of the questionnaire are not relevant for your country, please indicate it briefly in the report and ignore the question(s). If, on the contrary, the questionnaire does not address issues that are of interest for your report, please contact the general rapporteur (juliette.lelieur@unistra.fr) before introducing them. If it is easier for you to handle the questions in a different order, feel free to do so. However, please **keep the general layout of the questionnaire** (I. II. III. / A. B. / 1.2.3.) when organizing your report.

Thank you for your participation!

I. PREDICTIVE POLICING

1. National practices

General questions

1.1. Is there a definition of "predictive policing" in your country? If so, please provide it and indicate its date and origin.

1.2. Are AI-based systems used for predictive policing in your country? If so, please indicate the names of these systems, the first year they were used, and the company or companies (national or foreign) that produce them.

1.3. If AI-based systems are not used for predictive policing in your country but there are plans to use them in the future, please answer the following questions in the light of those plans. If the police in your country have refrained from procuring AI-based systems on the basis of negative findings made abroad, please indicate this. Was there a political decision – at the national or local level – not to rely on AI-based systems for policing activities? What were the arguments for this decision?

1.4. Please briefly describe how the AI-based systems used in your country work from a technological perspective. [5]

1.5. What kind of data are used by these AI-based systems? [6]

1.6. In what areas are these AI-based systems used (urban areas, suburbs, problem neighbourhoods; specific business or financial markets, local or regional markets, multinational companies; territories where minority population is living or where important national interests are at stake, etc.)?

1.7. What kind of criminal activities do the AI-based systems focus on? [7]

1.8. What type of organizations rely directly on AI-based systems? [8]

1.9. What kind of concrete results do AI-based systems produce? [9]

1.10. How are these results used to improve policing? Have the results provided by AI-based systems led to any changes in policing methods?

1.11. What are the political or socio-economic incentives – at the national or local level – for using AI-based systems? [10]

1.12. What are the concrete objectives pursued by using AI-based systems.[11] Is there a difference between the stated objectives (see question 1.11.) and the objectives actually pursued?

1.13. How are AI-based systems for predictive policing perceived by the public in your country? How are they presented in the media? What is the opinion of police officers, law professors, writers, philosophers, intellectuals?

[5] Machine learning, deep learning, machine reasoning, etc.

[6] Crime data, police files, open sources, data collected for investigations, protected personal data, etc.

[7] Street crime, property crime, violent crime, terrorism, fraud, economic and financial crime, cybercrime, political crime, etc.

[8] Police, private companies working for the police, private security companies, regulators, etc.

[9] Determining location and time where crime is likely to happen, profiling people who are likely to commit a particular type of crime, profiling groups or networks where crime may be committed, etc.

[10] Policy based on safety and security promises, need to reduce policing costs, need to support innovative high-tech industry, etc.

[11] To save time, improve effectivity, reduce costs, etc.

Assessment of reliability, impartiality and effectiveness

1.14. Has the reliability of the AI-based systems used for predictive policing in your country been evaluated? [12] If so, was the assessment done by the authority using the system or by third parties? [13] What were the findings and were they findings taken into consideration by the organizations using the AI-based systems?

1.15. Has the impartiality of the AI-based systems used in your country been evaluated? [14] If so, was the assessment done by the authority using the system or by third parties? [15] What were the findings and were they findings taken into consideration by the organizations using the AI-based systems?

1.16. Has the effectiveness of using AI-based systems for policing/reducing crime been evaluated in your country? If so, was the assessment done by the authority using the system or by third parties? [16] What were the findings and did lead to approbation or criticism in your country? [17]

1.17. Have any public authorities that have experimented with using AI-based systems for predictive policing in your country decided not to use them in the future? If so, why?

2. Normative framework

Law and soft law

2.1. Are there national legal rules concerning AI-based systems for predictive policing in your country? If so, please briefly describe this legislation and its main objectives (keep the details about the content for questions 2.8 to 2.15). If not, please indicate whether your country is considering adopting such legislation and what are the arguments.

2.2. Do government memos, ministerial recommendations or other normative instruments produced by the executive authorities of your country deal with AI-based systems for predictive policing? If so, please describe them briefly and explain their main objectives.

2.3. Are there soft law sources, private sector regulations [18] concerning predictive policing in your country? If so, please briefly describe them and explain their main objectives.

2.4. Does your national criminal justice system refer to international or regional normative instruments concerning the use of AI-based systems for predictive

[12] Errors, false positives/negatives, etc.

[13] The company that produced the AI-based system, the industry, public or private research institutions, or independent experts, etc.

[14] Bias, inclusion, etc.

[15] See note 11.

[16] See note 11.

[17] E.g. the AI-based system leads to a more effective use of police human resources or makes it possible to deter crime that wouldn't be deterred otherwise; predictive policing through AI-based systems is useless or even counterproductive.

[18] Ethics charters, codes of conducts, best practices guides, etc.

policing? If so, please mention these instruments and describe their impact on policing in your country.

Case law

2.5. Have the judicial authorities[19] or regulators of your country issued decisions in cases in which AI-based systems were used for predictive policing? In what context, and what decisions did they issue? How did legal commentators respond?

2.6. Have the criminal courts of your country decided cases in which AI-based systems were used for predictive policing? How did they rule in those cases and how did legal commentators assess those rulings?

2.7. Have the civil, administrative or constitutional courts – or other independent authorities – issued decisions in cases in which AI-based systems were used for predictive policing? How did they decide and how did legal commentators assess those decisions?

Substantive guarantees

2.8. Are the guarantees discussed in questions 1.14 to 1.16 (reliability, impartiality, effectiveness) addressed by law in your country? If so, please describe the normative instruments providing for these guarantees.[20] May victims be compensated? Feel free to elaborate on elements that are significant.

2.9. Is there an obligation for AI-based systems to be certified or labelled before they can be used for predictive policing? What are the substantive conditions for obtaining certification or a label? Which (independent) authority is authorized to issue the certificate or label? What are the procedures and who verifies compliance?

2.10. Are the authorities using AI-based systems for predictive policing in your country obliged to continuously monitor and adjust them?

2.11. How is transparency about the technological functioning of AI-based systems guaranteed?[21] Are companies that produce AI-based systems allowed to refer to unclear mechanisms (“black box”) or claim the technology is a trade secret and refuse to provide explanation of how their product works?

2.12. Are the companies producing AI-based systems accountable for the results they provide?[22] If so, how are they held accountable?

2.13. How do the organizations that use AI-based systems for predictive policing in your country guarantee transparency about their practices?

2.14. Are these organizations accountable for the actions they undertake based on indications provided by AI? How is accountability concretely guaranteed? If, for instance, a person is arrested on the basis of an incorrect AI-based system calculation,[23] what happens?

[19] E.g. prosecution services, tribunal deciding on investigation measures.

[20] Hard law, soft law, case law.

[21] Peer review, auditing systems, etc.

[22] For instance, because of an incorrect calculation a person is identified as a criminal although she/he is not.

[23] She/he did not commit the crime.

2.15. What other substantive obligations are imposed on the police authorities that use AI-based systems? Are there any particular recommendations they are encouraged to follow? Feel free to discuss any rule that is relevant for the accuracy and interest of your report.

3. General principles of law

3.1. Is there a discussion in your country about protecting the *right to equality* – or the right to non-discrimination – with respect to AI-based systems used for predictive policing, especially due to the observation that processing methods may reproduce or aggravate human discrimination? What positions do legal commentators take?

3.2. Is there a discussion in your country about protecting the *right to privacy* with regard to AI-based systems used for predictive policing? Do the normative instruments provide satisfactory protection in this regard? Are there ways to challenge unlawful access to and use of personal data? May victims be compensated? What positions do legal commentators take?

3.3. Is there a discussion in your country about protecting the *right to liberty and security* of persons against AI-based systems used for predictive policing? If so, please elaborate on normative instruments, case law and any other significant measures. What positions do legal commentators take?

3.4. Is there a discussion in your country about respecting the *principle of proportionality* in using AI-based systems for predictive policing? Have measures been taken to safeguard proportionality? What positions do legal commentators take?

3.5. Is there a discussion in your country about *procedural legality*, that is to say the requirement that enforcement authorities base their investigation on a suspicion (and not vice-versa) respective to predictive policing with the use of AI-based systems?

3.6. Is there a discussion in your country about *principles of constitutional law* with regard to using AI-based systems for predictive policing? Feel free to discuss any principle that is relevant for your report.

II. PREDICTIVE JUSTICE

1. National practices

General questions

1.1. Is there a definition of “predictive justice” in your country? If so, please mention it and indicate its date and origin.

1.2. Are AI-based systems used for predictive justice in your country? If so, please indicate the names of these systems, the first year they were used and the companies producing them (national or foreign companies).

1.3. If AI-based systems for predictive justice are not used in your country but there are plans to use them in the future, please answer the following questions in the light of those plans. If any of your country's criminal justice authorities have refrained from procuring AI-based systems for predictive justice, for instance on the basis of negative findings made abroad, please mention it. Was there a political decision – at national or local level – not to rely on AI-based systems in the criminal justice system? What were the arguments for this decision?

1.4. Since when and for what purposes are AI-based systems used in your country? Please explain whether these systems are principally or exclusively risk assessment tools [24] or whether they produce judicial decisions. [25] If they do both (risk assessment and suggested legal outcomes for the case), please indicate this.

1.5. Please briefly describe how the AI-based systems used in your country work from a technological perspective. [26]

1.6. What kind of data are used by these AI-based systems? [27]

1.7.Who relies directly on the AI-based systems for predictive justice? [28]

1.8. If public authorities use AI-based systems for predictive justice in your country, which decisions do they in fact take on the basis of AI-based systems calculations? [29]

1.9. Are any of your country's judicial authorities obliged to use AI-based systems at any stage of the criminal process? If so, which ones and why? Does the digital industry's lobbying play a role on mandatory use of AI-based systems?

1.10. What are the political or socio-economic incentives for using AI-based systems? [30]

1.11. What are the objectives of those who use AI-based systems for predictive justice? [31] Is there a difference between the stated objectives (see question 1.10.) and the objectives actually pursued?

1.12. If private companies or individuals use AI-based systems to calculate judicial decisions, in what types of decisions do the systems' predictions differ from the criminal justice system's decisions? [32]

[24] Calculation of the probability that a natural or legal person will exhibit a particular "behaviour": re-offending/recidivism, dangerousness, non-compliance, etc.

[25] Calculation of probabilities, based on a legal situation, to predict a judicial decision: decision-producing software, chatbots, robot lawyers, etc.

[26] Machine learning, deep learning, machine reasoning, etc.

[27] Crime data, data collected for investigations, protected personal data, legal data, government and/or soft law data, case law data at a national level or from local tribunals, open sources, etc.

[28] Prosecution services, judges, social workers, prison system, regulators, lawyers, forensic experts, private operators advising companies in view of settlement or other negotiations; start-ups hired by lawyers to provide advice or that suggest alternatives to criminal prosecution, etc.

[29] Sentencing, release, probation, parole, supervision; non-prosecution decision, decision on compliance obligations, etc.

[30] Policy of harsher/softer criminal justice response to individuals; government's inability to meet the costs of the criminal justice system or desire to reduce these costs; desire to support innovative high-tech industry, etc.

[31] To increase the neutrality/objectivity of judicial decisions, provide for better judicial consistency, individualize decisions to fit each litigant; save time and human resources.

[32] Decisions on prosecution, on the amount of penalties, on victims' compensation, etc.

1.13. Do these predictions affect the decisions issued within the public criminal justice system or will the case be resolved outside of that system?

1.14. Are offers for alternative dispute resolution based on AI calculations popular in your country? For litigation involving small or large amounts?

1.15. How are AI-based systems for predictive justice perceived by the public in your country? How are they presented in the media? What do legal practitioners, legal commentators, writers, philosophers, and intellectuals say about them?

Assessment of reliability, impartiality, equality, adaptability

1.16. Has the reliability of the AI-based systems used in your country for predictive justice been evaluated? [33] If so, was the assessment done by the authority using the system or by third parties? [34]

1.17. Has the impartiality of the AI-based systems used in your country for predictive justice been evaluated? [35] If so, was the assessment done by the authority using the system or by third parties? [36]

1.18. What are the findings of the studies or surveys mentioned in questions 1.17 and 1.18? Could errors, bias etc. be identified? If so, what were they? Were the findings taken into consideration by the authorities using AI-based systems?

1.19. Have AI-based systems used for predictive justice been found to provide more neutrality in the criminal justice system than humans do?

1.20. Have AI-based systems been found to provide more consistency in criminal justice decisions than humans do? It is possible to state that they enhance equality between litigants?

1.21. Have AI-based systems been found to provoke a general change in responses to crime or other violations of the law? If so, are these responses harsher or softer?

1.22. Have AI-based systems been found to adapt to new situations? Do they recognize new facts and take them into account to produce decisions that depart from previous case law?

1.23. Have any public authorities or private entities that have experimented with AI-based systems for predictive justice purposes in your country decided not to use them in the future? If so, why?

2. Normative framework

Law and soft law

2.1. Are there national legal rules governing the use of AI-based systems for predictive justice in your country? If so, please briefly describe this legislation

[33] Errors, false positives/negatives, etc.

[34] The company that produced the AI-based system, the industry, public or private research institutions, or independent experts.

[35] Bias, inclusion, etc.

[36] See note 32.

and its main objectives (keep the details for questions 2.7 to 2.18). If not, please indicate whether your country is considering adopting such legislation and what the arguments.

2.2. Do government memos, ministerial recommendations or other normative instruments produced by the executive authorities of your country deal with AI-based systems for predictive justice? If so, please briefly describe them and explain their main objectives.

2.3. Are there soft law sources[37] concerning predictive justice in your country? If so, please briefly describe them and explain their main objectives.

2.4. Does your national criminal justice system refer to international or regional normative instruments concerning AI-based systems for predictive justice? If so, please cite these instruments and describe their impact on predictive justice in your country.

Case law

2.5. Have the criminal tribunals or courts of your country been confronted with AI-based systems used for predictive justice? In what context and how did they rule? What did legal commentators say about these rulings?

2.6. Have the civil, administrative or constitutional courts – or other independent authorities – been confronted with AI-based systems used for predictive justice? How did they rule and how did legal commentators assess their rulings?

Substantive guarantees

2.7. Are the guarantees discussed in questions 1.16 to 1.23 (reliability, impartiality, equality, and adaptability) addressed by law in your country? If so, please describe the normative instruments providing for these guarantees[38]. Feel free to elaborate on elements that are significant in your country.

2.1. Is prior authorization required to market an AI-based system for predictive justice? If so, does the law of your country[39] impose technological requirements on producers? Are producers obliged to include criminal justice professionals while designing the software? Do they have to regularly monitor and update the software?

2.8. Must AI-based systems for predictive justice be certified or labelled? What are the substantive conditions posed for issuing a certificate or label? Which (independent) authority is authorized to issue a certificate or label? What is the procedure and who verifies compliance?

2.9. Are the professionals of your national criminal justice system who rely on AI-based systems trained to review the data used for producing judicial decisions and to review these decisions themselves at any time? If possible, please indicate the probability that the judge, judicial authority, regulator, etc. will follow the AI-based system's suggestion as to how to apply the law.

[37] Ethics charters, codes of conducts, best practices guides.

[38] Hard law, soft law, case law.

[39] See note 36.

2.10. How is transparency about the technological functioning of AI-based systems guaranteed? [40] Are companies allowed to refer to unclear mechanisms ("black box") or claim the technology is a trade secret and refuse to be transparent about how their product works?

2.11. How is transparency about using AI-based systems for predictive justice guaranteed in your country? Must individuals be informed case by case about the use of AI-based systems by the judicial authorities, regulators, etc. deciding on their legal situation? Who has to provide them with this information? Do the other parties to the proceedings have to be informed, too, or is the information public?

2.12. Must the parties also be informed of the substantive results provided by AI calculation? Must they be informed of the percent of probability attained and the possible errors arising from the calculation?

2.13. Do the authorities that use AI-based systems for predictive justice in your country have to inform individuals whose cases are handled with AI assistance about the data that were used by the algorithmic calculation? Do they have to do so under oath?

2.14. Do they have to provide those individuals with information on the scientific process of the AI calculation – under oath?

2.15. Are the companies producing AI-based systems for predictive justice accountable for the results they provide? If so, how is accountability guaranteed?

2.16. Are the public institutions that use AI-based systems for predictive justice accountable for the actions they undertake based on indications provided by AI? Concretely, how is accountability guaranteed? If, for instance, conditional release is given to a person on the basis of an incorrect AI-based system calculation[41], what happens?

2.17. Are the professionals of your country's criminal justice system who rely on AI-based systems trained to review the data used to produce judicial decisions and to review those decisions themselves at any time?

2.18. What other substantive obligations are imposed on those who use AI-based systems for predictive justice purposes in your country? Are they encouraged to follow any particular recommendations? Feel free to discuss any rule that is relevant for the accuracy and interest of your report.

3. General principles of law

3.1. Is there a discussion in your country about protecting the *right to equality* – or right to non-discrimination – with regard to AI-based systems used for predictive justice, especially due to the observation that processing methods may reproduce or aggravate human discrimination?

3.2. Is there a discussion on whether the *judge's independence* is affected when a judge or a court is assisted by AI-based systems? Are there special means or methods to guarantee the judge's independence while using AI? [42]

[40] Peer review, auditing systems, etc.

[41] She/he does re-offend.

[42] Collegiality, ethics committee, supervision, etc.

3.3. Is there a discussion on the need to recognize the *right of access to a human judge*, at least for some types of cases?

3.4. Is there a discussion about protecting the *presumption of innocence* when an AI-based system is used to establish the probability that a person is dangerous or is likely to reoffend?

3.5. Is there a discussion about guaranteeing the *right to a fair trial* with regard to AI-based systems used for predictive justice, including equality of arms and an adversarial process? How can the use of an AI-based system for predictive justice be challenged by law? Can only the parties to a case appeal, or can third parties affected by the use of the AI-based system also appeal? [43]

3.6. Is there a discussion about guaranteeing the *right to defence* by people whose legal situation is handled with assistance from AI-based systems? Does your country provide for appropriate means to defend oneself against an algorithmic calculation? If so, please elaborate on that question and highlight legal commentators' thoughts.

3.7. Is there a discussion on whether the *right to appeal* is properly guaranteed when AI-based systems are used on first instance as well as at appeal level, in particular when the same AI-based system is relied on?

3.8. Are there specific ways to challenge an AI calculation, including the scientific validity of the algorithm and the selection of data? Are there specific conditions for obtaining judicial review of an AI-based decision?

3.9. Is there a discussion about *principles of constitutional law* with regard to using AI-based systems for predictive justice? Feel free to discuss any principle that is relevant for your report.

3.10. Is there an epistemological discussion about replacing legal reasoning with mathematical calculation for criminal justice purposes? If so, is this discussion linked to a general principle of law? What are the arguments of legal commentators and intellectuals, and of legal practitioners?

3.11. Is there a discussion about the possibility that criminal justice – or parts of it – will be privatized through the development of Legal Tech in your country?

3.12. Is there a discussion about equality of litigants before the criminal justice system, and especially on whether expensive human-made decisions will be reserved to those who can afford them, while inexpensive, software-made decisions will be available for everyone?

III. EVIDENCE LAW

1. Evidence gathering through AI-based systems

1.1. Are there AI-based systems used in your country to process and sort through large quantities of documents and communications, such as e-mails from a firm's numerous employees, to gather evidence of a crime or other violation of the law? [44]

[43] Privacy/family rights violations or reputational harm to individuals/companies.

[44] E.g. TAR/CAL Relativity.

1.2. If so, who uses them? [45] Is there a particular type of procedure where the use of such AI-based systems is especially prevalent? [46]

1.3. Are there AI-based systems used to extract data from mobile devices and decode and analyse that data to gather evidence? [47] If so, who uses them and in what circumstances?

1.4. Are there other kinds of AI-based systems used to help investigators gather evidence of a crime or other unlawful conduct? If so, who uses them and in what circumstances?

1.5. Is there a normative framework governing the AI-based systems referred to in questions 1.1, 1.3 and 1.4 and their use over the course of the criminal process? If so, please briefly describe the existing (or planned) regulation(s) and indicate whether any limitations or conditions have been placed on using these systems.

1.6. In particular, explain whether the defendant is provided with information regarding the particular AI-based system used, and whether he/she can easily and efficiently challenge the way in which such evidence was collected.[48]

1.7. Have any courts been confronted with the use of AI-based systems to gather evidence? If so, please elaborate on the rulings given by those courts.

1.8. Is there any legal commentary on using AI-based systems to gather evidence? If so, please give an insight into this literature. In particular, if no legal framework exists in your country, please indicate whether scholars are in favour of regulation in this area.

2. Evidence produced by AI-based systems

2.1. Are any AI-based systems that perform facial recognition and/or voice recognition used in your country to produce evidence for the purpose of criminal justice? If so, by whom and under what circumstances?

2.2. Do AI-based systems produce other kinds of evidence for the purpose of criminal justice? If so, what kinds of evidence do these systems produce and who uses it?

2.3. Is there a normative framework governing evidence-producing AI-based systems and their use over the course of the criminal process? If so, please elaborate on any existing or planned regulations and especially on any limitations or conditions placed on AI-produced evidence, and answer questions 2.4 to 2.9. In case no legal framework exists, please indicate whether scholars are in favour of a regulation and why.

2.4. How are the reliability and neutrality of AI-based systems producing evidence for the purposes of criminal justice guaranteed by law?

2.5. How does your legal system guarantee that defendants can effectively challenge AI-produced evidence? [49]

[45] Criminal justice authorities, forensic firms, law firms, etc.

[46] Settlement negotiations, deals, etc.

[47] E.g., UFED Ultimate-Cellebrite.

[48] Equality of arms, rights of defence.

[49] Equality of arms, rights of defence.

2.6. Does AI-produced evidence fall into a specific category of evidence in your legal system? [50] What are the consequences in terms of criminal procedure law?

2.7. May information provided by AI-based systems used by non-investigative authorities serve as evidence in criminal proceedings? [51]

2.8. Is there a normative standard for the admissibility of AI-produced evidence? If so, is this standard different from the common standard for admissibility of evidence in your country?

2.9. Are there specific exclusionary rules concerning AI-produced evidence? If so, please present these rules and explain whether they differ from the common rules on admissibility in your national legal system.

2.10. Is your country a party to a treaty or other type of regional or international agreement on the admissibility of digital evidence? If so, please specify which agreements and elaborate on the consequences for the admissibility of AI-produced evidence in your country.

2.11. Have the courts of your country been confronted with AI-produced evidence? If so, please cite the existing case law and elaborate on the ruling given by the courts.

2.12. Is there significant academic debate in your country regarding the use of AI-based systems for producing evidence and the admissibility of AI-produced evidence in criminal proceedings? If so, please give an insight into the relevant literature.

3. Evidence assessed through AI-based systems

3.1. Are AI-based systems used in your country to help judges, courts or regulators assess criminal evidence?

3.2. If so, does the AI-based system evaluate the probative value of single pieces of evidence or does it assess the overall conclusive force of the evidence as a whole? Please briefly describe how the AI-based system works from a technological point of view.

3.3. Is it conceivable in your country that in a criminal trial, a person’s guilt would be assessed with help of an AI-based system? Is there significant academic debate on this issue, including with regard to the presumption of innocence?

3.4. Are there rules (or drafts of normative instruments) on using AI-based systems for assessing pieces of evidence or for assessing the culpability of a person during a criminal trial? If so, please elaborate on these rules.

3.5. Have any courts been confronted with judicial decisions or criminal judgements for which the evidence was assessed with the help of AI-based systems? If so, please cite the existing case law and elaborate on the rulings given by the courts.

[50] Findings/statement, testimony, expert evidence, etc.

[51] See for example the drowsiness detection and distraction warning system embedded in an automated vehicle referred to in the introduction to this questionnaire.

List of topics for special reports (Section III)

1. The role of AI-based systems in negotiated proceedings

2. Certification of AI-based systems used in criminal litigation

3. Fundamental procedural rights v. AI-based systems in criminal justice: is there a need for a right to a human justice?

4. Cross-border admissibility of AI-evidence

Questionnaire - Section IV

International Perspectives on AI: Challenges for Judicial Cooperation and International Humanitarian/Criminal Law

Prof. Milena Sterio

Objectives and Scope

The purpose of this Questionnaire is to solicit national responses regarding the following issue related to Artificial Intelligence (AI): the use of AI and its impact on International Humanitarian Law and on International Criminal Law. This Questionnaire briefly summarizes relevant legal issues, and then lists a series of questions related to this important legal issue.

I. International Humanitarian Law and International Criminal Law

A) Summary of Issues

- The use of Automated Weapon Systems (AWS) raises legal implications related to both ius ad bellum and ius in bello.

- The use of AWSs can influence public opinion and policy in favor of war, because the use of AWSs minimizes risks of death or bodily injury to soldiers/individuals involved in a war. Thus, the use of AWSs may have an impact on ius ad bellum.

- The use of AWSs can negatively affect the respect of fundamental principles of ius in bello, such as the principles of distinction and proportionality.

- By removing the human element from war, the use of AWSs can contribute to the increase in the number of deaths because of the absence of human feelings, such as fear and compassion, which may play a role in reducing the number of deaths.

- The use of AWSs may cause significant collateral damage.

- AWSs can commit international crimes; this raises serious attribution of criminal responsibility questions, including issues related to command responsibility (for crimes committed by “killer robots”). Thus, an international approach to AWSs may be necessary

- The use of AWSs can raise jurisdictional issues, because AWS use may be trans-territorial. This also enhances the need toward a global approach to AWSs.

B) Questions:

1. -Are AWSs defined in your national law? If so, where (military code? Legislation?)?

2. -Does your national law limit the use of AWSs in any way? If so, how?

3. -Is there significant academic and/or policy debate in your country regarding the use of AWSs? If so, please briefly describe the majority and the minority view.

4. -Within your legal system, which entity can officially declare war or officially begin using force against another country? The President, Congress, Parliament, etc.?

5. -Are there legal limitations on such declarations of war/uses of force? If so, which ones?

6. -Is your country bound by any specific regional agreements which limit the use of military force, or which obligate your country to become involved in a defensive operation?

7. -Are fundamental ius in bello principles, such as the principles of distinction and proportionality, embedded in your national law? If so, which type of law – military code of conduct, national law, etc.?

8. -What type of national law governs the conduct of soldiers in your legal system?

9. -Is there relevant case law/prosecutions of soldiers for war crimes, where such soldiers have violated the principles of distinction and/or proportionality? Or where such soldiers have caused excessive collateral damage?

10. -What type of criminal liability do soldiers and commanders face within your national system if they commit war crimes and/or other misconduct? Are soldiers and commanders subject to court martial procedures only, or are they also subject to criminal liability outside of the military system?

11. -What modes of liability exist within your national criminal system?

12. -Does your national criminal law provide for command responsibility/other types of liability? If so, what are the requirements for command responsibility?

13. -Is there case law within your criminal justice system or your military system of commanders for abuses committed by their subordinates, using the mode of liability known as command responsibility? If so, please provide relevant citations and a brief summary of such cases.

14. -Is there significant academic and/or policy debate in your country regarding the attribution of responsibility to soldiers/operators/commanders for misconduct of AWSs? If so, please briefly describe the majority and the minority view.

15. -Does your national system recognize any other modes of attribution of criminal liability?

16. -Does your national military or criminal system address the issue of liability for the "misconduct" of AWSs? Can an operator and/or his/her commander face criminal liability in such circumstances?

17. -Is there any relevant case law, within the criminal justice system or within the military system, which addresses the issue of operator/commander liability for crimes committed by AWSs? If so, please provide relevant citations and a brief summary of such cases.

18. -What mechanisms exist in your national law to handle jurisdictional/conflict-of-law disputes? Please cite any relevant case law on jurisdictional disputes.

19. –Does domestic law apply to AI systems processing data inserted into the Cyberspace from abroad?

20. –Does domestic law apply if the AI hardware system involved in committing a criminal offense is on national territory, but the artificial agent operates on websites or networks that can be traced back to foreign countries (and the converse situation)?

21. -If a crime using AWSs is committed using software located in your home country but hardware located elsewhere, how does your domestic law localize such a crime? Would such a crime be considered as being committed within the borders of your country? Please cite any relevant case law.

22. -Does your government have extradition treaties with other countries which cover crimes committed by AWSs? Name such extradition treaties. What offenses are typically covered in such extradition treaties?

23. –Have agreements/protocols been concluded between your State and other States on judicial and police cooperation?

24. –To what extend have the domestic law and the debate on the subject among scholars been influenced by international sources, initiatives, white papers or reports developed at European and/or International levels?

II. List of Topics for Special Reports (Section IV)

1. Jurisdiction/conflict-of-laws issues related to the investigation and prosecution of crimes committed using AWSs

2. Addressing collateral damage issues related to the use of AWSs

3. The role of supra-national tribunals in prosecuting crimes committed through the use of AWSs, and the relationship between such supra-national prosecutions and any national prosecutions