

AIDP-IAPL International Congress of Penal Law

Artificial Intelligence and Criminal Justice

*Prof. Katalin Ligeti**

Already in 1997, IBM supercomputer Deep Blue showed, to the astonishment of the world, that almost no activity was ‘too human’ for artificial intelligence (AI) systems, not even playing chess with and defeating the world chess champion Garry Kasparov. More than twenty years later, AI has become an integral part of our lives. From digital voice assistants like Siri and Alexa to automated purchase suggestions, from cleaning robots to drones, AI systems are everywhere and their diffusion is expected to grow exponentially in the future.

Unsurprisingly, AI-related projects and initiatives have mushroomed over the last few years. Just to name a few, in April 2018 the European Commission issued a communication titled ‘Artificial Intelligence for Europe’,¹ which was followed by the creation of a High-Level Expert Group on Artificial Intelligence (AI HLEG) in June 2018. The UN Interregional Crime and Justice Research Institute (UNICRI) opened its Centre for Artificial Intelligence and Robotics in 2017, while the Committee of Ministers of the Council of Europe set up an Ad Hoc Committee on Artificial Intelligence in September 2019. In the context of the Council of Europe, it is also worth mentioning that the European Commission for the Efficiency of Justice (CEPEJ) came up with the ‘European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment’ at the end of 2018.²

AI raises a raft of questions for all legal systems around the world.³ The first of these questions concerns the very same meaning of ‘Artificial Intelligence’ since there is no consensus on the exact meaning of this concept.⁴ The definition by the European Commission can be used here as a useful reference point. According to the Commission, AI refers to

systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image

* This concept paper has been conceived and drafted together with Dr. Fabio Giuffrida (University of Luxembourg). All webpages have been last accessed on 8 November 2019.

¹ COM(2018) 237 final, 25 April 2018. One year later, the Commission issued a new communication on ‘Building Trust in Human-Centric Artificial Intelligence’ COM(2019) 168 final, 8 April 2019.

² On AI and ethics see also, e.g., L. Floridi et al., ‘AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations’ (2018) 28 *Minds and Machines* 689.

³ Among the uncountable studies see, for instance, W. Barfield and U. Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar 2018); A. Bensoussan and J. Bensoussan, *IA, robots et droit* (Bruylant 2019); T.F. Claypoole, *Law of Artificial Intelligence and Smart Machines: Understanding A.I. and the Legal Impact* (ABA Publishing 2019).

⁴ For example, in S. J. Russel and P. Norvig, *Artificial intelligence: A modern approach* (3rd edn, Upper Saddle River: Pearson Education 2013) 1–5, eight definitions of AI are examined and compared.

analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones [...]).⁵

This definition singles out some intrinsic features of AI systems, namely their ability to: a) *collect* and *analyse data* from the surrounding environment; and b) *take actions* to achieve the machine's specific *goals*, which are usually predefined by a human operator. These abilities are the equivalent of what is usually meant with 'intelligence' (or 'rationality') when talking about human beings.⁶ The reference to 'some degree of autonomy' is also of the utmost importance: despite human inputs, AI systems (can) act independently, e.g. they can choose among different courses of actions the one that looks the most appropriate to achieve their goals. Autonomy also refers to the fact that some AI systems, like humans, can *learn*: building both on the data they are fed with and on those they collect, AI systems can develop their 'skills' and adapt their 'behaviour' over time. 'Machine learning' thus implies that AI systems '[identify] patterns in available data and then [apply] the knowledge to new data'.⁷

Against this backdrop, legislators are required to keep pace with the scientific innovations and, when appropriate, regulate the unprecedented problems that AI raises. In the literature, there is already a considerable number of studies concerning the implications of AI for civil law, especially for liability law,⁸ and criminal law literature is increasingly paying attention to the matter. There is indeed a strong need to conceptualise and address the several legal issues that AI poses. At the level of international organisations, while the EU has not yet launched any initiative concerning AI and criminal justice, the Council of Europe has recently established a Working Group of Experts on Artificial Intelligence and Criminal Law, which will mostly focus on substantive criminal law. On the basis of its work, the option of adopting a standard-setting instrument addressing AI, which might take the form of a Council of Europe convention, will be considered.⁹

By definition, criminal law rules deal mostly with human beings and their behaviours, so that the application of such rules to AI systems is not straightforward. For instance, to what extent is a crime committed by an AI system attributable to a human being? Perhaps stretching to sci-fi scenarios, what could be, if any, the conditions to consider AI systems themselves criminally responsible? These questions echo those concerning the criminal liability of legal persons, another sensitive topic with which legislators and courts have had to cope in recent years and that was one of the subjects of the XX Congress.¹⁰ Further issues to examine relate to the opportunities that AI systems present for the criminal justice system. Can we rely on AI to adopt decisions on criminal

⁵ European Commission, 'Artificial Intelligence for Europe', cit., 1.

⁶ Cfr. AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines. Definition developed for the purpose of the AI HLEG's deliverables' (8 April 2019) available at <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>, 1).

⁷ European Commission, 'Artificial Intelligence for Europe', cit., 11. 'Machine learning' is a broad category and includes different learning procedures: see more in, e.g., AI HLEG, 'A Definition of AI', cit., 3–4.

⁸ See, for instance, A. Renda, 'Artificial Intelligence. Ethics, governance and policy challenges' (2019) Report of a CEPS Task Force, available at www.ceps.eu/ceps-publications/artificial-intelligence-ethics-governance-and-policy-challenges/, 82–90.

⁹ www.coe.int/en/web/artificial-intelligence/work-in-progress.

¹⁰ When assessing the impact of AI on substantive criminal law, parallels are often drawn between corporate criminal liability and AI's (potential) criminal liability (see, e.g., U. Pagallo and S. Quattrocchio, 'The impact of AI on criminal law, and its twofold procedures', in W. Barfield and U. Pagallo (eds.), op. cit., 402–405).

law cases? How can AI systems help law enforcement authorities in preventing, detecting, and combating crime?

The XXI International Congress of Penal Law will try to answer these and further questions stemming from the interplay between AI and criminal law by taking into account the various aspects of criminal justice: general and special part of substantive criminal law, procedural law as well as issues linked to the administration of justice, and international criminal law. The four sections of the Congress should analyse changes and tendencies regarding policies, norms, and practices. The technical nature of the subject and the indisputable fact that ‘the technological developments have far outpaced legal or policy debates’¹¹ around it call for an *inter-disciplinary* approach. Practitioners, scholars from other branches of law, and experts in fields other than law, especially those involved in developing AI systems, but also bioethicists, criminologists, scientists, and crime analysts, should be encouraged to attend the Congress and share their expertise. Cross-fertilisation of ideas is crucial to understanding the multifarious aspects of AI and pave the way for mature reflections on how (criminal) law should deal with such a complex matter.

Section 1. Traditional Criminal Law Categories and AI: Crisis or Palingenesis?

Section 1 of the Congress will focus on the general part of substantive criminal law and address the question of whether and how traditional criminal law categories – especially *actus reus*, *mens rea*, and causation – can apply to crimes committed by/through AI systems. When AI crosses the path of criminal law, these traditional concepts may experience a crisis. The example of autonomous driving is helpful to grasp the reasons of this.¹² In the event of an accident involving personal injury or causing death to a passer-by, who is responsible? Several options can be explored. The most unrealistic, at least for the time being, is that of considering the car itself (criminally) responsible. Although some authors do not entirely rule out the possibility of endorsing a direct liability model,¹³ this seems unfeasible. Even admitting that the accident caused by the car amounts to an *actus reus*, it would be very difficult to claim that this act was supported by the car’s *mens rea*:

It would make little (social) sense to attribute culpability to a being that is incapable of recognizing its own past and evaluating its past actions in accordance with a moral reference system. An entity that does not have a conscience cannot participate in a dialogue on ethical issues and cannot respond to reproach.¹⁴

¹¹ A. G. Ferguson, ‘Policing Predictive Policing’ (2017) 94 *Washington University Law Review* 1115, 1148.

¹² The issue of autonomous driving is also the main focus of the Council of Europe Working Group of Experts on AI and Criminal Law. On criminal law issues related to autonomous driving see, e.g., J. Gurney, ‘Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles’ (2015) 5 *Wake Forest Journal of Law & Policy* 393; S. Gless et al., ‘If Robots Cause Harm, Who Is to Blame: Self-Driving Cars and Criminal Liability’ (2016) 19 *New Criminal Law Review* 412. For broader remarks beyond autonomous driving see, e.g., F. Basile, ‘Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine’ (2019) *Diritto Penale e Uomo*, available at https://dirittopenaleuomo.org/contributi_dpu/intelligenza-artificiale-e-diritto-penale-quattro-possibili-percorsi-di-indagine/, 1, 24 ff.

¹³ See G. Hallevey, *Liability for Crimes Involving Artificial Intelligence Systems* (Springer 2015) 102 ff.

¹⁴ S. Gless et al., ‘If Robots Cause Harm’, op. cit., 423.

Likewise, it is even less sensible to ‘punish’ a machine, at least as long as the machine ‘is not imbued with a will to live’.¹⁵ In other words, if the AI system is not in a position of understanding the sanction and learning from it, punishment is of no use.¹⁶

In order not to create accountability gaps, it would then be necessary to look for the human responsibility behind the accident. This would imply ascertaining whether the manufacturer, the programmer, and/or the user are responsible. The easiest scenario would be that of an autonomous car that is expressly programmed with the aim of killing, as in this case the AI system would simply be used as an instrument of crime.¹⁷ Leaving aside this somehow extreme hypothesis, however, some problems arise. The assessment of the human responsibility should in fact take into account several factors, e.g. whether there was any negligence in designing/using the car and whether a human being (in the car or remotely) was able to intervene and disengage the autonomous driving system.¹⁸ For example, the US National Transportation Safety Board has recently found that, in the accident that was caused in 2018 by an Uber self-driving test vehicle in Arizona and that killed a woman who was crossing the road, there were some flaws in the system, which was not in a condition to recognise a person walking outside pedestrian crossing. Furthermore, the driver insider the car was distracted when the accident happened and she could thus face criminal charges.¹⁹

The liability models that can be used to attribute the responsibility for AI machines’ accidents to human beings are the ‘perpetration-by-another’ model, whereby the AI system is considered the ‘other’ entity that humans use to commit the crime, and the ‘natural probable consequence’ model, according to which the manufacturer, programmer, and/or user are responsible because the offence is a natural and probable consequence of their (negligent) action of creating, programming, and/or using the machine.²⁰ These categories are to be found in several criminal justice systems, for instance to regulate the criminal responsibility of accomplices, but their applicability to AI systems, which are different from both mere instruments of crime and (human) partners in crime, deserves further reflections. By the same token, it is to be examined whether strict liability models can play

¹⁵ *Ivi*, 424, where the authors underline that it is difficult to imagine sanctions ‘against Intelligent Agents that would fulfill the same purposes as criminal sanctions imposed on human beings’, since robots ‘are incapable of understanding the meaning of punishment and therefore cannot draw a connection between anything “done to them” and their prior fault’.

¹⁶ For similar remarks on the little sense of ‘punishing’ AI machines – at least for the time being – see, for instance, U. Pagallo, *The Laws of Robots. Crimes, Contracts, and Torts*, Springer, 2013, 50–51; D. Lima, ‘Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law’ (2018) 69 *South Carolina Law Review* 677, 688–689; T. C. King et al., ‘Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions’ (2019) *Science and Engineering Ethics* 1, 20.

¹⁷ See, S. Gless et al., ‘If Robots Cause Harm’, op. cit., 425; G. Hallevy, ‘The Basic Models of Criminal Liability of AI Systems and Outer Circles’ (2019) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3402527, 2–3.

¹⁸ See, more extensively, F. Douma and S.A. Palodichuk, ‘Criminal Liability Issues Created by Autonomous Vehicles’ (2012) 59 *Santa Clara Law Review* 1157, 1160 ff. For further remarks on negligence and liability for crimes committed by AI systems see S. Beck, ‘Intelligent agents and criminal law—Negligence, diffusion of liability and electronic personhood’ (2016) 86 *Robotics and Autonomous Systems* 138.

¹⁹ ‘Uber in fatal crash had safety flaws say US investigators’ (*BBC News*, 6 November 2019) available at www.bbc.com/news/business-50312340.

²⁰ Cfr. D. Lima, op. cit., 691 ff.; G. Hallevy, ‘The Basic Models of Criminal Liability’, op. cit., 1–8; T. C. King, op. cit., 20–22; P. Yeoh, ‘Artificial intelligence: accelerator or panacea for financial crime?’ (2019) 26 *Journal of Financial Crime* 634, 638–640.

a role in this context and whether an agreement can be found on the notion of a socially permissible risk concerning autonomous driving, since ‘the crucial question in the development of automated driving might concern what kind of risk respective societies are willing to accept’.²¹

In addition, another traditional concept of criminal law, i.e. causation, may have to be rethought when it comes to AI-related crimes. It can happen that offence committed by AI machines cannot be easily traced back to the human being behind the system. For instance, one could think of robots that were produced by humans who had no intent whatsoever to commit a crime. If the accident is caused by the faulty process of machine learning that the AI system undertakes, rather than by a potential human negligence in programming or using it, should we consider the causation chain between the human behaviour and the accident to be interrupted by an unpredictable event? Or should not we think in this way since AI systems cannot be considered as proper ‘persons’ who can break the chain of causation?²²

In sum, the attribution of crimes committed by/through AI systems to responsible individuals is a major challenge to traditional ways of criminal law thinking. This section of the Congress should thus examine the consequences of AI for the well-established categories of the general part of criminal law, especially *mens rea*, *actus reus*, and causation, and discuss whether they are sufficient to regulate the new phenomena or need instead some (deep) rethinking to face the challenges ahead.

Section 2. Old and New Criminal Offences: AI Systems as Instruments and Victims

Section 2 of the Congress will focus on the special part of substantive criminal law, which is likely to undergo substantial changes in the coming years due to the advent and diffusion of AI. Section 2 will examine at least two different scenarios. First, it should discuss how AI systems can be used to commit ‘traditional’ crimes. Some studies have already highlighted the extent to which criminal organisations can benefit from AI. For instance, drug trafficking may become easier – and much less risky for criminals – if the illegal substances are moved from one place to another by means of drones.²³ The same goes for terrorist attacks that may be carried out by placing explosive materials on AI machines.²⁴ Another crime that AI may facilitate is online fraud, especially ‘spear phishing’, which refers to ‘email or electronic communications scam targeted towards a specific individual,

²¹ S. Gless, ‘Working Paper II. Document prepared for the 1st meeting of the Working Group of Experts on Artificial Intelligence and Criminal Law’ (2019) available at www.coe.int/en/web/cdpc/home, 4.

²² Cfr U. Pagallo, op. cit., 53 and 75. See also D. Lima, op. cit., 684.

²³ According to Europol, organised crime groups ‘involved in drug trafficking will likely invest in drone technology for trafficking purposes in order to avoid checks at border crossing points, ports and airports’ (Europol, ‘European Union Serious and Organised Crime Threat Assessment’ (2017) 34).

²⁴ See F. Douma and S.A. Palodichuk, op. cit., 1166; M. Brundage et al., ‘The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation’ (2018) Future of Humanity Institute, University of Oxford; Centre for the Study of Existential Risk, University of Cambridge, available at <https://maliciousaireport.com/>, 27 ff.; T. C. King et al., op. cit., 12–13.

organization or business'.²⁵ While phishing by means of emails that are blatantly fake is not often successful, AI systems can create and send fraudulent emails that are tailored to the recipient, who can then be convinced to follow a malicious link and/or share his or her data with the fraudster.²⁶

Second, AI may lead to *new* crimes altogether. In a 2019 report by UNICRI and Interpol, we read that a 'study on "new crimes" involving the malicious use of AI and robotics should be conducted'.²⁷ On the one hand, AI systems can become 'victims' of crime and it is likely that new definitions and rules will be needed to regulate these situations.²⁸ For instance, AI systems may be sabotaged by third parties so that these systems will be impaired from achieving their goals and/or induced to commit a crime. One could think of persons who intentionally disrupt the software of autonomous driving cars, in this way provoking accidents that were entirely out of control of the programmer and user of the vehicle.²⁹

On the other hand, AI is a powerful instrument for dangerous behaviours that could be criminalised in the future. AI systems may be tasked, for example, with the creation and spreading of fake news.³⁰ While this already represents a complex issue in contemporary society, similar conducts do not usually amount to a crime, with a few exceptions.³¹ Since AI has the potential to escalate this phenomenon to the point where it would represent a daunting and unprecedented threat to our democracies, as the machines' level of accuracy is likely to make it difficult even for the most attentive user to distinguish truth from fiction, it is worth examining whether the conducts at issue should be criminalised in order to reduce their potentially devastating effects.

Finally, the possible interactions between AI and cryptography, with a focus on those technologies that build on cryptography such as blockchain, will deserve further attention in the future. It is difficult to regulate the legal implications – including criminal law ones – of blockchain and crypto-assets per se. The possible combination with AI may raise even more complex questions as this may facilitate the commission of existing or new crimes, and potentially require the introduction of *ad hoc* criminal law provisions. Due to the lack of any in-depth analysis of the issue in the literature, the Congress will represent the ideal opportunity to start identifying these forthcoming challenges and reflecting on them.

²⁵ This definition, which is taken from the website of the cybersecurity and anti-virus provider Kaspersky (www.kaspersky.com/resource-center/definitions/spear-phishing), also adds: 'Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer'.

²⁶ Spear phishing has been subject to an experiment by two computational social scientists, J. Seymour and P. Tully, 'Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter' (2016) available at www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf, which is discussed by T. C. King et al., *op. cit.*, 2. Risks of spear phishing are also examined by, e.g., M. Brundage et al., *op. cit.*, 18–21.

²⁷ UNICRI Centre for Artificial Intelligence and Robotics and Interpol Innovation Centre, 'Artificial Intelligence and Robotics for Law Enforcement' (2019) available at www.unicri.it/in_focus/on/interpol_unicri_report_ai, 23.

²⁸ Cfr. F. Basile, *op. cit.*, 32–33.

²⁹ F. Douma and S.A. Palodichuk, *op. cit.*, 1165; M. Brundage et al., *op. cit.*, 5.

³⁰ M. Brundage et al., *op. cit.*, 29 and 46.

³¹ See, e.g., A. Schetzer, 'Governments are making fake news a crime – but it could stifle free speech' (*The Conversation*, 7 July 2019) available at <https://theconversation.com/governments-are-making-fake-news-a-crime-but-it-could-stifle-free-speech-117654>.

Section 3. AI and Administration of Justice: Predictive Policing and Predictive Justice

Section 3 will examine the impact of AI on the administration of justice. In particular, it will focus on criminal procedural law and, more broadly, law enforcement, by looking at predictive policing and predictive justice mechanisms. By using algorithms that process enormous quantity of data, these mechanisms make predictions about where and when crimes are likely to be committed, and even by whom in some cases (predictive policing)³² and about whether a suspect or defendant is likely to flee or commit further crimes, with the consequence that criminal courts can deny bail or opt for harsh sentences (predictive justice). These are far from being sci-fi speculations: already in 2006, a US scholar argued that ‘prediction of criminality has become de rigueur in our highly administrative law enforcement and prison sectors—seen as a necessity, no longer a mere convenience’.³³ More recently, during the 2018 Global Meeting on the Opportunities and Risks of AI and Robotics for Law Enforcement, ‘the use of AI tools for the purposes of prediction and analysis’³⁴ turned out to be the most cited application of AI technology for law enforcement purposes.

In the US, for instance, Californian police use a software called PredPol to ‘[p]redict where and when specific crimes are most likely to occur’,³⁵ although this instrument has recently been met with criticism as it did not help in reducing crime.³⁶ Some European police forces resort to similar software, Precobs (Pre Crime Observation System).³⁷ The logic behind these and other predictive policing systems is simple: some crimes, such as theft and robberies, ‘are to a large extent predictable, because criminals with a distinguishable profile tend to commit the same type of crime, at roughly the same location and time of the day’.³⁸

As for predictive justice, there are nowadays reportedly ‘more than 200 risk assessment tools available in criminal justice and forensic psychiatry, which are widely

³² Traditionally, predictive policing ‘is not actually predicting a particular crime, but predicting an elevated risk of crime based on pre-determined place-based factors’, but there is now a shift towards ‘the use of predictive technologies to identify individuals and groups involved in predicted criminal activity’ (A. G. Ferguson, ‘Policing Predictive Policing’, op. cit., 1142).

³³ B.E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (University of Chicago Press 2006) 16.

³⁴ UNICRI Centre for Artificial Intelligence and Robotics and Interpol Innovation Centre, op. cit., 9. See also C. Slobogin, ‘Principles of Risk Assessment: Sentencing and Policing’ (2018) 15 *Ohio State Journal of Criminal Law* 583; M. Gialuz, ‘Quando la giustizia penale incontra l’intelligenza artificiale: luci e ombre di risk assessment tools tra Stati Uniti ed Europa’ (2019) *Diritto penale contemporaneo* 1, available at www.penalecontemporaneo.it/d/6702-quando-la-giustizia-penale-incontra-l-intelligenza-artificiale-luci-e-ombre-dei-risk-assessment-too.

³⁵ www.predpol.com/.

³⁶ M. Puente and C. Chang, ‘LAPD changing controversial program that uses data to predict where crimes will occur’ (*Los Angeles Time*, 15 October 2019) available at www.latimes.com/california/story/2019-10-15/lapd-predictive-policing-changes.

³⁷ See A. Završnik, ‘Algorithmic justice: Algorithms and big data in criminal justice settings’ (2019) *European Journal of Criminology* 1, 2.

³⁸ R. Peeters and M. Schuilenburg, ‘Machine justice: Governing security through the bureaucracy of algorithms’ (2018) 23 *Information Polity* 267, 272.

used to inform sentencing, parole decisions, and post-release monitoring'.³⁹ One of the most famous, at least in the US, is COMPAS (Correctional Offender Management Profiling for Alternative Sanctions).⁴⁰ COMPAS assesses the risk of recidivism, which is calculated by taking into account both an interview with the defendant and information from his or her criminal history. The COMPAS risk assessment, however, 'does not predict the specific likelihood that an individual offender will reoffend. Instead, it provides a prediction based on a comparison of information about the individual to a *similar data group*'.⁴¹

These words are taken from a landmark decision in the field of AI and criminal justice, *State v. Loomis* (2016), where the use of COMPAS was challenged before the Supreme Court of Wisconsin. The defendant, who was sentenced to six years of imprisonment after the COMPAS risk assessment had considered his risk of recidivism high, claimed that his right to due process had been violated because, inter alia, it was unclear how COMPAS made its assessments, and it was therefore impossible to challenge their accuracy, and the use of the predictive justice software had violated his right to an individualised sentence.⁴² The Supreme Court of Wisconsin did not share his views and decided that, if used properly, courts' reliance on COMPAS risk assessments in the sentencing phase does not violate the right to due process.⁴³ In the case of *Loomis* – and this should happen, according to the Supreme Court of Wisconsin, in any other case where predictive justice instruments are used – the court of lower instance reached its decision by relying on 'other independent factors', so that the use of the COMPAS risk assessment was 'not determinative in deciding whether *Loomis* could be supervised safely and effectively in the community'.⁴⁴

In the light of the foregoing, section 3 of the Congress shall delve into the several problems that predictive policing and justice instruments raise for the administration of justice. First, it should be discussed whether predictive policing is not in fact counterproductive. As predictions on the future are made on the basis of data from the past, the algorithms can lead police authorities to invest their money and resources in patrolling areas that are already known to be prone to crime, while all other areas and crimes (including those offences for which the reporting rate is low) could continue to be neglected.⁴⁵ One of the reasons why *PredPol* attracted criticism was precisely because it

³⁹ *Ivi*, 273.

⁴⁰ See, for instance, A. Christin, 'Algorithms in practice: Comparing web journalism and criminal justice' (2017) *Big Data & Society* 1, 5–6.

⁴¹ *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), para. 15 (emphasis added). Harcourt speaks of predictive policing instruments as 'actuarial methods', as 'they use statistical methods [...] on large datasets of criminal offending rates in order to determine the different levels of offending associated with a group or with one or more group traits and, on the basis of those correlations, to predict the past, present, or future criminal behavior of a particular person' (B. E. Harcourt, op. cit., 16).

⁴² *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), para. 34. For a commentary see H.-W. Liu, C.-F. Lin and Y.-J. Chen, 'Beyond *State v. Loomis*: artificial intelligence, government algorithmization and accountability' (2019) 27 *International Journal of Law and Information Technology* 122.

⁴³ *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), para. 8.

⁴⁴ *Ivi*, para. 9. The Court warned about some risks connected with the use of COMPAS, yet this is unlikely to be sufficient to eradicate all the problems stemming from risk assessments (see 'Criminal Law – Sentencing Guidelines – Wisconsin Supreme Court Requires Warning before Use of Algorithmic Risk Assessments in Sentencing—*State v. Loomis*, 881 N.W.2d 749 (Wis. 2016)' (2017) 130 *Harvard Law Review* 1530, 1536).

⁴⁵ R. Peeters and M. Schuilenburg, op. cit., 274; A. Završnik, op. cit., 7.

‘essentially provided information already being gathered by officers patrolling the streets’.⁴⁶

Second, if a person is suspected of committing future crimes – and then investigated – on the basis of algorithmic calculations that draw on statistical data and/or the analysis of patterns and behaviours that are not criminal per se, some basic human rights would be at stake, beginning with the presumption of innocence. Incidentally, this might also exacerbate the relations between the public and law enforcement authorities, which, especially in some areas, are already tense and rife with mistrust.⁴⁷ Third, predictive policing and justice are thought to provide neutral and objective information, while human judgements are intrinsically biased. This argument has been rebutted by studies that proved that AI machines used in the administration of justice ‘embed existing biases and perpetuate discrimination’.⁴⁸ After all, since AI systems work on the basis of data inputted by human beings, the choice of these data becomes crucial and may turn out to be itself biased.⁴⁹ The human component can never be entirely set aside also because algorithms usually come up with a number or a given result, but it is then for the user to attach a meaning to that figure or outcome: ‘For instance, at what probability of recidivism should a prisoner be granted parole? Whether this threshold ought to be a 40 percent or an 80 percent risk of recidivism is an inherently “political” decision based on the social, cultural and economic conditions of the given society’.⁵⁰

Finally, predictive policing and justice prompt broader systematic reflections on the future role of public authorities (courts, prosecutors, and police) in the enforcement of the (criminal) law, a role that will become much more proactive compared to the (mostly) reactive one they currently play.⁵¹ Furthermore, as their activities are likely to be always more influenced, if not determined, by mathematical formulas,⁵² we could witness a silent shift of responsibility from public authorities towards (private) companies, and ultimately towards the experts who create and programme AI systems. This is however highly problematic from the perspective of public authorities’ accountability and transparency,⁵³ especially because the way AI systems work is often not clear at all, and it may also be covered by trade secret.⁵⁴ Many sensitive decisions concerning individuals are thus left in

⁴⁶ M. Puente and C. Chang, ‘LAPD changing controversial program’, op. cit.

⁴⁷ A. G. Ferguson, ‘Policing Predictive Policing’, op. cit., 1163.

⁴⁸ A. Završnik, op. cit., 4, who refers to the ProPublica’s report by J. Angwin et al., ‘Machine Bias – There’s software used across the country to predict future criminals. And it’s biased against blacks’ (2016) available at www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. See also R. Peeters and M. Schuilenburg, op. cit., 274; Council of Europe Committee of experts on internet intermediaries (MSI-NET), ‘Study on the human rights dimension of automated data processing techniques (in particular algorithms) and possible regulatory implications’ (2017) MSI-NET(2016)06 rev3 FINAL, 11–12.

⁴⁹ A. Završnik, op. cit., 8–9. See also A. Christin, op. cit., 3. Humans can also commit errors and this may affect the quality of the predictive mechanism (see A. G. Ferguson, ‘Policing Predictive Policing’, op. cit., 1150 ff.).

⁵⁰ A. Završnik, op. cit., 10.

⁵¹ See, for instance, A. G. Ferguson, ‘Predictive Prosecution’ (2016) 51 *Wake Forest Law Review* 705, 731 ff.

⁵² Cfr. R. Peeters and M. Schuilenburg, op. cit., 274–275.

⁵³ See A. G. Ferguson, ‘Policing Predictive Policing’, op. cit., 1169 ff.; A. Babuta, M. Oswald and C. Rinik ‘Machine Learning Algorithms and Police Decision-Making. Legal, Ethical and Regulatory Challenges’ (2018) RUSI Whitehall Report 3-18, 17–22.

⁵⁴ See, for instance, P. W. Nutter, ‘Machine Learning Evidence: Admissibility and Weight’ (2019) 21 *Journal of Constitutional Law* 919, 941–944.

the hands of obscure and unclear mechanisms ('black-box AI').⁵⁵ The scenario can become even more problematic if AI will be used not only to predict future crimes or risks of recidivism but also to decide criminal law cases altogether, replacing judges and juries. Automated decision systems have already been tested in civil proceedings so it would not be surprising if there will be some attempts to inquire whether they can also work in criminal law contexts.⁵⁶

In sum, extensive and in-depth reflections on whether, to what extent and under which conditions predictive methods are truly compatible with the basic tenets of modern democracies – including fundamental rights such as privacy, presumption of innocence, and defence rights – cannot be postponed anymore.

Section 4. International Perspectives on AI: Challenges for Judicial Cooperation and International Humanitarian/Criminal Law

Section 4 of the Congress will examine some international implications of the use of AI. In particular, this section will deal with the impact of AI on: a) evidence gathering, which will be looked at through the prism of international cooperation; and b) international humanitarian law and international criminal law, especially with regard to the use of robots in war contexts.

As for evidence gathering, it ought to be noted that AI systems can be of great value to law enforcement authorities, even beyond the above-mentioned examples of predictive policing.⁵⁷ Analysing, for example, DNA or social media profiles 'produces large amounts of complex data in electronic format',⁵⁸ which may contain useful patterns that human analysis could not be able to grasp. AI-backed tools can also be used to identify fake art works⁵⁹ or persons by means of facial recognition software, which 'could identify a defendant even with video or photographic evidence in less than ideal circumstances'.⁶⁰ AI can also help in locating events and places. In 2017, the International Criminal Court requested the arrest of a Libyan warlord by relying on information deriving from satellite images and videos, which were uploaded online by his acolytes and showed some

⁵⁵ See the 'Statement of Concern About Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations' (2016) published on *American Civil and Liberties Union* (<https://www.aclu.org>); A. Christin, op. cit., 3. As the EU High-Level Expert Group on AI explains, 'Some machine learning techniques, although very successful from the accuracy point of view, are very opaque in terms of understanding how they make decisions. The notion of *black-box AI* refers to such scenarios, where it is not possible to trace back to the reason for certain decisions' (AI HLEG, 'A Definition of AI', cit., 5).

⁵⁶ See F. Basile, op. cit., 14–16.

⁵⁷ See, for instance, L. Goldmeier, 'How Artificial Intelligence is Revolutionizing Investigation for Law Enforcement' (*Briefcam*, 21 August 2018) available at www.briefcam.com/resources/blog/how-artificial-intelligence-is-revolutionizing-investigation-for-law-enforcement/. An extensive overview of the ways AI can support law enforcement can be found in the recent report by UNICRI Centre for Artificial Intelligence and Robotics and Interpol Innovation Centre, op. cit. A testament to the increasing importance of the topic is the fact that the 2019 OSCE Annual Police Experts Meeting was devoted to 'Artificial Intelligence and Law Enforcement - An Ally or Adversary?' (see www.osce.org/event/2019-annual-police-experts-meeting).

⁵⁸ C. Rigano, 'Using Artificial Intelligence to Address Criminal Justice Needs' (2019) *National Institute of Justice Journal*, 6.

⁵⁹ L. Floridi, 'Artificial Intelligence, Deepfakes and a Future of Ectypes' (2019) 31 *Philosophy & Technology* 317. Interestingly, the author notes that AI can also be used to *create* fake work arts.

⁶⁰ P. W. Nutter, op. cit., 929–930.

executions he had ordered: ‘Geographical features seen in the videos—buildings, roads, trees, hills—were located via time-stamped high-resolution satellite images. In this way, video, photos, satellite images, and other data are triangulated to verify events in a specific time and place’.⁶¹ While in that case most of the analysis was carried out by humans, in the future ‘substantial portions of it could be automated or enhanced by machine learning’.⁶²

When the outcome of algorithmic calculations by AI systems is used as evidence before a criminal court, however, the fundamental right to a fair trial risks being violated at least for two different reasons. First, as mentioned, the algorithmic processes that analyse the data and end up providing public authorities with a given piece of evidence are often obscure, so that the defendant is not in a position to challenge the way in which evidence has been gathered: ‘Insofar as individuals in a legal process are unable to understand and contest, even with the help of legal counsel, complex algorithmic systems used to process evidence alleged to relate to them, there is a significant threat to due process rights’.⁶³

Second, and consequently, the use of AI-related evidence poses a risk to the principle of equality of arms.⁶⁴ Even if this principle has to discount the difference between the situation of public authorities and that of individuals, an insurmountable advantage to the former flows from the use of AI in the process of evidence gathering. If investigations are based on AI techniques, therefore, the defendant should be in a position to understand how evidence has been gathered, while ‘the denial of discovery in relation to the program, code, or data governing the AI system [...] would represent a clear infringement of the principle of Equality of Arms between the parties’.⁶⁵ If the code is discovered, the defendant will likely need to find an expert who would be able to understand and challenge the algorithmic process on which police and prosecutors relied.⁶⁶ At the same time, however, the integral discovery of how AI machines work may be detrimental to law enforcement authorities’ activities and companies’ trade secrets, and may also lead to endless disputes over the reliability of AI systems that could hamper or substantially prolong criminal proceedings.

In sum, it will be necessary to strike a balance between the advantages that AI brings to the administration of justice and the respect of key principles of criminal justice, such as the right to due process and rights of defence, which are at stake when an individual is left to argue against obscure decisions that are in essence taken by AI experts outside the walls of criminal courts.⁶⁷ Since AI continues to lag in common sense reasoning, thereby profoundly questioning the tenets of criminal procedure, session 4 of the Congress should examine whether AI-backed tools should be held to a certain standard of explanation and if

⁶¹ S. Livingston and M. Risse, ‘The Future Impact of Artificial Intelligence on Humans and Human Rights’ (2019) 33 *Ethics & International Affairs* 141, 143.

⁶² M. M. Maas, ‘International law does not compute: Artificial intelligence and the development, displacement or destruction of the global legal order’ (2019) 20 *Melbourne Journal of International Law* 29, 44.

⁶³ M. Veale, ‘Algorithms in the Criminal Justice System’ (2019) *The Law Society of England and Wales*, 57. Cfr. S. Gless, ‘Working Paper II’, op. cit., 4–5.

⁶⁴ *Ibidem*.

⁶⁵ U. Pagallo and S. Quattrocchio, op. cit., 396.

⁶⁶ In this case, the traditional criteria to evaluate scientific evidence – such as the known US *Daubert* criteria – can come into play in order to assess whether the algorithm possesses some sufficient level of accuracy (P. W. Nutter, op. cit., 948).

⁶⁷ See P. W. Nutter, op. cit., *passim*; A. Završnik, op. cit., 14.

yes what is the applicable standard and what are the guarantees that should surround the use of AI-related evidence. For instance, a solution that could help foster reliability and transparency of AI techniques would be, according to some authors, ‘to ask (and provide) for independent certification of the AI system’s trustworthiness. An expert-witness could be appointed by the judge to verify either the algorithmic process, or the neural network of a certain AI system, whenever the parties express their doubt about the correctness of automated data’.⁶⁸

While new approaches and solutions to evidentiary matters are needed at the national level, the situation becomes even more complex in cross-border settings. Cross-border exchange of evidence, especially from the perspective of the admissibility and use of evidence in a different State than that in which evidence was gathered, has always represented a critical issue of international cooperation in criminal matters. Even in a context such as that of the European Union, where harmonisation in criminal matters is on the rise, there has been so far no political will to agree on minimum rules concerning the mutual admissibility of evidence.⁶⁹ On top of that, the new – and still largely unresolved – problems connected with digital evidence add a further note of complexity.⁷⁰ Against this backdrop, therefore, it is an open question, which has not been yet addressed in the literature, whether the existing instruments of cooperation in criminal matters can ensure exchange, admissibility, and use of AI-related evidence in a satisfactory way.⁷¹ If each country ends up regulating the issue of AI and criminal evidence according to its own principles, rules, and perhaps even technical standards, the panoply of different regimes may hamper judicial cooperation, so that one may wonder whether a coordinated approach on the international level would not be appropriate.⁷²

As in any other case where AI systems may be used, however, the positive effects of the new technologies should not be forgotten.⁷³ It is worth mentioning that, while it brings international cooperation in uncharted territory, AI could also help national authorities to deal more efficiently with requests for cooperation. According to UNICRI and Interpol, one

⁶⁸ U. Pagallo and S. Quattrocchio, *op. cit.*, 398. The authors however notice that, while this ‘would certainly increase the chances to challenge the accuracy of the data’, it only represents ‘an “indirect” challenge, since it would be mediated by the direct experience of the court’s expert, whom the defence may not trust’ (*ibidem*). See also M. Cross, ‘Algorithms and Schrodinger’s Justice’ (2017) *The Law Society Gazette*. In this context, it is worth adding that Principle 4 of the CEPEJ Ethical Charter is that of ‘transparency, impartiality and fairness’, according to which data processing methods should be made accessible and understandable, and external audits should be authorised.

⁶⁹ See, for instance, J. Vervaele, ‘Lawful and Fair Use of Evidence from a Human Rights Perspective’, in F. Giuffrida and K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (University of Luxembourg 2019) 56–67.

⁷⁰ Once more, the intense negotiations on ‘e-evidence’ within the EU are a testament to these new challenges. See, for instance, S. Tosza, ‘The European Commission’s Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks’ (2019) *eu crim* 212. The topic was also addressed during the XIX International Congress of Penal Law (see section IV of the Recommendations of that Congress).

⁷¹ See also S. Gless, ‘Working Paper II’, *op. cit.*, 5–6, where the author points out that the Council of Europe Convention on Cybercrime may not be sufficient to face all the challenges connected with AI-related evidence.

⁷² Further problems might also be related to the issue of dual criminality, a traditional principle of mutual legal assistance, e.g. if some countries allow the use of self-driving cars and others do not (*ibidem*).

⁷³ For instance, S. Gless et al., ‘If Robots Cause Harm’, *op. cit.*, 430–431, stress that, in spite of the complex problems that autonomous driving raises, society may nonetheless have ‘a valid interest in promoting the use of self-driving cars’ as they ‘might indeed reduce the overall harm caused in street traffic’.

example of possible future use of AI and robotics consists precisely in autonomously researching, analysing and responding to requests for international mutual legal assistance.⁷⁴

Moving on to international humanitarian law (IHL) and international criminal law (ICL), the issue of autonomous weapon systems (AWSs) and their impact on traditional principles of IHL and ICL has gained attention in the literature. Governments invest massively in research and realisation of AWSs, which, once fully created and extensively diffused, can represent invaluable resources for the military. An AWS can be defined as ‘a weapon system that, based on conclusions derived from gathered information and preprogrammed constraints, is capable of *independently selecting and engaging target*’.⁷⁵ ‘Autonomous’ is therefore different from ‘automated’, since only ‘autonomous weapons’ can act independently of human inputs. A difference is usually made between ‘human-out-of-the-loop’ weapons, which are indeed the ‘autonomous’ ones, and ‘human-in-the-loop’ or ‘human-on-the-loop’ weapons, which instead feature some form of human control.⁷⁶ For the purpose of this paper, ‘AWSs’, ‘killer robots’, and ‘AI systems’ will be used as synonyms.

The first question AWSs raise is not strictly legal but has noteworthy legal implications: can their use make war a ‘less serious issue’ and therefore cause more wars than in the past? It is unquestionable that the use of robots by a given State reduces the number of its own losses in war.⁷⁷ A robot-war can ‘lower public awareness’ since ‘a fully-automated military mission transforms war into a fairly *technical and bureaucratic* operation, risk-free so to speak, so that causes of war may also be trivial, once you imagine both armies engaging no humans but only robot soldiers’.⁷⁸ To put it even more bluntly, ‘a president who sends someone’s son or daughter into battle has to justify it publicly ... But if no one has children in danger, is it a war?’⁷⁹ In essence, AWSs can change the approach of politicians and public opinion to war, in a way that does not necessarily help to reduce wars in the future, rather the contrary. The impact of AWSs on the *ius ad bellum*, namely the set of rules that regulate the conditions to enter into war, deserves therefore further attention.⁸⁰

⁷⁴ UNICRI Centre for Artificial Intelligence and Robotics and Interpol Innovation Centre, op. cit., vi.

⁷⁵ R. Crootof, ‘The Killer Robots Are Here: Legal and Policy Implications’ (2015) 36 *Cardozo Law Review* 1835, 1854 (emphasis added).

⁷⁶ See, e.g., Human Rights Watch, ‘Losing Humanity. The Case against Killer Robots’ (2012) available at www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots, where the following three definition can be found: ‘Human-in-the-Loop Weapons: Robots that can select targets and deliver force only with a human command; Human-on-the-Loop Weapons: Robots that can select targets and deliver force under the oversight of a human operator who can override the robots’ actions; and Human-out-of-the-Loop Weapons: Robots that are capable of selecting targets and delivering force without any human input or interaction’. See also, for instance, P. Alston, ‘Lethal Robotic Technologies: The Implications for Human Rights and International Humanitarian Law’ (2011) 21 *Journal of Law, Information & Science* 35, 40–41.

⁷⁷ M. Wagner, ‘The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems’ (2014) 47 *Vanderbilt Journal of Transnational Law* 1, 10.

⁷⁸ U. Pagallo, op. cit., 59 (emphasis added). See also M. E. O’Connell, ‘Seductive Drones: Learning from a Decade of Lethal Operations’ (2011) 21 *Journal of Law, Information & Science* 116, 133 ff.

⁷⁹ ‘Drones and democracy. Unmanned aerial vehicles are changing the democracy that uses them’ (*The Economist*, 1 October 2010) available at www.economist.com/babbage/2010/10/01/drones-and-democracy.

⁸⁰ U. Pagallo, op. cit., 58 ff.

Second, AWSs can also affect the *ius in bello*, which instead refers to the principles and rules that should apply during war.⁸¹ There is an ongoing debate on whether AWSs undermine or strengthen the fundamental principle of distinction, according to which no civilians or civilian targets can be attacked during wars. On the one hand, one may argue that, as long as AWSs are programmed to avoid civilian targets, they may actually be better placed than human combatants to ensure the respect of the principle at hand.⁸² On the other, however, there is no guarantee that, in practice, robots will be able to spare more civilians than human beings can, not least because AI systems – even the most advanced ones – will not have the necessary human abilities to figure out whether, in a given situation, a person or a target is civilian or not.⁸³ The following example is enlightening:

During a counterinsurgency operation in a village, soldiers receive information that combatants may be hiding inside a house. Unbeknownst to the soldiers, no insurgents are present. Inside of the home, boys are playing with a ball. The children kick the ball towards the gate as the soldiers enter the main door. The male inhabitants of this area carry a dagger called the *kirpan* for purely religious reasons. One of the parents watching the children realizes that the children are in danger and tries to warn them by screaming in their direction to stay away from the gate.⁸⁴

This situation should not pose any real problem for human soldiers, who are likely to realise immediately that children chasing a ball do not represent a threat. Whether AWSs could reach the same conclusion is however unclear, since ‘certain distinctions far surpass the abilities of today’s robotics, at least at this stage: distinguishing a weapon from a cultural or religious symbol; distinguishing the agonized face of a person in fear for her or his children from a threatening face; distinguishing children playing from threats’.⁸⁵ It seems unlikely that AWSs are capable of undertaking the highly context-dependent and essentially qualitative assessments that war situations often require.

A third concern about the use of killer robots relates to another basic principle of IHL, the principle of proportionality. According to the First Additional Protocol to the Geneva Conventions, the principle of proportionality is violated by an attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.⁸⁶ Such a qualitative exercise can hardly be carried out by AI systems.⁸⁷ Furthermore, by removing the human element from war, the use of killer robots can contribute to increase the number of deaths as there will be no room for those human feelings that play a role in war contexts (fear, compassion, etc).⁸⁸ Already in 2010, the special rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston,

⁸¹ *Ibidem* 60 ff.

⁸² R. Crootof, *op. cit.*, 1866–1868.

⁸³ See, for instance, N. Sharkey, ‘Automating Warfare: Lessons Learned from the Drones’ (2011) *Journal of Law, Information & Science* 140, 143–144.

⁸⁴ M. Wagner, *op. cit.*, 22.

⁸⁵ *Ibidem* 23. See also P. Alston, *op. cit.*, 54–55; T. Krupiy, ‘Regulating a Game Changer: Using a Distributed Approach to Develop an Accountability Framework for Lethal Autonomous Weapon Systems’ (2018) 50 *Georgetown Journal of International Law* 45, 48–50.

⁸⁶ Art 51(5)(b) of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

⁸⁷ N. Sharkey, *op. cit.*, 144–145; M. Wagner, *op. cit.*, 23 ff.

⁸⁸ *Ibidem* 40 ff.

singled out a similar problem with respect to the use of drones in war. He noted that drones may help developing what he called ‘a “Playstation” mentality to killing’.⁸⁹ If drones are controlled remotely, it will be easier for the ‘cubicle warriors’ who ‘operate from behind computer screens, physically far away from the battlefield’⁹⁰ to kill other persons than it would be for a soldier on the ground. The distance from the battlefield can become even greater when AWSs will be used; in this case, disincentives to kill can drastically decrease or even disappear. Furthermore, if AI systems are maliciously or improperly designed, their use can jeopardise the other fundamental principle of IHL according to which weapons that cause superfluous injury or unnecessary suffering shall be prohibited.⁹¹

Finally, it flows from the above that killer robots can easily end up committing international crimes. This brings the issue of AI systems’ criminal liability back up. The discussions and outcomes of section I of the Congress should therefore inform also the last section, as the attribution of criminal responsibility for (international) crimes committed by robots is an unresolved matter under ICL as well. In this context, the issue is perhaps even more complex since liability for international crimes usually involves high level politicians or civil servants (doctrine of command responsibility), and their liability may not be easy to detect when it comes to crimes committed by means of killer robots.⁹² The risk is to create a ‘system of organized irresponsibility that shuffles responsibility from one actor to another without holding anyone accountable in the end’.⁹³ Some authors therefore suggest to use a ‘distributed approach’ to accountability, which ‘ascribes responsibility to a senior political leader, a senior defense official responsible for promulgating policy on [lethal AWSs], a weapon manufacturer, a weapon designer, a military commander, and an operator’.⁹⁴ In practice, however, such a system may not play out well.

As is the case with cross-border cooperation on evidence gathering, therefore, an international approach on AWSs should be explored.⁹⁵ Some call for an absolute ban on the use of AWSs in war,⁹⁶ at least as long as their use is unlikely to be compliant with the core principles and rules of IHL,⁹⁷ while others support the conclusion of an international agreement that regulates the development and use of AWSs.⁹⁸ The XXI Congress will

⁸⁹ Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston (28 May 2010) A/HRC/14/24/Add.6, para 84.

⁹⁰ L. Royakkers and R. van Est, ‘The cubicle warrior: the marionette of digitalized warfare’ (2010) 12 *Ethics and Information Technology* 289, 291.

⁹¹ Cfr. M. Hagger and T. McCormack, ‘Regulating the Use of Unmanned Combat Vehicles: Are General Principles of International Humanitarian Law Sufficient?’ (2011) 21 *Journal of Law, Information & Science* 74, 80–81.

⁹² See, for instance, P. Alston, *op. cit.*, 51–52; J. D. Ohlin, ‘The Combatant’s Stance: Autonomous Weapons on the Battlefield’ (2016) 92 *International Law Studies* 1, 14 ff.; T. Krupiy, *op. cit.*, 51 ff.

⁹³ M. Wagner, *op. cit.*, 39.

⁹⁴ T. Krupiy, *op. cit.*, 45.

⁹⁵ Cfr. M. Brundage et al., *op. cit.*, 42.

⁹⁶ This position is supported by several NGOs, including ICRAC (International Committee for Robot Arms Control), which, together with other organisations, has launched the ongoing ‘Campaign to Stop Killer Robots’.

⁹⁷ It has been claimed that ‘[AWS] should not be deployed at all until the deploying country, and by extension the international community, has satisfied itself that doing so can be done consistent with the requirements of international humanitarian law’ (M Wagner, *op. cit.*, 51). See also Human Rights Watch, *op. cit.*

⁹⁸ G. Bills, ‘LAWS unto Themselves: Controlling the Development and Use of Lethal Autonomous Weapons Systems’ (2015) 83 *The George Washington Law Review* 176.

represent an invaluable occasion to discuss whether similar stances are feasible and really capable of reducing the significant risks connected with the use of killer robots.