Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?

Sunčana Roksandić[*], Nikola Protrka[**], Marc Engelhart[***]
[*] University of Zagreb, Faculty of Law, Zagreb, Croatia
[**] Police College, Zagreb, Croatia
*** Goethe University, Faculty of Law, Frankfurt a.M., Germany
suncana.roksandic@pravo.hr , nprotrka@fkz.hr, marcengelhart@web.de

Abstract - **From all kinds of industry, communication, education, banking, government, service, manufacturing, medical, and more, Artificial Intelligence (hereinafter: AI) applications may be found in many sectors of our life. Public safety and criminal justice are gaining advantages thanks to artificial intelligence. For example, traffic safety systems detect infractions and alert authorities. AI is also assisting in the identification of criminals. As a public safety resource, AI is being researched in a number of ways. Face recognition is becoming increasingly popular as an AI application in both the public and private sectors. For law enforcement authorities, AI applications boost efficiency, promote data-driven processes, and extend capabilities. AI technology can help law enforcement agencies make judgments and complete tasks in general. They can strengthen data-driven procedures, increase efficiency, or extend capabilities for specific activities or choices. However, recognized human rights as adjudicated by European Convention of Human Rights are calling for caution in the development and usage of AI within the European Union. Fair Trials and 114 civil society organizations have launched a collective statement to call for an Artificial Intelligence Act which foregrounds fundamental rights in November 2021. This Act is under preparation in the EU. Ethics Guidelines for Trustworthy AI from 2019 , by High Level Expert Group on Artificial intelligence set up by the European Commission, (hereinafter: Ethical Guidelines) are underlining how it is necessary to develop, deploy and use trustworthy AI systems in a way that adheres to the ethical principles of: respect for human autonomy, prevention of harm, fairness and explicability. European Parliament Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (hereinafter: Resolution) underlines that AI, alongside benefits, possesses great risks for fundamental rights and democracies based on the rule of law. AI should not be seen as an end in itself, but as a tool for serving people, with the ultimate aim of increasing human well-being, human capabilities and safety. In this article the authors will analyse some of the concerns taking into accounts principles set in Ethical Guidelines and human rights concerns. As the Regulation on AI is underway in the EU, the authors will stress some of the concerns that should be addressed in its wording.**

Keywords - artificial intelligence, analysis, law enforcement authorities, human rights, ethical guidelines, EU Resolution and Regulation on AI.

I. INTRODUCTION

Artificial intelligence (hereinafter: AI) is increasingly affecting our daily lives. The way the world uses data and linked technology will have a big impact on its growth and development. AI has the potential to drastically alter our lives — for better or worse . Global data production is anticipated to increase from 33 zettabytes in 2018 to 175 zettabytes in 2025 (one zettabyte is a thousand billion gigabytes). [1]

Some countries have already established themselves as leaders in the digital economy and business-to-business applications. With a high-quality digital infrastructure and a legislative framework that respects privacy and freedom of expression as well as other fundamental rights, the future looks bright. People might benefit from AI-assisted health care, safer automobiles and other modes of transportation, and customised, less expensive, and longer-lasting products and services. It may also make information, education, and training more accessible. Because of the Covid-19 outbreak, the requirement for distant learning has grown more urgent. AI may potentially make the workplace safer by allowing robots to perform risky tasks, as well as create new employment opportunities as AI-driven sectors expand and develop.

The criminal justice system is usually not (yet) among the most relevant AI fields, but becomes increasingly one of the most rapidly growing ones as it offers some enticing promises: Massive data sets could be processed quicker, prisoner flight risks could be assessed more correctly, and crime or even terrorist attacks might be foreseen and averted (preventive policing). Online platforms are already using AI to identify and respond to illegal and unacceptable online behaviour. Hence AI is expected to be employed increasingly in crime prevention (the field mainly dealt with by the police but also by intelligence agencies) and in the detection and prosecution of criminals (what is the classic task of the criminal justice system with its prosecution agencies and the courts).

However, the rapid growth of AI systems also poses potential risks and potentially violates human rights. This can be – what might be surprising – on the one hand stem from an underuse of AI systems. Underuse of AI may not only mean missed chances for the EU but also might result in inadequate implementation of significant programmes, such as the EU Green Deal. Besides the loss of competitive edge in comparison to other regions of the globe, economic stagnation, and less opportunities for people it might directly affect the right to health and security and even the right to life (in case of negative climate effects etc.). Underuse might be due to public and industry distrust of AI, insufficient infrastructure, a lack of initiative, low investments, or fragmented digital marketplaces, as AI's machine learning is data-dependent.

On the other hand, and this is often much more in the public focus, the overuse of AI can have negative effects on human rights. Overuse may be troublesome, when AI applications or the specific use of AI turn out to be ineffective, such as when used for explaining complicated social issues. This is especially true in the sphere of antisocial behaviour and hence in regard to the core field of antisocial behaviour, criminal delinquency. In this regard, the overuse of AI, or the usage of AI that is not trustworthy or that might infringe human rights calls for caution particularly in criminal matters and when used extensively for prevention, in law enforcement and within prison systems. This holds true especially for member states of the Council of Europe and the EU with their high human rights standards.[2]

One main aspect for AI use in the criminal sphere is that the outcomes of AI are determined by how it is created and the data it consumes. Both the design and the data might be skewed, either purposefully or accidentally. Some crucial features of a problem, for example, may not be coded into the algorithm (because of its vagueness and complexity), or the system may be built to reflect and perpetuate structural prejudices. In addition, using numbers to describe complicated social realities may give the impression that the AI is accurate and exact when it is not, as it is undercomplex. If done incorrectly, AI might lead to discriminatory choices based on race, sex, or age in criminal cases regarding investigation measures, detention decisions, recidism prognosis or dangerousness assessments (in addition to other problematic non-criminal fields such as hiring or terminating employees, making loans, etc.). The right to privacy and data protection may be seriously harmed by AI such as by the use of facial recognition technology, internet surveillance or profiling of persons. Furthermore, AI allows for the integration of data that a human has provided into fresh data, which might result in unexpected conclusions. It could also be used to make deepfakes, which are very realistic fake video, audio, and pictures that might not only pose financial hazards or ruin reputation but can also give rise to criminal prosecutions of the person faked. [3]

The pace of AI implementation varies substantially among countries. Some countries, including several EU Member States, make more use of AI applications, or embedded AI systems, in law enforcement and the judiciary than others, which is partly due to a lack of regulation and regulatory differences which enable or prohibit AI use for certain purposes. The increasing use of AI in the criminal law field is based in particular on the promises of much greater effectiveness (e.g. that it would reduce certain types of crime and that it leads to more objective decisions) and efficiency (which is of great attractiveness in overloaded justice systems) whereas these promises, however, do not always hold true.[4]

II. Artificial Intelligence and Law Enforcement

We now live in a period in which Al is a reality, and its effects on our everyday lives are quite substantial and profound. AI is changing our lives in a variety of ways, from phones to automobiles to money and medical care. AI is hence a rapidly evolving discipline of computer science and increasingly of the legal field. For our purposes AI can be described as a machine's ability to perceive and respond to its environment without requiring direct human involvement, as well as to do tasks that would ordinarily need human intelligence and decision-making processes. Machine learning is an AI application that simulates this ability and allows computers and software to learn from their mistakes.[5] Depending on how much weight is put on the element of “would need human intelligence” the field of AI is rather broad (if not meant literally) or rather narrow (if really tasks shall be fulfilled that up to now need human intelligence). This applies not only to the general use of AI in everyday life but also to its criminal justice application. The majority of systems still struggle with first steps of digitalization such as the introduction of electronic files reaching from the police investigation to the final court decision or electroniccommunication within the justice institutions and with these institutions. As the situation is in criminal cases more complex than in civil cases due to the number of parties involved (police, prosecution, courts, defendant, attorneys-at-law, experts, administrative agencies etc.) and the higher legal standards (procedural rights of the accused etc.) the implementation process takes time. This also means that “real” AI applications such as a robo-judge or a robo-prosecutor are not numerous and often in an experimental state.

In order not to limit the of AI applications to much, the Ethical Guidelines that a broader approach that is not so much connected to intelligent human decision making. In the Ethical Guidelines, AI systems are described 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. This means that 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. This is not completely like human decision making, but with respect to the element of learning much more then a preprogrammed solution pattern. As a scientific discipline, AI therefore 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).[6]In the criminal justice field all of these aspects are of relevance, although differing according to the stage of the proceedings. In the investigating phase more emphasis is placed on real time surveillance techniques whereas in the prosecuting and judicial phase data analysis and reasoning play a major role.

Among the AI systems already used in practice in the criminal justice system pattern recognition is very significant. Humans are good at spotting patterns, and we learn to distinguish things, people, complicated human emotions, information, and circumstances on a regular basis via experience. AI aims to duplicate these human capabilities in software algorithms and computer hardware. Self-learning algorithms, for example, use data sets to figure out how to recognize people based on their images, complete complex computational and robotics tasks.[7]

Examining a huge number of potentially relevant images and videos in a timely and exact manner is a time-consuming and arduous process prone to human error owing to weariness and other factors. Unlike humans, machines do not grow weary. Analysts are putting algorithms to the test to see whether they can learn to distinguish one person from another based on facial characteristics in the same way that a human analyst can like the Intelligence Advanced Research Projects Activity's Janus computer-vision project. In order to identify subjects, intelligence analysts may be asked to study still photographs or video recordings. Face recognition software that is automated is required to manage the massive amount of photos and video generated by the proliferation of cameras. This programme has traditionally performed well on frontal stances with good lighting, such as passport shots. When illumination is bad, resolution is low, features are obscured, camera angles change, and/or the facial expression is uncontrollable, it is less accurate "in the wild." The Janus initiative was launched in 2014 with the intention of revolutionising face recognition by combining data from many perspectives from various sensors and visual sources to achieve major improvements in speed and accuracy. Model-based matching was used in the software, and algorithms were built that were unaffected by subject position, light, or movement. The Janus program ran for five years and concluded in July 2020 with accomplishments: Based on independent assessment using test photos and sequences, algorithms that are twice as accurate as the most frequently used government-off-the-shelf systems; Achieved programme performance targets of 85 percent verification accuracy and 98 percent retrieval accuracy among the top 20 results from a 1 million topic gallery, with a false match rate of 1 in 100,000 and Searching large-scale repositories at near-logarithmic rates is possible. [8]

How important this automated recognition can be in the criminal justice sphere demonstrates a successful pilot project by the Ministry of Justice of the State of North Rhine-Westphalia, the Central and Contact Point Cybercrime (ZAC) of the Cologne Public Prosecutor's Office and Microsoft Germany.[9] A legally secure and hybrid cloud solution for the automated detection and categorization of online child and youth pornography was developed. Compliance with strict legal requirements was ensured by a specially developed abstraction algorithm that completely and irreversibly abstracts and anonymizes (deconstructs) the image files. After this deconstruction, no image content is recognizable to the human eye. This process takes place exclusively in the data centers of law enforcement agencies. It was able to correctly categorize images in 92 percent of all cases. As the AI-based analysis of the suspect material could take place both locally in the authorities' data centers (on-premises) and in Microsoft's German data centers it was possible to expand computing power at short notice and as needed, for example, to evaluate large volumes of data in parallel. This enables the authorities not only to save time and helps to decrease the psychological pressure on the persons screening the pictures and videos but also enables to uncover crimes that are still ongoing (and might therefore prevent ongoing child abuse more quickly).

Another important aspect of AI is its (alleged) ability to predict behaviour. This plays a major role in attempts to prevent crimes where research by now is e.g. extended to by making use of virtual environments in order to understand the criminal mind more in depth.[10] Instead of photographing and identifying illegal behaviour in progress, the University of Houston has developed algorithms that provide continuous monitoring to analyse activity and anticipate impending suspicious and criminal conduct over a network of cameras. Using clothing, skeletal structure, movement, and direction prediction, this research also focuses on recognising and re-acquiring individuals of interest across several cameras and pictures. [11] This means that AI must not only be able to analyse human behaviour but also be able to connect it to illegal acts as defined by criminal offenses.

One major aspect is also the identification of specific persons, even when only parts of them can be seen on a picture or video. For human re-identification, a prototype code was created that allows for the creation of a gallery probe from input videos and the matching of an input observation to the identifications in the gallery. The created prototype contains two modular components, despite the fact that it is not an integrated system for re-identification. A video is sent into one module, which does person detection and tracking. Tracking makes it possible to create a gallery or a probe dataset. Re-identification based on human components is included in the second module. To identify body sections, the photos in the selected gallery and probe datasets are first segmented. If numerous photographs of the person are available, an appearance description is created as a model for each body component and integrated over many images of the individual. This technology allows e.g. security officials to automatically watch surveillance recordings, which aids in the detection and prediction of suspicious activity, allowing for the prevention or mitigation of a security danger. For a range of applications, the ability to model basic activity patterns using video data from a single camera has been proven.

The issues that remain are connected to re-identification and human behaviour comprehension. [12]

Another use of AI algorithms tries to improve traditional forensic analysis. An example is the gunshot analysis with the recognition of pattern signatures: Audio files from cellphones and smart devices were analysed by Cadre Research Labs "based on the observation that the content and quality of gunshot recordings are influenced by firearm and ammunition type, scene geometry, and the recording device used". The Cadre scientists are developing algorithms to "detect gunshots, distinguish muzzle blasts from shock waves, determine shot-to-shot timings, determine the number of firearms present, assign specific shots to firearms, and estimate probabilities of class and caliber" using a well-defined mathematical model, all of which could help law enforcement in investigations. [13]Among the existing AI applications predictive analysis is one of the most challenging method. Traditional handmade predictions entails analysing massive volumes of data in order to anticipate and develop potential results. This is mostly the job of police officers, probation officials, and other professionals in the criminal justice system, who must accumulate experience over many years. The task is time-consuming and prone to bias and error. Using AI, large amounts of legal and legal precedent data, social data, and media may be used to make predictions on future anti-social behaviour, recommend rulings, detect criminal enterprises, and predict and report people who are vulnerable to criminal enterprises. AI can also being used to predict potential victims of violent crime based on relationships and behaviour. The Chicago Police Department and the Illinois Institute of Technology used algorithms to collect data and create initial classifications in order to develop social networks and conduct analysis in order to identify potential high-risk individuals.[14]

Such predictive policing yet often promises more than it can – at least at this moment of time – keep. The reliability of the predictions are often limited or to general in order to be really helpful. The success of offense-based predictions (that would allow to allocate police resources more precisely) is not very high: a project in Baden-Württemberg on predicting burglaries (based on a near-repeat approach) was abandoned after the pilot phase.[15] If person-based predictive policing approaches are more reliable is not clear; at least such AI based predictions allow to take into account a large number of different criteria based on a large amount of data and are – at least in theory – not so much prone to subjective and biased decision making as human prognosis making is.[16]

The examples demonstrate that AI can boost efficiency and effectiveness, but that one has to look in detail at the respective application. This means especially that the development and usage of AI in law enforcement within EU and Council of Europe member states must follow human rights concerns and be regulated according to already guaranteed procedural rights and level of guaranteed human rights. In that vein, aforementioned EU Resolution for example expresses its great concern over the use of private facial recognition databases by law enforcement actors and intelligence services, such as US based privately owned company Clearview AI , a database of more than 10+ billion pictures that have been collected from public web sources, including social networks and other parts of the internet, and including from EU citizens.[17]; the general use of a service such as Clearview AI by law enforcement authorities in the European Union would not be consistent with the EU data protection regime. But one can imagine narrow exceptions such as the use of the respective data in order to identify war crime criminals or victims in conflicts such as the war in the Ukraine.[18] To that extent the general call for a ban on the use of private facial recognition databases in law enforcement – the position of the aforementioned EU Resolution – demonstrates a typical problem of the current debate thinking in black and white boxes which does not do justice to the complexity of AI applications. . This can be different for other aspects, e.g. a ban on AI-enabled mass scale scoring of individuals [also provided for by the resolution [19]] seems quite considerate as a any form of normative citizen scoring on a large scale by public authorities, in particular within the field of law enforcement and the judiciary, would lead to the loss of autonomy, endanger the principle of non-discrimination and thus seriously impedes core fundamental rights (right to privacy, the general freedom to act and, in particular human dignity). But even in this case the approach might be to general if it includes e.g. (the very common) credit scoring. In order to better understand and regulate this area, a crucial element is greater transparency of the use of AI applications in the EU so that states should provide information on the tools used by their law enforcement and judicial authorities, the types of tools in use, the purposes for which they are used, the types of crime they are applied to, and the names of the companies or organisations that developed those tools. In addition, there is a need for information on the usefulness of AI application, such as on ; false positive and false negative rates or the difference (improvement?) to the situation before. This means implementation of AI and evaluation need to go hand in hand in order to assess the success and the risk of the often fundamental changes in criminal justice administration. The analysis should not only focus on the EU countries, but also take into account the situation worldwide. The EU might be more restrictive than other states but in the context of international cooperation the use of extensive AI applications and the legality of these AI technologies and applications in use by law enforcement authorities and the judiciary can reappear. If the EU is restrictive on the use of AI but accepts information other states collect as evidence by extensively exploiting the AI potential no high standard of human rights protection is achieved. The current cases of the use of FBI information by national prosecutors among Europe that stems from a FBI measure (where the FBI set up its own encrypted device company, called “ANOM”), a measure not possible in most Europeans states, is a vivid example of such an internationalized criminal justice field.[20] This means thatthe EU must lobby to raise standards at international level and to find a common and complementary legal and ethical framework for the use of AI, in particular for law enforcement and the judiciary, that fully respects European (human rights) standards (of data protection such as in the relevant directive for law enforcement agencies [21], privacy etc.). To that extent specific guidelines for individual measures (e.g. on person-based predictive policing) would be helpful, and respective legislation essential.

A sign of recognition of this problem at the EU level is visible in adoption of The General Data Protection Regulation 2016/679, [22] particularly it's Article 22(1): (that builds on the EU Directive 95/46 from 1995).

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. EU Commission considers this step as part of the "EU's sustainable approach to technologies" by "embracing change on the basis of the Union's values" [23]. Although this is an important regulation, the mere existence of the rule since 1995 also indicates that the EU so far has made no difference between automatization and AI. But, and this hhas also been emphasised by Roksandić et al., with that proclamation, among others, the EU defined its basic approach and boundaries for developing and using AI systems: Therefore, EU values are the guiding principles not only in reviewing existing regulations but also in proposing new ones that will correspond to growing usage of AI in everyday life and in setting boundaries in 'furnishing products with artificial intelligence.'[24]

III. ARTIFICIAL INTELLIGENCE ACT WHICH FOREGROUNDS FUNDAMENTAL RIGHTS - EXPECTING EU'S AI ACT

The aforementioned Resolution can be seen as a forerunner of a Regulation on AI in the EU. Currently, a Proposal for a Regulation of the EU Parliament and of the Council laying down harmonised rules on AI (AI Act) and amending certain EU legislative acts is under way. [25]

It is clear that "the horizontal nature of the proposal requires full consistency with existing Union legislation applicable to sectors where high-risk AI systems are already used or likely to be used in the near future". Hence the proposal is also without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) with a set of harmonised rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems. Furthermore, the proposal complements existing Union law on non-discrimination with the necessary specific requirements that aim to minimise the risk of algorithmic discrimination, in particular in relation to the design and the quality of data sets used for the development of AI systems complemented with obligations for testing, risk management, documentation and human oversight throughout the AI systems' lifecycle.[26] According to the Proposal (para 27), high-risk AI systems should only be placed on the Union market or put into service if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation minimises any potential restriction to international trade, if any. It is to be welcomed that the Proposal does not only take a broad approach in regard to high risk AI systems so that a broad protection mechanism is established but that it also does specifically address law enforcement agencies. The Proposal names important areas such as AI systems intended to be used by law enforcement authorities for individual risk assessments, polygraphs and similar tools or to detect the emotional state of natural person, to detect 'deep fakes', for the evaluation of the reliability of evidence in criminal proceedings, for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons, or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences, as well as for crime analytics regarding natural persons.[27]

Although these examples (in the introductory comment) are a good illustration of the most problematic issues, the Proposal is not limited to such serious usage, but includes a much broader concept of high-risk systems. To that extent it is doubtful if this approach is not too general as in the legal regulation itself it neither does substantially differentiate between levels of high risk systems not does it address more in detail the vast field of law enforcement activities. Also, if a system is not classified as high risk, there are hardly any rules to follow although there are many systems that can have an "indirect midlevel" effect on citizens. Especially digital systems within police or criminal justice authorities where there is no direct contact to outsiders may have a significant impact just by the way how files are organised, stored or how cases are worked up.

Is is emphasised in the Proposal that "the obligations for ex ante testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary. In case infringements of fundamental rights still happen, effective redress for affected persons will be made possible by ensuring transparency and traceability of the AI systems coupled with strong ex post controls."[28]. In addition, "the proposal also prohibits AI-based social scoring for general purposes done by public authorities. Finally, the use of 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply." [29] Again, the intended far reaching protection mechanism in regard to faulty AI decisions and remedy measures, the restrictions on scoring and biometric use are to be welcomed as the offer more regulation than we had before. Yet, again, the proposal does not do justice to the variety of existing (and possible) AI applications. In this context it is not possible to go too much into the details of the proposed legislation; but – pars pro toto – the handling of the fair trial principle, one of the corner stones of a just criminal proceeding, is illustrative: The fair trial principle is mentioned several times in the introductory commentary (e.g. para. 28, 38, 40) but is not explicitly taken up later in the regulations. Of course one could argue that the various rules on transparency, risk control etc. contribute to guaranteeing fair trials. But these rules remain rather general. A right of the defense to be informed about relevant criteria, the algorithm and the impact of an automated calculation e.g. in risk assessments used for decisions on the suspension of an arrest warrant or in regard to probation decisions would have been much more adequate and specific for dealing with risks and opportunities AI applications offer. But to do the EU efforts on AI regulation some justice other proposals in the field, such as the one from 114 civil society organisations, among which is also Fairtrials, that have "launched a collective statement to call for an Artificial Intelligence Act which foregrounds fundamental rights" on November 30, 2021 follow a similar general approach.[30] In their Collective Statement, the signatories call for, among others: Prohibitions on all AI systems that pose an unacceptable risk to fundamental rights including a ban on the use of AI systems that attempt to profile and predict future criminal behaviour; Obligations on users of (i.e. those deploying) high-risk AI systems to facilitate accountability to those impacted by AI systems; Consistent and meaningful public transparency; Meaningful rights and redress for people impacted by AI systems; A cohesive, flexible and future-proof approach to the risk of AI systems; A truly comprehensive AI Act that works for everyone.[31]

The civil society organisations called on the Council of the European Union, the European Parliament, and all EU member state governments to ensure that the forthcoming Artificial Intelligence Act achieves the 9 goals as follows: A cohesive, flexible and future-proof approach to 'risk' of AI systems (1); Prohibitions on all AI systems posing an unacceptable risk to fundamental rights (2); Obligations on users of high-risk AI systems to facilitate accountability to those impacted by AI systems (3); Consistent and meaningful public transparency (4); Meaningful rights and redress for people impacted by AI systems (5); Accessibility throughout the AI life-cycle (6); Sustainability and environmental protections (7); Improved and future-proof standards for AI systems (8); A truly comprehensive AIA that works for everyone (9).

IV. CONCLUSION

The recent development shows that the EU is openly awareof concerns over the extensive usage of AI in law enforcement and judiciary and does not unreservedly welcome the dynamic technical revolution. But the picture of possible advantages and disadvantages and the necessary legal requirements are by far not clear. On a general level it is clear that some usage could infringe human rights and would be contrary to human dignity. E.g., as stated in the EU Resolution, the use and collection of any biometric data for remote identification purposes, for example by conducting facial recognition in public places, as well as at automatic border control gates used for border checks at airports, may pose specific risks to fundamental rights, the implications of which could vary considerably depending on the purpose, context and scope of use; it further highlights the contested scientific validity of affect recognition technology, such as cameras detecting eye movements and changes in pupil size, in a law enforcement context; and it is of the view that the use of biometric identification in the context of law enforcement and the judiciary should always be considered 'high risk' and therefore be subjected to additional requirements, as per the recommendations of the Commission's High-Level Expert Group on AI[30]. In the Proposal of the EU Regulation on AI, the regulation of real time biometric AI use (Art. 5) is constructed as a general prohibition with a number of exceptions that leave the impression that the exception is rather the general rule.[31] In addition, the requirements for exceptions are vague and the protection mechanism for individuals are scarce, although the measure is not even classified as a high-risk AI use but as a prohibited AI application. Insofar the Proposal sets some limits for the actions by law enforcement authorities and diminishes the existing significant degree of power imbalance with its risks of overdue surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights. But it does not give clear guidance and specific protections mechanism for criminal proceedings. So the first big steps to address AI use in the criminal justice sphere have been taken, but many more smaller steps have to follow.

It is therefore especially recommendable that Ethical Guidelines on AI not only set the main principles that would and should be used in development and usage of AI in the EU but also that they take up much more the already existing diversification of AI applications and provide for specific criteria to differentiate useful and harmful applications and a legal protection mechanism that takes these differences into account. It would be a substantial progress if the the AI Act would take up and would be in line with those principles.

Every day, new AI applications in criminal justice emerge, paving the door for future opportunities to assist the criminal justice system and, in turn, promise to improve public safety. Data pattern analysis might be utilised to disrupt, degrade, and indict illegal operations and activities. Algorithms might also help criminal justice professionals protect the public in previously unimagined ways by preventing victims and prospective offenders from slipping into illicit pursuits. AI technology has the potential to provide situational awareness and context to law enforcement, allowing officers to make better-informed decisions in potentially dangerous situations. AI has the potential to become a permanent part of our criminal justice system, supporting investigators and law enforcement authorities in their efforts to better safeguard the public. This technical development should be accompanied by a sound and reasonable legal framework effectively providing for human rights safeguards.

REFERENCES

[1] European Parliament (2021) European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))

[2] Roksandić Vidlička, S.; Elīna Liepiņa, L.; Ostapchuk, S, (2019), Bioethical and Legal Challenges of Artificial Intelligence and Human Dignity // Human rights in 21st century / Jovanović Miodrag ; Virady Tibor (eds.), Netherlands: Eleven International Publishing, 2020. pg. 269-288

[3] Kritikos, M. (2019) Artificial Intelligence ante portas: Legal & ethical reflections, European Parliammentary Research Service, Scientific Foresight Unit (STOA), available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634427/EPRS_BRI(2019)634427_EN.pdf [accessed 13.1.2022]

[4] European Parliament (2021) European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) , Recital C

[5] Brynjolfsson, E.; McAfee, A. (2017) The Business of Artificial Intelligence: What It Can — and Cannot — Do for Your Organization, Harvard Business Review

[6] Ethics Guidelines for Trustworthy AI, High Level Expert Group on Artificial intelligence set up by the European Commission, 2019, available at: https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf [accessed 13.1.2022]

[7] Giosué Lo Bosco, G.; Di Gangi, A. (2017) Deep Learning Architectures for DNA Sequence Classification, Fuzzy Logic and Soft Computing Applications

[8] National Science and Technology Council and the Networking and Information Technology Research and Development Subcommittee (2016) The National Artificial Intelligence Research and Development Strategic Plan (pdf, 48 pages), Washington, DC: Office of Science and Technology Policy, October 2016.)), available at: https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf [accessed 13.1.2022]

[9] Microsoft Germany (2021), Künstliche Intelligenz bewährt sich im Einsatz gegen Kinderpornografie; available at: https://news.microsoft.com/de-de/kuenstliche-intelligenz-im-einsatz-gegen-kinderpornografie/ [accessed 22.4.2022].

[10] Gelder JL Van et al., (2019) The virtual reality scenario method: Moving from imagination to immersion in criminal decision-making research, Journal of research in crime and delinquency 56 (3), 451-480

[11] IARPA (2021) The Intelligence Advanced Research Projects Activity, "Janus," Washington, DC: Office of the Director of National Intelligence, available at: https://www.iarpa.gov/index.php/research-programs/janus [accessed 13.1.2022]

[12] University of Houston (2015) Learning Models for Predictive Behavioral Intent and Activity Analysis in Wide Area Video Surveillance, NIJ award number 2009-MU-MU-K004, available at: https://nij.ojp.gov/library/publications/learning-models-predictive-behavioral-intent-and-activity-analysis-wide-area [accessed 13.1.2022]

[13] Cadre Research Labs (2016) Development of Computational Methods for the Audio Analysis of Gunshots, NIJ award number 2016-DN-BX-0183, available at: https://nij.ojp.gov/funding/awards/2016-dn-bx-0183 [accessed 13.1.2022]

[14] Illinois Institute of Technology (2011) Chicago Police Predictive Policing Demonstration and Evaluation Project at the Chicago Police Department, NIJ award number 2011-IJ-CX-K014, available at: https://nij.ojp.gov/funding/awards/2011-ij-cx-k014 [accessed 13.1.2022]

[15] Dominik Gerstner, Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany, European Journal for Security Research volume 3, pages 115–138 (2018); see also Sommerer L (2017) Geospatial Predictive Policing—Research Outlook. A Call For Legal Debate. NK Neue Kriminalpolitik. Forum für Kriminalwissenschaften, Recht und Praxis (2), pp. 147–164. https://www.nomos-elibrary.de/10.5771/0934-9200-2017-2-147/geospatial-predictive-policing-research-outlook-a-call-for-legal-debate-jahrgang-29-2017-heft-2 [accessed 22.4.2022]

[16] Tzu-Wei Hung & Chun-Ping Yen, On the person-based predictive policing of AI, Ethics and Information Technology volume 23, pages 165–176 (2021).

[17] European Parliament (2021) European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) , para 28.

[18] Paresh Dave and Jeffrey Dastin, Exclusive: Ukraine has started using Clearview AI's facial recognition during war (March 14, 2022). https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/ [accessed 22.4.2022]

[19] European Parliament (2021) European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) Para 32.

[20] Department of Justice, U.S. Attorney's Office, Southern District of California, FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown (June 8, 2021), https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive [accessed 22.4.2022].

[21] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016, http://data.europa.eu/eli/reg/2016/679/2016-05-04

[23] European Commission, Communication from the European Commission to the European Parliament, the European Council, the Council, the European Economic and Social committee and the Committee of the Regions (COM(2018)237 final), Artificial Intelligence for Europe, 2018, p. 20, https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe [accessed 13.1.2022]. See also European Parliament (2021) European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) , para 28, Para 35

[24] Roksandić Vidlička, S.; Elīna Liepiņa, L.; Ostapchuk, S, (2019), Bioethical and Legal Challenges of Artificial Intelligence and Human Dignity // Human rights in 21st century / Jovanović Miodrag ; Virady Tibor (eds.)., Netherlands: Eleven International Publishing, 2020.pg. 269-288, pg. 276.

[25] European Commission, PROPOSAL FOR THE REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussels, 21.4.2021, COM(2021) 206 final, 2021/0106(COD), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 . [accessed 13.1.2022]

[26] Ibid, 1.2.Consistency with existing policy provisions in the policy area.

[27] Ibid, 3.5.Fundamental rights.

[28] Ibid. 5.2.2. Prohibited Artificial intelligence Practises (Title II).

[29] Ibid. Para 38.

[30] Fair Trials calls for an EU Artificial Intelligence Act for fundamental rights, News, November 30 2021, available: https://www.fairtrials.org/articles/news/fair-trials-calls-eu-artificial-intelligence-act-fundamental-rights/

[31] EU Artificial intelligence Act for Fundamental Rights. A Civil Society Statement (2021), December 31, 2021, available: https://www.fairtrials.org/app/uploads/2022/01/Political-statement-on-AI-Act.pdf

[32] European Parliament (2021) European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) , para 30.

[33] European Commission, PROPOSAL FOR THE REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussels, 21.4.2021, COM(2021) 206 final, 2021/0106(COD), para 38.