Implications of New Technologies on Criminal Justice System

Marina Matic Boskovic*

Abstract

The crime landscape has changed tremendously in the past years due to advancement in technology. The technological innovations from the end of XX century have transformed nearly every component of the criminal justice system. Technology has become a key component of most criminal activities and enables significant level of flexibility for criminals. Technology also significantly supports law enforcement authorities in prevention, detection, investigation, prosecution and enforcement of criminal sanctions. The author in the paper analysis the key benefits of the new technology for efficiency of the criminal justice system, as well as areas of human rights concern. Special area of concern is use of artificial intelligence and predictive models in the policing, investigation and enforcement of criminal sanctions. Some of the new technology were already part of the European Court of Human Rights jurisprudence and developed standards should be embedded in the legislation. The needed balance between human rights protection and efficiency of criminal investigations could be established through comprehensive assessment of the new technology prior to its adoption by policy makers. In addition, the evaluation system has to be established to monitor application of the new instruments in practice and enable timely review of instruments in case of human rights infringement.

Keywords: *technology, human rights, cybercrime, predictive models, internet, criminal justice*

I. Introduction

The development and extensive use of information and communication technologies has generated new forms of crime or new forms of perpetrating crimes and consequently new types of evidence[1]. Starting in the 1980s, personal computers became available for home use, and as of 2019, 83 percent of households in the European Union had access to a personal computer, while in Serbia 73 percent of household had at least one computer[2]. As a consequence of advancement of computer technology today we have global banking, in which complex transactions can be

* Research Fellow, Institute for Criminological and Sociological Research, Belgrade, Republic of Serbia. Contact: m.m.boskovic@roldevelopmentlab.com.

[1] Evidence – European Informatics Data Exchange Framework for Courts and Evidence – Overview of existing legal framework in the EU Member States, 2015, available at: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf 26.12.2020.

[2] Proportion of households having access to a personal computer 2014-2019, (2020) Eurostat, available at: https://ec.europa.eu/eurostat/statistics-explained/index.php? title=File:Proportion_of_households_having_access_to_a_personal_computer,_2014_and_2019_(%25)_CPC20.png 25.12.2020.

completed electronically. Information is also available to us more quickly due to development of internet. By 2019, the share of EU households with internet access had raisin to 90 percent and in Serbia to 80 percent[3]. Certainly, these advances in technology have changed the life.

Offenders very quickly integrate new technologies in their operations. The use of new technologies is especially spread among organized criminal groups and includes cybercrime, online trade of illicit goods and services, use of encrypted communication channels by criminals for impediment of detection, investigation and prosecution of crime, new forms of payment such as crypto currencies etc.[4].

Advancement of technology also put in the risk consumers who are exposed to online scams and fraud, which can affect consumer confidence and could lead to a reduction in consumer expenditure and function of digital market. Recently conducted survey in EU on Scams and Fraud Experience by Consumers, showed that slightly more than half of Europeans personally experienced one of the types of scams and fraud[5] in the last two years, when purchasing goods or services[6]. As a consequence there is substantial level of concern among online consumers about potential misuse of their personal data or theft of their credit card details[7]. It is estimated that in the EU adult population incurred 24 billion EUR of financial losses resulting from scams and fraud over a two-year period[8].

Technologies also facilitated prevention, detection, investigation, prosecution and enforcement of sanctions[9]. With most of lives organized online, especially in time of COVID-19 pandemic and introduced restrictions, people are using latest technologies to communicate with friends, families and colleagues. Many countries introduced e-government to more efficiently interact with citizens and businesses. Spread of the technology has a consequence creation of digital traces. Criminal activities are also conducted using ICT and evidence in criminal cases nowadays are very often in electronic form. The electronic evidence has to be handled by using specific methods to secure its authenticity and integrity, since it can be easily modified, overwritten or deleted[10].

Recent decades have seen the emergence of closed-circuit television (CCTV) surveillance as a mainstream crime prevention measure used around the world. Use of CCTV is based on the crime prevention strategy by reducing criminal opportunities and increasing the perceived risk of offending through modification of the physical

---

[3] Digital economy and society statistics – households and individuals, (2020) Eurostat, available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_ and_individuals#Internet_access 25.12.2020.

[4] Crime in the age of technology, (2017) Europol, 3.

[5] Types of scams and fraud that were included in the survey includes buying scams, identity thefts and monetary fraud.

[6] Survey on Scams and Fraud Experienced by Consumers – Final Report, January 2020, European Commission, 10.

[7] The 2015 DG JUST study on "Perceived and actual barriers with online (cross-border) purchases" found that 30% of online consumers were concerned that personal data may be misused and 25% that payment card details may be stolen while shopping online domestically.

[8] Survey on Scams and Fraud Experienced by Consumers – Final Report, 15.

[9] Smith, G. R, (2007) Crime Control in the Digital Age: An exploration of Human Rights Implications, *International Journal of Cyber Criminology*, Vol. 1, Issue 2, 167-179.

[10] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, 157.

environment[11]. Findings of the assessment show that CCTV is associated with a significant and modest decrease in crime[12]. Surveillance technology can also enhance the investigation of crime.

Computers will offer nearly unlimited possibilities for aggregating information and sharing it with other criminal justice agencies. Due to development of technology within the European Union the Prüm Decision allows the exchange of basic fingerprints, DNA and vehicle registration data[13].

New technologies are also used in trials and in judicial decision making-for example, computer models based on social science research are used in assessing the likelihood of recidivism. The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool produces a risk score that predicts a person's likelihood of committing a crime in the next two years and is widely used by courts across the USA[14].

COVID-19 pandemic and measures of social distancing have impact on court operations. Majority of countries were looking for solutions that would limit interaction with courts and suspension of non-urgent cases was one of the applied measures. To enable functioning of the courts, countries where level of information technology development allowed introduced modalities of online hearings and/or other use of modern technologies during proceedings like electronic filing[15].

The new technologies such as electronic bracelets are being used in corrections. Electronic monitoring has been used in Europe since the 1990s and continues to expand[16]. It is predominantly been used to enforce curfews and home detention, but newer technologies are emerging and can help create and monitor exclusion zones.

Although technologies enabled criminal justice authorities to prevent and investigate crimes and offered many protections for suspects and accused persons, risks of violation of human rights have arisen from the modalities of law response to cybercrime.

The policy makers sometimes include novelties attracted by development and efficiency of technology without thorough assessment of influence on human rights. Fundamental rights, democracy and the rule of law need to be protected in cyberspace while protecting against incidents, malicious activities and misuse[17]. These rights and freedoms also include the right to a fair trial, in particular when preparing a defense case where electronic evidence is included.

---

[11] Clarke, R.V. (1995) Situation crime prevention, *Crime and Justice*, Vol. 19, 90-160.

[12] Piza, E., Welsh, B., Farrington, D. and Thomas, A. (2019) CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis, *Criminology and Public Policy,* Vol 18, Issue 1, 135-159.

[13] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime; Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[14] Brennan, T., Dieterich, W., Ehret, B., (2009) Evaluating the predictive validity of the COMPAS Risk and Needs Assessment System, *Criminal Justice and Behavior,* Vol. 36, Issue 1, 21-40.

[15] Kostic, J., Matic Boskovic, M., (2020) How COVID-19 Pandemic influences Rule of Law backsliding in Europe? In. M. Reljanović (ed.) Regional Law Review, Institute of Comparative Law, Belgrade, 77-91.

[16] Nellis, M., (2014) Understanding the electronic monitoring of offenders in Europe: expansion, regulation and prospects, *Crime, Law and Social Change*, Vol. 62, Issue 4, 489–510.

[17] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 2.

In the article benefits of use of new technologies will be briefly assessed as well as challenges in using technologies in regard to human rights protection.

II. Benefits of use of new technologies

The benefits of the new technologies for prevention, detection, prosecution and enforcement of criminal sanctions are without doubts. Several analyses confirmed that use of technology contributed to all segments of the criminal justice system.

The new technology and tools are used for the prevention of crime, through predictive models that use geospatial modeling for predicting future crime concentrations[18]. The police in USA are using tools of data mining, machine learning and artificial intelligence to make accurate predictions and applied it to human resource management[19].

Police across the world are using artificial intelligence tools to detect the preparatory phase of crime. Technology tools are using large amount of data that are collected and supposed to excavate planners of crimes which are yet to be committed. The tools are also used to detected already committed crimes based on database that contain information on victims, perpetrator, risky places, or other items, such as background noise in the video[20].

The new technologies are also used by courts to assess the likelihood of recidivism and the likelihood of those awaiting trial to escape, or of offenders in bail and parole procedures. The courts in the USA are using different software for analysis of likelihood and predictions.

The use of CCTV as tool for prevention of corruption resulted in the decrease of crime rate, dure to increase offender hesitate to commit crimes at places covered by surveillance. Furthermore, CCTV has the potential to assist police after crimes are committed to identify offender[21] and to provide visual evidence for use in criminal investigations[22]. In addition, accused persons are more willing to plea guilty when there is visual evidence[23]. The CCTV also has potential to have impact on increase of reported crime, since CCTV can detect crimes that would have otherwise gone unreported[24].

Advancement of technology, both computer and medical have impact on the criminal justice system. Arguably the most important advance has been the DNA testing and their effect on legal outcomes by providing certainty about identity in a wat that has not been possible before. Cross-border crimes and establishment of

---

[18] McClendon, L., Meghanathan, N., (2015) Using Machine Learning Algorithms to Analyze Crime Data, *Machine Learning and Applications: An International Journal*, Vol. 2, No. 1, 1-12.

[19] Eck, J.E., Chainey, S., Cameron, J.G., Leitner, M., Wilson, R.E., (2005) Mapping Crime: Understanding Hot Spots, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/209393.pdf 28.12.2020.

[20] Završnik, A., (2020) Criminal justice, artificial intelligence systems, and human rights, *ERA Forum* 20**,** Springer, 567-583.

[21] Ratcliffe, J., (2006) Video surveillance of public places, Problem-Oriented Guides for Police – Response Guide Series, Guide No. 4, U.S. Department of Justice Office of Community Oriented Policing Services, Center for Problem-Oriented Policing.

[22] Ashby, M. P. J., (2017) The value of CCTV surveillance cameras as an invstigative tool: An empirical analysis, *European Journal on Criminal Policy and Research,* Vol. 23, Issue 3, 441-459.

[23] Piza, E., Welsh, B., Farrington, D. and Thomas, A., 139.

[24] Winge, S., Knutsson, J., (2003) An evaluation of the CCTV scheme at Oslo central railway station. *Crime Prevention and Community Safety,* Vol. 5: 49- 59.

national DNA databases incentivize exchange of DNA profiles among countries, but also development of international database. At the international level Interpol established DNA Gateway database that provides member states with the opportunity to load DNA profiles and access to submitted profiles through 24/7 communication system[25]. While in the EU, article 4 of the Council Decision 2008/615/JHA allows direct access to other countries database to compare unidentified DNA profiles from one EU Member State with all DNA profiles from another national DNA database for the investigation of criminal offences.

Although technology is advancing the fingerprints identification continuous to form an integral part of the detection of a wide range of crime types, especially volume crime such car thefts and burglary[26]. Due to development of computer many law enforcement agencies have abandoned the practice of taking ink fingerprints of those arrested and have purchased technologies that instead allow them to take digital fingerprints, which can then be instantly transmitted to database to search for a match. Technology enables faster and more accurate searches. Automatic fingerprint matching can perform fingerprint comparison at the rate of tens of thousands of times each second, and the result can be sorted according to the degree of similarity and combined with any other criteria that may be available to further filter the candidates, all without human intervention[27].

Another technology assisting law enforcement as the effective means of criminal investigation is the Global Positioning System (GPS) tracking devices. Electronic tracing can be distinguished from electronic surveillance equipment in that the location of the subject is the primary goal of tracking. The GPS tracking devices are used in investigation of crimes, but also in enforcement of criminal sanctions. In USA GPS is used for enforcing more complicated supervision orders[28]. As an investigation tool, the GPS devices and technology got public interest with the Scott Peterson trial in 2004, when police attached GPS devices to a number of Peterson's vehicles to track his movement after disappearance of his wife[29]. The Peterson trial was the first case in USA when judge allowed the GPS evidence into trial.

III. Challenges for human rights

Although new technology contributes to the efficiency of the criminal justice system, there should be stressed that the same rights that people have offline must also be protected online[30]. The focus on the relationship between new technology and

[25] Matić Bošković, M., (2019) DNA profiles and database – relevance and ethical dilemmas in criminal justice, In: Stevanović, I., Vujičić, N. (ed.), *Kazneno pravo i medicina*, Institute for Criminological and Sociological Research, Belgrade, 337-351.

[26] Adderley R., Bond J. (2008) Police Forensic science performance indicators – a new approach to data validation. In: Ellis R., Allen T., Petridis M. (ed.) Applications and Innovations in Intelligent Systems XV, SGAI 2007, Springer, London, 163-174.

[27] Moses, K. R., (2011) Automated Fingerprint Identification System, In: Fingerprint Sourcebook, National Institute of Justice, Washington DC.

[28] Roman, J. K., Liberman, A. M., Taxy, Sm., Downey, P. M. (2012) The Costs and Benefits of Electronic Monitoring for Washington D.C, Urban Institute, Washington D.C.

[29] Elmes, G.A., Roedl, G., Conley, J., (2014) Forensic GIS: The Role of Geospatial Technologies for Investigating Crime and Providing Evidence, Springer.

[30] United Nations, Human Right Council, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A/HRC/21/L.6 (21 September

human rights is relatively new. The debate on the issue was initiated in 1968, during the International Conference on Human Rights in Teheran, which resulted in adoption of Resolution 2450 (XXIII) which invited the Secretary General to begin a process of interdisciplinary studies to define appropriate standards of protection of human rights and fundamental freedoms against the potential impact of new technologies[31].

Use of the technology in the detection, investigation and prosecution of crime, as well as in the enforcement of criminal sanctions impose risks of infringement of human rights. Information technologies, for example, can lead to gross violation of individual privacy. The ability to monitor computer usage creates a number of potential human rights concerns including infringements of human freedom, freedom of thought and expression, and the right to privacy, but also right to fair trial and presumption of innocence.

To ensure human rights protection in investigation of cybercrime different international and regional instruments are adopted. The Council of Europe's Convention on Cyber crime (2001) incorporates various provisions designed to safeguard human rights norms and privileges in connection with cyber crime investigations, such as requirements for judicial or other independent supervision, proportionality, and respect for and consideration of the rights of third parties. Given the strength of the provisions allowing search, seizure and surveillance, however, these have been criticized by some privacy advocates as being inadequate.

The key instruments within the Council of Europe are the Ethical Charter on the use of artificial intelligence in judicial systems that the European Commission for the Efficiency of Justice (CEPEJ) has adopted and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The case-law of the European Court of Human Rights is also crucial when it comes to respecting private life, liberty, security and providing effective remedies to challenge intrusions into private life and to protect individuals from unlawful surveillance, including surveillance conducted through using of the new technology.

a. Discrimination

Inclusion of artificial intelligence to help police determine where the next crime spot might be or to determine the risk that a person awaiting criminal trial poses to society was followed by explanation that decisions are impartial, objective and based on facts[32]. However, the critics of the artificial intelligence and prediction models have demonstrated that these neutral systems replicate biases inherent in the data they are trained on or translate the particular ways of thinking into code[33]. If a system is fed with human biases, even unconscious, the result will inevitably be bias, thus reinforcing discrimination and prejudices.

2012), available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session21/A.HRC.21.L.6_en.doc 25.12.2020.

[31] Coccoli, J., (2017) The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era, *Peace Human Rights Governance*, Vol. 1, Issue 2, 223-250.

[32] Miller, AP. (2018) Want less-biased decisions? Use algorithms. *Harvard Business Review*, July 26. https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms 28.12.2020.

[33] O'Neil, C., (2016) Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, New York, Crown Publishers.

Predictive policing has raised concern, since this became the predominant model of policing[34]. Country specific studies of predictive policing implemented in Germany[35], and UK[36] raised question of objectivity of the model, since inputs for automated calculation of future crime are given by police. As a consequence, a police choices, priorities and omissions become the inputs algorithms use[37].

In the USA tools for assessing criminality have been used in criminal justice for decades. However, the recent studies around bail, sentencing, policing and parole from criminal justice system demonstrated that racial and ethnic profiling leads to harsher criminal sentences for certain groups. Assessment of COMPAS, a predictive model of the risk of criminal recidivism, used until recently by various courts in the USA to support judges' decisions on release request, showed that model has strong racist bias. The model assigned a double risk to backs who will not actually commit a crime compare to whites in the same conditions[38]. The model, presumably inherited the bias present in the historical sentences and is affected by the fact that the American prisons population over-represents blacks.

Due to restricted budget resources and increase caseload, the European countries are also looking into predictive models as solution to improve efficiency of criminal justice systems. However, the policy makers in Europe are cautious and adopted several instruments to mitigate possible risks. The European Union Fundamental Right Agency warns that decision making based on predictive models and other related methods is relatively new and there is need to develop further safeguards in this area[39]. Also, European Parliament warned that maximum caution is required in order to prevent unlawful discrimination and the targeting of certain individuals or groups by reference of race, color, ethnic or social origin, or any other characteristic[40]. In addition, CEPEJ adopted in 2018 already mentioned Charter on the Use of Artificial Intelligence in Judicial Systems.

b. Right to privacy

Police investigative techniques exploiting new technologies ensures more efficiency in investigation and prosecuting crime, but their high degree of intrusiveness affects upon right to privacy. Some of new technologies, such as interception of communication, silent video surveillance of the home interior, enables policy to bypass physical barriers.

To respond appropriately to new types of offences related to technology use

---

[34] Wilson, D., (2018) Algorithmic patrol: The futures of predictive policing, In. Završnik, A., (ed.) Big Data, Crime and Social Control, London, Routledge, 108-127.

[35] Egbert, S., (2018) About discursive storylines and techno-fixes: The political framing of the implementation of predictive policing in Germany, *European Journal for Security Research*, Vol. 3, Issue 2, 95-114.

[36] Stainer, I., (2016) Enhancing Intelligence-Led Policing: Law Enforcement's Big Data Revolution, In. Bunnik, A., Cawley, A., Mulqueen, M., Zwitter, A., (ed.) Big Data Challenges: Society, Security, Innovation and Ethics, London, Palgrave, 97-113.

[37] Joh, E.E., (2017) Feeding the machine: Policing, crime data and algorithms, *William and Mary Bill of Rights Journal,* Vo. 26, Issue 2, 287-302.

[38] Pedreschi, D., Miliou I., (2020) Artificial Intelligence (AI): New developments and innovations applied to e-commerce, European Parliament, PE 648.791.

[39] European Union Agency for Fundamental Rights (2018) #Big Data: Discrimination in data-supported decision making, FRA Focus.

[40] European Parliament (2017), Fundamental rights implications of big data, P8_TAPROV (2017)0076.

authorities across the Europe introduced specific rules on use of undercover agents in online communication, interception of electronic communication, remote searches of computer system, preservation of stored computer data etc.[41]. Use of those specific rules should be in line with safeguards introduced for implementation of special investigation techniques and rules governing their gathering should be applied. European Court of Human Rights in several cases identified that implementation of special investigation techniques violates article 8, right to privacy, of the European Convention of Human Rights. In the case *Klass v Germany* the European Court of Human Rights stated that whatever system of surveillance is adopted, there should be adequate and effective guarantees against abuse[42]. The assessment has a relative character and depends on all the circumstances of the case, including nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit etc.[43].

Establishment of the national and supranational databases with DNA profiles, fingerprints and vehicle registration data raised question how to ensure proper balance between individual rights, including right to privacy and public safety[44]. DNA sample collection, retention, access and use of DNA samples are linked to fundamental rights. DNA data base contain DNA profile and collected DNA samples (cellular material). The issue of storage is usually under discussion and critics. Even the European Court of Human Rights stated in the case *S and Marper v United Kingdom*[45] that there had been a violation of article 8, right to respect for private life of the European Convention of Human Rights. The Court considered in particular that the use of modern scientific techniques in the criminal- justice system could not be allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. Any State claiming a pioneer role in the development of new technologies bore special responsibility for "striking the right balance". The Court concluded that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in this particular case, failed to strike a fair balance between the competing public and private interests[46].

Use of new technology for surveillance purposes may violate right to privacy. The European Court of Human Rights in the case *Shimovolos v Russia* held there had been violation of article 8 of the Convention in the case concerned the registration of a human rights activist in the surveillance database, which collected information on activist's movements[47]. The creation and maintenance of the database and the

---

[41] Ortiz-Pradillo, J.C., (2017) The new regulation of technology-related investigative measures in Spain, *ERA Forum*, Springer, 425-435.

[42] Case *Klass v Germany*, Application No. 5029/71. See: Deployment of special investigative means, Council of Europe, 2013, 14-43.

[43] Case *Malone v UK*, Application No. 8691/79; case *Leander v Switzerland*, Application No 9248/81; *Huvig v France*, Application No. 11105/84.

[44] Vervaele, J.A.E., (2008) *Information sharing between intelligence and law enforcement authorities in combating international terrorism*, In. Becker, S. Derenčinović, D., (ed.) *International Terrorism: the Future Unchained?,* Zagreb, 49-82

[45] Application No. 30562/04 and 30566/04 *S and Marper v United Kingdom*.

[46] Matić Bošković, M., (2019) DNA profiles and database – relevance and ethical dilemmas in criminal justice, 345.

[47] Case *Shimovolos v Russia*, Application No. 30194/09.

procedures for its operations were governed by a ministerial order which had never been published and there we no indication of the minimum safeguards against abuse of the database. Similar position on the secret surveillance for national security purposes the Court had in the case *Szabo and Vissy v Hungary*[48] due to lack of safeguards to avoid abuse.

IV. Conclusions

The new technologies are transforming every segment of the criminal justice system, from prevention to enforcement of criminal sanctions. It is inevitable that the criminal justice system follows trends to be in line with technology used by offenders, however rules for its use should be clear, transparent and in line with rule of law standards.

The presented analysis confirmed that application of new technology has as a result more efficient and more effective law enforcement agencies as well as investigation and prosecution. However, the criminal justice system must ensure balance between the protection of fundamental rights and efficient criminal justice. The jurisprudence of the European Court of Human Rights confirmed that same standards of human rights protection have to be followed when country introduce new technologies in the legislation and when law enforcement authorities apply new technologies.

Prior to introduction of the new technologies in the criminal justice system the policy makers in cooperation with researchers should conduct thorough assessment and analyze implications on human rights protection. Standards and principles for inclusion of the new technology should be set to guide its use, especially if there is discussion on introduction of predictive models and artificial intelligence.

Once when new technologies are introduced the comprehensive evaluation system should be established to monitor their potential for violation of human rights and to take necessary measures for improvement. The ex-post analysis of predictive model showed that algorithms incorporated all bias that exists and there is a need to introduce mechanism for prevention of such challenges.

References

1. Adderley R., Bond J. (2008) Police Forensic science performance indicators – a new approach to data validation. In: Ellis R., Allen T., Petridis M. (ed.) Applications and Innovations in Intelligent Systems XV, SGAI 2007, Springer, London, 163-174.

2. Ashby, M. P. J., (2017) The value of CCTV surveillance cameras as an invstigative tool: An empirical analysis, *European Journal on Criminal Policy and Research,* Vol. 23, Issue 3, 441-459.

3. Brennan, T., Dieterich, W., Ehret, B., (2009) Evaluating the predictive validity of the COMPAS Risk and Needs Assessment System, *Criminal Justice and Behavior,* Vol. 36, Issue 1, 21-40.

4. Clarke, R.V. (1995) Situation crime prevention, *Crime and Justice*, Vol. 19, 90-160.

[48] Case *Szabo and Vissy v Hungary,* Application No. 37138/14.

5. Coccoli, J., (2017) The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era, *Peace Human Rights Governance*, Vol. 1, Issue 2, 223-250.

6. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

7. Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

8. Eck, J.E., Chainey, S., Cameron, J.G., Leitner, M., Wilson, R.E., (2005) Mapping Crime: Understanding Hot Spots, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/209393.pdf 28.12.2020.

9. Egbert, S., (2018) About discursive storylines and techno-fixes: The political framing of the implementation of predictive policing in Germany, *European Journal for Security Research*, Vol. 3, Issue 2, 95-114.

10. Elmes, G.A., Roedl, G., Conley, J., (2014) Forensic GIS: The Role of Geospatial Technologies for Investigating Crime and Providing Evidence, Springer.

11. European Commission Survey on Scams and Fraud Experienced by Consumers – Final Report, January 2020.

12. European Informatics Data Exchange Framework for Courts and Evidence – Overview of existing legal framework in the EU Member States, 2015, available at: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf 26.12.2020.

13. European Parliament (2017), Fundamental rights implications of big data, P8_TAPROV(2017)0076.

14. European Union Agency for Fundamental Rights (2018) #Big Data: Discrimination in data-supported decision making, FRA Focus.

15. Europol, Crime in the age of technology, (2017).

16. Eurostat, Digital economy and society statistics – households and individuals (2020), available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_accessed 25.12.2020.

17. Eurostat, Proportion of households having access to a personal computer 2014-2019 (2020), available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Proportion_of_households_having_access_to_a_personal_computer,_2014_and_2019_(%25)_CPC20.png 25.12.2020.

18. Joh, E.E., (2017) Feeding the machine: Policing, crime data and algorithms, *William and Mary Bill of Rights Journal,* Vol. 26, Issue 2, 287-302.

19. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 2.

20. Kostic, J., Matic Boskovic, M., (2020) How COVID-19 Pandemic influences Rule of Law backsliding in Europe? In. M. Reljanović (ed.) Regional Law Review, Institute of Comparative Law, Belgrade, 77-91.

21. Matić Bošković, M., (2019) DNA profiles and database – relevance and ethical dilemmas in criminal justice, In: Stevanović, I., Vujičić, N. (ed.), *Kazneno pravo i medicina*, Institute for Criminological and Sociological Research, Belgrade, 337-351.

22. Matić Bošković, M., (2019) DNA profiles and database – relevance and ethical dilemmas in criminal justice.

23. McClendon, L., Meghanathan, N., (2015) Using Machine Learning Algorithms to Analyze Crime Data, *Machine Learning and Applications: An International Journal*, Vol. 2, No. 1, 1-12.

24. Miller, AP. (2018) Want less-biased decisions? Use algorithms. *Harvard Business Review*, July 26. https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms 28.12.2020.

25. Moses, K. R., (2011) Automated Fingerprint Identification System, In: Fingerprint Sourcebook, National Institute of Justice, Washington DC.

26. Nellis, M., (2014) Understanding the electronic monitoring of offenders in Europe: expansion, regulation and prospects, *Crime, Law and Social Change*, Vol. 62, Issue 4, 489–510.

27. O'Neil, C., (2016) Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, New York, Crown Publishers.

28. Ortiz-Pradillo, J.C., (2017) The new regulation of technology-related investigative measures in Spain, *ERA Forum*, Springer, 425-435.

29. Pedreschi, D., Miliou I., (2020) Artificial Intelligence (AI): New developments and innovations applied to e-commerce, European Parliament, PE 648.791.

30. Piza, E., Welsh, B., Farrington, D. and Thomas, A. (2019) CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis, *Criminology and Public Policy,* Vol 18, Issue 1, 135-159.

31. Piza, E., Welsh, B., Farrington, D. and Thomas, A., 139.

32. Ratcliffe, J., (2006) Video surveillance of public places, Problem-Oriented Guides for Police – Response Guide Series, Guide No. 4, U.S. Department of Justice Office of Community Oriented Policing Services, Center for Problem-Oriented Policing.

33. Roman, J. K., Liberman, A. M., Taxy, Sm., Downey, P. M. (2012) The Costs and Benefits of Electronic Monitoring for Washington D.C, Urban Institute, Washington D.C.

34. Smith, G. R, (2007) Crime Control in the Digital Age: An exploration of Human Rights Implications, *International Journal of Cyber Criminology*, Vol. 1, Issue 2, 167-179.

35. Stainer, I., (2016) Enhancing Intelligence-Led Policing: Law Enforcement's Big Data Revolution, In. Bunnik, A., Cawley, A., Mulqueen, M., Zwitter, A., (ed.) Big Data Challenges: Society, Security, Innovation and Ethics, London, Palgrave, 97-113.

36. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013.

37. United Nations, Human Right Council, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A/HRC/21/L.6 (21 September 2012), available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session21/A.HRC.21.L.6_en.doc 25.12.2020.

38. Vervaele, J.A.E., (2008) *Information sharing between intelligence and law enforcement authorities in combating international terrorism*, In. Becker, S. Derenčinović, D., (ed.) *International Terrorism: the Future Unchained?,* Zagreb, 49-82.

39. Wilson, D., (2018) Algorithmic patrol: The futures of predictive policing, In. Završnik, A., (ed.) Big Data, Crime and Social Control, London, Routledge, 108-127.

40. Winge, S., Knutsson, J., (2003) An evaluation of the CCTV scheme at Oslo central railway station. *Crime Prevention and Community Safety,* Vol. 5: 49- 59.

41. Završnik, A., (2020) Criminal justice, artificial intelligence systems, and human rights, *ERA Forum* 20, Springer, 567-583.