ՀԱՅԱՍՏԱՆԻ ԱՄԵՐԻԿՅԱՆ ՀԱՄԱԼՍԱՐԱՆ

LL.M. Program

ԻՐԱՎԱԳԻՏՈՒԹՅԱՆ ՄԱԳԻՍՏՐՈՍԻ ԾՐԱԳԻՐ

TITLE

New player in the field of law: the impact of artificial intelligence on human rights and regulation thereof

STUDENT: ZOYA TOVMASYAN

SUPERVISOR: PROF. ADELAIDA BAGHDASARYAN

NUMBER OF WORDS

11.684

Table of Contents

LIST OF ABBREVIATIONS

AI	**Artificial intelligence**

ML	**Machine Learning**
DL	**Deep Learning**
RL	**Reinforcement Learning**
UDHR	**Universal Declaration of Human Rights**
ICCPR	**International Covenant on Civil and Political Rights**
ECHR	**European Convention on Human Rights**
ECtHR	**European Court of Human Rights**
GDPR	**General Data Protection Regulation**
CEC	**Central Electoral Commission**
IHRL	**International Human Rights Law**

Introduction

"Through all human history, civilizations have created ways to explain the world around them — in the Middle Ages, religion; in the Enlightenment, reason; in the 19th century, history;

in the 20th century, ideology…The most difficult yet important question about the world into which we are headed is this: What will become of human consciousness if its own explanatory power is surpassed by Artificial Intelligence, and societies are no longer able to interpret the world they inhabit in terms that are meaningful to them?"

Henry Kissinger

The research and development of AI are over half a century old. The term originated in 1956, though the concept goes back to the late 1700s. Artificial intelligence is a notably capacious term. One definition of AI is included in the European Commission communication on Artificial Intelligence for Europe: "Artificial intelligence (AI) refers to systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals".[1] Artificial general intelligence is the system that displays intelligence across multiple domains, with the ability to learn new skills, and which simulate or even exceeds in speed human intelligence.

Nowadays, the influence of AI extends in various areas, from healthcare to judiciary. Progress in modern technologies is of immense importance as they reshape all spheres of life, and consequently, the field of human rights could not remain intact. Many AI applications are so well-integrated in everyday life that people do not apprehend the scales of its impact. The employment of these technologies generally relies on the generation, accumulation, processing, and sharing of large amounts of data about personal behavior. While some of these uses, like spam filters or proposed items for online shopping, may seem innocuous, others can have more grave effects and may even pose unprecedented perils to the right to privacy and the right to freedom of expression. It incites consideration of whether current perceptions of human rights and mechanisms of their enforcement are adequate in the new socio-technical landscape. The ability of digital technologies to exercise functions create new menaces and prospects of wrong-doing.

The capability of AI to distinguish and profile people more efficiently than any other agent leads to discrimination in a variety of ways. Beyond creating commercial possibilities for some industries, it forms the foundation to discriminate distinct groups and persons, such as women, people of color, and ethnic minorities. The relevant example is Tay chatbot, released by Microsoft, on Twitter aimed to have human-like conversations (that includes humor and randomness) with Twitter users. Long with advanced algorithms, Tay intended to have the personality of an American woman aged between 18 and 24 and strived to set a relationship

[1] Gina, N. P., Talking to Bots: Symbiotic Agency and the Case of Tay. International Journal of Communication 10, 4919(2016). *available at* https://ijoc.org/index.php/ijoc/article/view/6277

with millennials with knowledge of slang and popular culture. Aimed at being an entertainment, Tay experiment turned into a fiasco in less than a day. Tay's communications with Twitter users produced a large number of tweets carried sexism, racism, antisemitism, and many forms of hate speech. The following tweets of Tay illustrate this point clearly, "feminism is cancer," "gamergate is good, and women are inferior," "Hitler was right. I hate the Jews." Due to design defects and correlated attacks, "Tay's learning algorithms replicated the worst racism and sexism of Twitter very quickly".[2] Microsoft shut down Tay and publicly apologized sixteen hours after its release.

The thesis at hand is structured in a manner to conduct in-depth research on the positive and negative impact of AI on fundamental human rights. The first chapter represents the nature and functioning of AI so as to understand how its technical capabilities may interact with human rights. Then, the focus is on the right to freedom of expression, the prohibition of discrimination, and the right to private and family life. The second chapter of research represents how AI may affect the specific elements of the right to a fair trial when used in the court proceedings. In particular, the analysis is on how intelligence application affects reasonable time requirement, independence and impartiality of the judge, equality of arms, and so on. The last chapter examines the link between automated technologies and the right to free elections. Further, the model e-voting and regulation in Armenia is discussed. Thus, the primary goal is to reveal how new voting technologies correlate with the obligation of a State to ensure universal, equal suffrage, and secure voting proceeding.

The purpose of the research is to reveal possible risks and opportunities oh human rights that arise from the application and development of AI. The approach chosen for the analysis is to identify how relevant international instruments and national law, designed ethical are corresponding to the challenges imposed by AI. The mapping of gaps in legal frameworks and risks arising from the deployment of AI will pave the way to come out with recommendations and possible solutions to the problems.

Chapter 1

The Nature of Artificial Intelligence and its influence on fundamental rights

"Technologies are morally neutral until we apply them."

[2] Gina, N. P., Talking to Bots: Symbiotic Agency and the Case of Tay. International Journal of Communication 10, 4921(2016). *available at* https://ijoc.org/index.php/ijoc/article/view/6277

§ 1.1. The nature of AI

The impact of AI on human rights is one of the most crucial factors nowadays since AI-driven technology expands its influence in various areas such as an individual's life, social media applications, public sector, etc. AI is frequently being utilized to assess people's personalities or skills, make decisions that can have severe and real consequences for human rights. As the Commissioner for Human Rights in a Human Rights Comment stressed that finding the right balance between technological development and human rights protection is an urgent matter.[3] Thus, the assessment of the potential influence of the AI system on human rights must be conducted while taking into account the nature, context, scope, and purpose of the system.

While referring to AI, up to date, there is no universal or agreed of what embody AI. Traditionally, AI refers to machines or agents that are capable of observing their environment, learning, and based on the knowledge and experience gained, taking intelligent action and proposing decisions.[4] In general, an average person assumes AI to be a humanoid robot, which is usually represented in films or science fiction books. Meanwhile, robotics is the sole subfield of AI, which is in use of many ML techniques and neural networks as well.

AI is the study of cognitive processes using the conceptual frameworks and tools of computer science.[5] All manner of intelligent behavior is in the realm of Al, including playing chess, solving calculus problems, making mathematical discoveries, understanding short stories, learning new concepts, interpreting visual scenes, diagnosing diseases, and reasoning by analogy. [6]

In the history of AI, there were many approaches: logic-based in the 1950s, knowledge-based experts in the 1070s and 1980s, and data-driven in the 2000s and onward. The current phase is marked for increased computing processing capabilities and data. Their combination promotes the progress of Machine Learning (ML). ML systems are trained, but not explicitly programmed. ML is supposed to read neural networks by processing large volumes of data and answers expected from the data as well. The development of ML resulted

---

[3] Safeguarding human rights in the era of artificial intelligence (13July, 2018) *available at* https://www.coe.int/en/web/commissioner/-/safeguarding-human-rights-in-the-era-of-artificial-intelligence

[4] Artificial Intelligence, European Perspective 8, 140 (2018)

[5] Edwina L. Rissland, Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning, 99 Yale L.J.(1990) *available at* https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=7293&context=ylj

[6] Ibid at. 1958

from the necessity of specialized graphic processors, the increase of data amount, and new advances in ML algorithms.

ML is also closely linked to concepts such as data mining and exploratory data analysis. Data discovery is the extraction of specific patterns of large databases using machine learning, statistics, and database systems. Data analysis is the tool by which machine learning achieves the goal, as mentioned above.

Amongst others, Deep learning (DL) is the subset of machine learning. It copes with unclassified and mixed data by increasing significantly the number of neural layers and neurons, and the amount of data used for the training. DL clear image and object recognition makes prominent inroads into areas as speech and natural language processing. The application of DL to multiple AI components has revolutionized the human-computer interaction and resulted in the creation of virtual assistants available on devices, such as Apple's Siri or Amazon's Alexa. Through the use of AI, Google has developed real-time translation of texts and voice, while Bing assistants interact with people in such a natural way, as people do with each other.

Reinforcement learning (RL) is another set of algorithms that make software agents take actions to maximize some notion of cumulative reward. The combination of RL and DL resulted in the creation of complex games, such as Go and Dota, in which computers outachieved leading human experts in the field.

Advances in technologies raise the potential for socially intelligent robotic to co-exist with humans, as in the case of co-workers, personal companions, or self-driving vehicles. The development of robotics raises the perspective of integration of AI in our everyday life, as the agents are capable of understanding human and social behavior. The incorporated form of AI can act upon and form human behavior and affect human to human social interaction. The interaction of humans and robots involves human emotions, which may result in empathetic action toward AI and affect human development over time. Thus, the methodological development of AI over the last half-century resulted from advances in computing power and the availability of data. Now, the applications of AI became the inalienable part of our everyday life, from filtering spam to music generation. They are increasingly used in government, industry, and commerce.

While the use of AI in these spheres has benefits, the ethical and legal involvement of the data usually falls outside of public attention. Without any doubt, the advantages from AI, ML, and DL are noteworthy in many spheres of life, but relying too much on AI may turn against users, restrict their rights or perpetuate injustice. In particular, decisions taken while

using AI systems lack transparency, accountability, and safeguards. To this end, the need to understand how the use of advanced technologies may affect the fundamental rights enclosed in the ECHR convention. Within this framework, the present Chapter will mainly focus on identifying the positive and adverse influence of AI on the rights that are mostly undermined according to the "Wagner Study" conducted by the Council of Europe. According to the study the most explicitly affected rights are:

- Right to a fair trial (Article 6);
- Right to respect for private and family life (Article 8);
- Freedom of expression (Article 10);
- Prohibition of discrimination (Article 14);
- Right to free elections (Article 3 Protocol 1).

In the present Chapter, the main focus will be on the right to private and family life, the right to freedom of expression, and the prohibition of discrimination. The aim is to reveal how AI systems and mentioned rights are interacting, how the existing laws and regulations are corresponding to the issues which arise while using data-driven tools, which are the main concerns and how they need to be addressed.

§ 1.2. AI and right to freedom of expression

The impact of AI on freedom of expression varies from how global digital platforms exert over our informational environment at both an individual and societal level. The application of AI in the online media environment can have both positive and negative influences on individuals' right to freedom of expression. First of AI affects people's rights to express themselves and to access information. Internet services and social media deploy numerous complicated and adaptive information-processing technologies for operations. These technologies and services provide an invaluable opportunity to people in expressing themselves and accessing information. Second, AI creates the conditions for a strong and active democratic exchange on online platforms. Third, filtering systems, such as content moderation, raise another concern on freedom of expression. Their application can raise issues of bias and surveillance that current legal frameworks have not adequately addressed.

The rise of techniques such as video surveillance, facial recognition, behavior analysis etc., by public authorities and private companies hinder freedom of expression.[7] There is no international standard that frames the use of AI and the right to freedom of expression. Meanwhile, the international standards apply to the use of AI by online intermediaries, such as social media platforms and search engines, for instance, "states should not impose a general obligation on intermediaries to monitor the information that they transmit, store, automate or otherwise use"[8] and "users should have the opportunity to challenge the blocking and filtering of content"[9]. For example, following the live video streaming via social media platforms of the attack on civilians by a lone terrorist in Christchurch in early 2019, the capacity of AI techniques used on online platforms to detect and delete illegal content was developed.

The right to freedom of expression is guaranteed under Article 19 of the Universal Declaration of Human Rights (UDHR) , the International Covenant on Civil and Political Rights (ICCPR), and European Convention for the Protection of Human Rights and Fundamental Freedoms. Article 10 of ECHR states that "everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".[10] Meanwhile, Article 19 of ICCPR prescribes that "Everyone shall have the right to hold opinions without interference. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.".[11] It is a positive obligation of a State to promote and protect the exercise of freedom of expression and negative obligation to refrain from its interference. The development of AI systems raises issues related to pluralism and diversity, as from one viewpoint, they create a platform for speakers to address a broad audience. Still, from the other side, the major online providers dominate the model of news and media worldwide. Furthermore, the content moderation through algorithms poses a particular set of

[7] The Global Principles on Protection of Freedom of Expression and Privacy, (2017) *available at* https://cedem.org.ua/en/library/the-global-principles-on-protection-of-freedom-of-expression-and-privacy/

[8] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (June 8, 2000) *available at* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

[9] Recommendation CM/Rec 6 of the Committee of Ministers to Member states on measures to promote and respect for freedom of expression and information with regard to internet filters (2008) *available at* https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2008-6-of-the-committee-of-ministers-to-member-states-on-measures-to-promote-the-respect-for-freedom-of-expression-and-informati?inheritRedirect=false

[10] Council of Europe, European Convention on Human Rights (3 September, 1953) *available at* https://www.echr.coe.int/Documents/Convention_ENG.pdf

[11] International Covenant on Civil and Political Rights (16 December, 1966) *available at* https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

content restrictions at potentially enormous scale on massive platforms. So, diversity and pluralism may be achieved in case if policymakers design safeguards or rules for greater user control.

The pivotal role in the regulation of platforms is to address human rights while content moderation. GDPR set up rules for data processing in the online environment, provides the basis for the protection of rights between users and platforms. Antitrust law must prevent unnecessary concentrations of power over media and communications. It's imperative to admit the importance of a comprehensive set of regulatory frameworks that implement necessary provisions for the adequate exercise of freedom of expression online.

Current industry initiatives around AI aim at the development of laws and standards that regulate content management and conduct oversight in compliance with these frameworks. The key concepts are fairness, accountability, and transparency. The aim of accountability framework is to ensure the risk assessment on human rights. Risk assessment may be deployed in particular cases such as terrorism content and disinformation. Formal risk assessment procedures provide an opportunity for in-depth consideration of the potential impact on fundamental rights that a product or policy poses as well as the various measures that are and may be taken to address them, i.e. Google conducted and published a human rights impact assessment for its Celebrity Recognition API.[12]

The use of AI in content moderation may rise issues related to lack of due process for user's activity and content. The central issue in this case is the development of dispute resolution and enforceability measures which will be in conformity with the rule of law. Many AI systems engaging with the freedom of expression are owned by companies that do not disclose trade secrets rules, which arise difficulties for civil society actors related to transparency around application and development, the complexity of these systems. Hence, the unrevealed nature of these systems raises barriers while studying the impact of AI on the right to freedom expression unless substantial harm occurs. So, the human oversight over these systems is paramount in all stages of development and employment of systems. Thus, the probability of human oversight in case of complaints regarding the use and impacts of algorithms for content regulation can provide a vital protection net for the rights and freedoms of affected users.

So, in this realms, the suggested way to safeguard the right of freedom of expression can be a "regulation by design" approach. This approach is fundamental in order to provide

[12] Google Celebrity Recognition API Human Rights Assessment | Executive Summary October 2019 *available at* https://services.google.com/fh/files/blogs/bsr-google-cr-api-hria-executive-summary.pdf

information accountability and privacy-friendly approach while using AI in content moderation. Through regulation by design approach the more robust field of freedom of expression can be achieved via the incorporation of freedom of expression standards in the design and employment of devices. Thus, along with accountability, fairness, and transparency, it can extend to the creation of relevant datasets and labeling practices along with ways by which AI is deployed.

§ 1.3. AI and right to respect for private and family life

The nexus of AI and the right to private and family life results from the capability of AI to recognize and process " the intimate from the available." The use of AI can affect the right to privacy in different ways, ranging from collecting a massive amount of data without the consent of users in proximity, identifying people who wish to remain anonymous or generating sensitive information about people from non-sensitive data, to making decisions which profoundly impact peoples' lives. Individuals are usually not able to identify how much data smart and interconnected devices generate, process, and share.

The ongoing debates around AI and privacy are complicated as policy, and regulatory discussions use AI in connection to a wide range of applications. In this regard, it seems that new technologies create such radical challenges that existing laws and regulations are not capable of handling. The fundamental right to privacy is established under Article 12 of UDHR, which proclaims that " No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation…Everyone has the right to the protection of the law against such interference or attacks".[13] IHRL requires that any interference with right to privacy must be in accordance with law, necessary in a democratic society and proportionate. AI-driven applications are capable to assess, sort or rank people without their consent. In this regard, he United Nations Human Rights Council noted with concern in March 2017 that "automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights".[14]

---

[13] Universal Declaration of Human Rights (10 December, 1948) *available at* https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_217(III).pdf

[14] U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L,7, para 2., (23 March, 2017)

Data protection has a crucial impact on the safeguard of the right to privacy. Data protection applies to an identified person, not to the privacy of groups or to other infringements that don't include personal data. GDPR regulations require a legal basis for processing data - and in addition to the principles of fairness, accountability and transparency, includes the core principles of purpose limitation and data minimization.[15] The GDPR also limits the use of automated decision-making in certain circumstances, and requires individuals to be provided with information as to the existence of automated decision-making, the logic involved and the significance and envisaged consequences of the processing for the individual.[16] The law introduces an overall prohibition (with narrow exceptions) to decisions "based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"[17]. Notably, the GDPR also defines profiling as the automated processing of data to analyze or to make predictions about individuals.[18] This definition recognizes that personal data can be produced by machine learning applications and other forms of profiling.[19] The GDPR introduces a range of provisions which encourage the design of less privacy-invasive systems, some of which have far reaching consequences for AI. The obligation to incorporate data protection by design and by default seeks to integrate data protection principles into the design of data processing operations. [20]

In current realms, AI is deployed to formulate diagnostics, support healthcare personnel, up to predict the possible evolution of the COVID-19 pandemic. States use AI to collect big data aiming to control epidemic risks through biometric devices, geolocation devices, and applications. It is noteworthy that Convention 108 prescribes that even in particularly difficult situations, data protection principle of lawfulness is respected and therefore it is ensured that data subjects are made aware of the processing of personal data related.[21] The principles set up by the Convention 108 prescribe that AI development relying on the processing of personal data should be carried out only if necessary and proportionate to the explicit, specified and legitimate purpose pursued. The key purpose of the proportionality here is to ensure that the individuals are subordinated from AI systems and legislative authorities employ AI considering the safeguard of public interest and individual rights.

[15] General Data Protection Regulation (GDPR) (5 May, 2016) available at https://gdpr-info.eu/
[16] GDPR, Articles 13, 14 and 22.
[17] GDPR, Article 22
[18] GDPR, Article 25
[19] GDPR, Article 4(4)
[20] L. Edwards, & M. Veale, "Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions'?", IEEE Security & Privacy, (2017).
[21] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January, 1981) *available at https://rm.coe.int/1680078b37*

Moreover, under the conventional provisions State are obliged to ensure that AI developers act in a socially responsible manner and are in a position to demonstrate that data processing is in compliance with the applicable law. The other key principle of Convention is to ensure transparency, so the public will be properly informed on purpose of data collection. Thus, data subject will be able to assess the consequences of AI application and get effective remedy in case of violations. Furthermore, "Convention 108+" acknowledges the necessity of exceptions and restrictions for the sake of pressing objectives of public and individuals' vital interests. Nevertheless, restrictions to its principles and rights must respond to very clear requirements, even during the state of emergency, to ensure the persisting respect of the rule of law and fundamental rights.[22] According to Article 11 of Convention exceptions shall be "provided for by law, respect the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society".[23] It is essential that measures are taken to ensure that data processed during the state of emergency will be adequately protected when the state of emergency is lifted. As the practice shows, i.e. in Israel and Italy, *smartphone* applications were developed that can be used to track the route of a person infected and inform people who contacted him or her. The development of these monitoring solutions should be based on a prior evaluation of the probable impact of the planned data processing on the rights and fundamental freedoms of data subjects. Furthermore, the data processing should be conducted in such a manner as to prevent or lessen the risk of adverse consequences of AI application.

In Armenia, the amendments to the Law on the State of Emergency and Law on Electronic Communications were passed to conduct muss surveillance of mobile devices of citizens to seize the spread of pandemic. In particular, procedures of data processing and civil surveillance by private company are defined. Furthermore, the law prescribes the process of destruction of data, ensuring the transparency and reliability of process. In particular, within 3 days the report on destruction pf data has to be submitted to the government. Also, a representative from each fraction of National Assembly has the opportunity to be present at deleting of data.

The surveillance on Armenian laws and provisions of Convention 108 show that the key points while using AI during data processing and mass surveillance are the respect for the principle of accountability, the adoption of risk assessment procedures and the application of other suitable measures to deprive the population from the risk of trivialization of mass

[22] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January, 1981) *available at* https://rm.coe.int/1680078b37
[23] Ibid

surveillance. So, the conclusion is that when AI is used in conformity with the established international standards, it favors society and helps to promptly respond to the global challenges.

§ 1.4. AI and prohibition of discrimination

The ability of AI to identify and profile people more efficiently than any other tool leads to discrimination in a variety of ways. Beyond creating economic opportunities for some industries, it forms the basis to discriminate particular groups and persons, such as women, people of color, and ethnic minorities. Article 14 of the European Convention on Human Rights states: "The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."[24] Protocol 12 to that Convention lays down a similar prohibition, with, regarding certain aspects, a broader scope. "The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."[25]

The real example of discrimination based on ethnicity occurred when the Chinese government used AI, in particular facial recognition, to identify and target members of the Uighur Muslim minority in Xinjiang. A system called Integrated Joint Operations Platform collected data on profile Uighurs via an application that forcefully installed to smartphones, wi-fi sniffers, online, and offline surveillance to predict potential terrorists. Chinese developers go on using ML to develop systems that will recognize "sensitive groups" and classify Uighurs and non-Uighurs. Firstly, developers supply the AI system with a notable amount of marked photos of Uighurs and non-Uighurs. Then, by using machine learning, artificial intelligence tries to find patterns and traits to identify Uighurs.[26] Thus the state-sponsored surveillance was conducted with a lack of respect for fundamental rights and the rule of law.

---

[24] ECHR, Article 14

[25] Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 177) (4 November, 2000) *available at* https://www.echr.coe.int/Documents/Library_Collection_P12_ETS177E_ENG.pdf

[26] Paul, M. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. Retrieved from New York Times(April 14, 2019), *available at* https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligenceracial-profiling.html

Persecution based on religious or political opinion is a severe human rights issue in many states. Another real-life example occurred when many churches worldwide bought a facial recognition system to identify churchgoers from Moshe Greenshpan. Churches use the system to distinguish the regular churchgoers to request contributions and track absent churchgoers to restrain them. This raises the question of legitimate aim while exploiting the application. Due to facial identification, religious organizations can follow irregular attendants and persons who stepped from them.

Direct and indirect discrimination are prohibited by the ECHR. The European Court of Human Rights describes direct discrimination as follows: "there must be a difference in the treatment of persons in analogous, or relevantly similar, situations", which is based "on an identifiable characteristic".[27] Indirect discrimination is interpreted further by the European Court of Human Rights as follows: " A difference in treatment may take the form of disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, discriminates against a group. Such a situation may amount to "indirect discrimination", which does not necessarily require a discriminatory intent." [28] Decision taken by AI system can unintentionally lead to indirect discrimination. Regarding indirect discrimination, the law focuses on the effects of a practice, rather than on the intention of the alleged discriminator.[29] Hence, the intention of discriminator is not key issue. However, the prohibition of indirect discrimination does not provide clear rules regarding AI decision-making. Hence, the intention of the discriminator is not a vital issue. However, the prohibition of indirect discrimination does not provide precise rules regarding AI decision-making. The notion of indirect discrimination occurs in somewhat open-ended standards, which are often challenging to implement in practice. It needs to be proven that a seemingly neutral rule, practice or decision disproportionately affects a protected group and is thereby prima facie discriminatory. In many cases, statistical evidence is used to show such a disproportionate effect.[30] Along similar lines, EU law says that a practice will not constitute indirect discrimination if it "is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary".[31] Whether an alleged discriminator can invoke such an objective justification depends on all the circumstances of a case and requires a

[27] ECtHR, Biao v. Denmark (Grand Chamber), No. 38590/10, para. 89 ,(24 May 2016).
[28] Ibid, para. 103.
[29] Ibid, para. 103.
[30] ECtHR, D.H. and Others v. Czech Republic (Grand Chamber), No. 57325/00, paras. 187-188. (13 November 2007).
[31] Council Directive 2000/43/EC of 29 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin Article 2(2)(b) (June 2000) *available at* https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0043

nuanced proportionality test.[32] Hence, it is not usually clear whether a specific practice breaches the prohibition of indirect discrimination. The prima facie type of discrimination can remain hidden, and the requirement of being shown may raise difficulties. For example, an organization could intentionally use proxies to discriminate on the basis of racial origin.

Another weakness relates to the non-discrimination law's concept of protected characteristics. The recent TikTok case, when the video of disabled people and people with facial disfigurements were removed from For you feed by moderators. Thus, people were the company was discriminating vulnerable users in a deceived effort to prevent them from being the center of attention that could turn sour.

In conclusion, non-discrimination statutes typically focus on (direct and indirect) discrimination based on protected characteristics, such as race, gender, or sexual orientation.[33] Supplementary regulation is needed to protect people against newly invented classes of unfair differentiation and illegal discrimination. The most relevant legal instruments to mitigate the risks of AI-driven discrimination are non-discrimination laws and data protection laws. There is a need for sector-specific rules to minimize the risk of unfair discrimination. Furthermore, new laws or procedures should be envisaged by the international community to mitigate and prevent discrimination risks of the use of AI systems for groups that have an increased risk of their rights being disproportionately impacted by it. Moreover, unbiased parties, i.e., international organizations, have to provide oversight and hold accountable States and organizations which use AI systems in the context of law enforcement, mainly to avoid profiling of individuals belonging to specific groups.

[32] *Hugh Collins and Tarunabh Khaitan*, Indirect Discrimination Law: Controversies and Critical Questions, pp. 1161-1170 (2018)
[33] A Theory of Discrimination Law (2015).

Chapter 2. Concept of fair trial under Article 6 of the ECHR and AI

The right to a fair trial is one of the inherent safeguards for the respect of democracy and the rule of law. The ECHR is considered to be "a living instrument", hence, this concept shall have to refer to innovations that may affect justice sector, including the possibility of automation of proceedings with AI tools.

The right to a fair trial is guaranteed to everyone under Article 6 of ECHR, which states that "In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."[34] The cited paragraph applies to civil, administrative and criminal processes. Paragraphs 2 and 3 are focusing on criminal process, accordingly hereinafter the main focus will be on paragraph 1 of the Article. The requirement of fairness applies to the proceedings in their entirety and it is not confined to the hearing between parties.[35]

It has been stated in the European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment that "When AI tools are used to resolve a dispute or as a tool to assist in judicial decision-making or to give guidance to the public, it is essential to ensure that they do not undermine the guarantees of the right of access to the judge and the right to a fair trial (equality of arms and respect for the adversarial process)".[36]

The elements of a fair trial reasonable are: time requirement, independent and impartial tribunal, equality of arms, immediacy, and right to get reasoned judgment will be assessed in connection with the use of AI in the court proceedings.

The duty to provide a final judgment within a reasonable time derives from the wording of the article and the principle of effectiveness. The reasonableness of the lengths of

---

[34] ECHR, Article 6

[35] ECtHR, *Stran Greek Refineries and Stratis Andreadia v Greece*, no. 13427/87, 9.12.1994, § 49.

[36] European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, European Commission for the efficiency of justice, p. 5. (3-4 December, 2018)
available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

proceedings in each case must be assessed in the light of the following criteria: the complexity of the case, the conduct of the applicant and the relevant authorities and what was at stake for the applicant in the case.[37] In the light of reasonable time requirement, the application of AI can significantly speed up the proceedings. AI can be used to predict decisions or to assist judges in the decision-making. In a scenario when AI is used to suggest a decision to a case brought to the court, the judge can either decide to cooperate with the AI's submission by citing or ignoring it. The use of AI will help to raise the consistency of court decisions and predictability of the law's application. Once there are expert machines, it will be easier to argue in some cases that the machines should be used to their full potential (instead of human judges), because the evidence will suggest that in those circumstances they will deliver better results than human experts.[38] In this case, it may turn out that decisions delivered by machines are so fair that judges are simply middlemen for machine-delivered decisions. Hence, it is essential that the processing made by AI, whether designed with the aim of providing legal advice, helping in drafting or in the decision-making process, is carried out in compliance with transparency, impartiality and equality, certified by an external and independent expert assessment.[39] The ability of AI to deal with a large amount of data and collect information in a short time may contribute to judicial efficacy. Furthermore, AI can be used in the automatic anonymization of decisions, which would speed up the whole process, and help to keep the public informed about the decisions.

The requirements of independence and impartiality are interconnected, as the court is formed by judges who are supposed to be independent and impartial. The ECtHR has outlined the following criteria to determine whether a judiciary is independent: "the manner of appointment of its members and the duration of their term of office; the existence of guarantees against outside pressure, and whether the body presents an appearance of independence"[40].To determine whether a court is impartial, the subjective and objective test has to be applied. According to the case law "The existence of impartiality for the purposes of Article 6 of the Convention must be determined according to a subjective test, that is based on the personal conviction of a particular judge in a given case, and also according to an objective test, that is ascertaining whether the judge offered guarantees sufficient to exclude any legitimate doubt in

[37] Council of Europe, European Court of Human Rights Guide on Article 6, Right to a fair trial, civil limb, p. 75 (31 December,2018)
[38] T.J. Buocz, Artificial Intelligence in Court – Legitimacy Problems of AI Assistance in the Judiciary, p. 41-59, p. 55. (2018)
[39] European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, European Commission for the efficiency of justice, p. 5. (3-4 December, 2018)
available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c
[40] ECtHR, *Findlay v. the United Kingdom*, Application no. 22107/93, § 73.

this respect".[41] The use of AI in judiciary may cause indirect effects on independence and impartiality. AI tools should be used with due respect for the principle of the rule of law, and judges' independence in their decision-making process.[42] While using AI, the implicit bias can be absorbed automatically in the utilization of ML from pure cultures. Then, accidental bias may occur as a result of ignorance by insufficiently careful development teams. Also, preference may be introduced intentionally. To suggest a decision, AI uses data and algorithms which were incorporated into it by a human, so AI is as biased as a human being. The fact that AI can be discriminatory as humans was proven on an example of the system used in the US. The COMPAS software aims to evaluate the risk of individuals committing the crime again when the judge is determining the sentence for an individual. The software exploits 137 questions through which it assesses risk and also "criminal personality," "social isolation," "substance abuse," and "residence/stability." The software-based on answers rates people on a scale from 1-10 (low-high risk), and the rate is used by the judge while deciding the sentence. The African-American populations were assigned a high-risk recidivism rate twice that of the other communities, and thus were receiving longer sentences only based on their race. So, it is evident that the algorithm used biased data on the past behavior of a particular group and affected the appearance of the independence of the court.

According to European Ethical Charter "AI should offer complete impartiality, free from human fallibilities and prejudices…The use of machine learning to combat discrimination should be encouraged". [43] It has been suggested in the Charter that: "Data based on judicial decisions that is entered into a software which implements a machine learning algorithm should come from certified sources and should not be modified until they have actually been used by the learning mechanism. The whole process must therefore be traceable to ensure that no modification has occurred to alter the content or meaning of the decision being processed.. The neutrality of algorithms is a myth, since their creators consciously or unintentionally transfer their own value systems into the algorithms."[44] Nevertheless, from the example above, it is clear that AI might be affected by the bias of the software developer who decides what kind of information and values incorporate into the machine. As it is not feasible to control the bias, thus the use of AI systems can harm the independence and impartiality of the judiciary.

[41] ECtHR, *Hauschildt v. Denmark,*, 24.5.1989, § 46.
[42] European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, European Commission for the efficiency of justice, p. 5. (3-4 December, 2018) *available at* https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c
[43] European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, p. 9.
[44] European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, p. 57

The equality of arms rule provides that all parties should have the same procedural rights unless there is an objective and reasonable justification not to do so, and there is no significant disadvantage to either party. Predictive justice systems are designed and can be helpful for judges in their decision-making and provide the scheme of the probability of success for the outcome of each type of dispute. The European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment has verified this since it has been stated in the Charter that: "The use of technological means should not cause imbalances between parties, since the use of digital means can indeed facilitate proceedings for certain operators and, on the contrary, pose difficulties for certain population types that are more uncertain or less familiar with computers. It is important that individuals are not left alone in front of their screens, and that they are informed that they can seek legal advice and are assisted where necessary".[45] It is possible that the parties would be imbalanced because of their different technological abilities or, for example, because of their age. Hence, the use of predictive justice systems can cause imbalances between the parties and violate the equality of arms principle.

The requirement of immediacy is the essential element to a fair trial. It has two core elements: the possibility to present the trial materials instantaneously to the tribunal, and the presence of the same judges for the duration of the proceedings and decision of the case. Every related fact must be presented to the court by straight means that are detected by the sense of sight or sense of hearing. As legal research and decision-making are correlated, when AI is used to do legal research, it may anticipate the judgment for the case since otherwise, it cannot do research. So, AI can guide the judge on decision-making based on data other than actual case materials. It will be much more apparent in the case when AI is participating in the decision or deciding plain cases autonomously. European Ethical Charter has suggested that parties must be clearly informed of any prior processing of a case by AI before or during a judicial process and have right to object, so that the case can be heard directly by a court within the meaning of Article 6 of the ECHR. [46] So, the use of AI may contribute to the immediacy of the court process by providing rapid legal research. Meanwhile, it is possible that the use of AI in the process could increase the already existing bias.

The right to a fair trial includes the possibility to learn the reasons for the court's decision. The extent of the duty to give reasons varies from the nature of decisions and factual circumstances of the case. While using AI to define the reasoning of the case, the issue of

[45] European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, p. 48.
[46] European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, p. 12.

transparency arises. The European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment has stated that there must be a balance between the intellectual property of certain processing methods and the need for transparency, impartiality, fairness and intellectual integrity when AI tools are used that may have legal consequences or may affects people's lives.[47] It means that the whole operating chain of the selection process and organization of data which directly impacts the learning phase of an algorithm has to be changed. In order to guarantee the reasoning of cases from AI systems, the code of human behavior has to be applied to it, which is extremely hard to imagine.

Thus, the use of AI in the court proceedings can contribute to the processing of the judicial workload promptly and efficiently, as AI is capable of processing information on a scale that is out of reach of any human judge. The application of AI will have a positive impact on the reasonable time requirement. AI algorithms can eliminate human failures, and significantly improve the work of a judge, go through big data and sort information, promote legal certainty with the possibility of doing in-depth research. Even so, the use of AI systems in the court proceedings can harm the independence and impartiality of the process, as human-created algorithms use the data provided by creators. Considering the positive impact of AI on the quality and efficacy of judicial system and bearing in mind that data-driven decisions may undermine the independence and impartiality of the process, the suggestion is to adjust the provisions of the European Ethical Charter to the current regulations of the European Convention of Human Rights. Thus, the regulations will be binding for all parties to the Convention. Besides, the European Court of Human rights, as a competent body will hear applications in the cases of breach of the right to a fair trial in automated proceedings.

[47] European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, p. 11

Chapter 3. The impact of AI on right to freedom of elections

The increasing digitalization of society around the world creates unprecedented opportunities for communication between citizens, politicians, and political parties. Social media and social messaging changed how politicians and electorates interact. The information related to elections flowing faster and easier than ever, coupled with expanded opportunities for its verification and correction by a growing number of stakeholders. AI technologies are used in electoral processes in the form of electronic voting (from voter registration to the tabulation of results). The issue arises whether the use of voting and counting technologies complies with international standards for democratic elections. New technological developments raise concerns about the disruptive impact on public debate. The political micro-targeting of individual voters driven by unlawfully obtained data raises the need to safeguard the integrity and credibility of electoral processes. The capacity of algorithms to inconspicuously amass data can be employed by candidates to manipulate voters by predicting their preferences.

The right to free elections is internationally recognized in a set of international documents. In particular, Article 3 of Protocol No. 1 of the European Convention of Human Rights states as follows: "The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature".[48] The right to free elections does not just concern the organization of elections. In essence, it entails recognition of universal, equal suffrage and encompasses both the right to vote and the right to stand for election. The expression of the will of the people must be respected through free elections. Therefore the confidentiality of voters' choices must be guaranteed when they vote. The requirement of elections been organized at reasonable intervals has to be followed. Every state is obliged to ensure that votes are cast by secret ballot or by equivalent free voting procedure since it is the heart of the democratic election process. Secrecy of the vote means that it should not be possible to associate a ballot with a specific voter. The essence of confidentiality is to grant the

[48] Protocol No.1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms (20 March,1952) *available at* https://www.refworld.org/docid/3ae6b38317.html

voter capability to exercise her or his choice freely, without the potential for coercion, intimidation, or vote-buying.

The growing use of AI in the elections process has advantages and raise potential challenges as well. While using AI, the main issue arises related to the direct physical observation of procedures. That is why many countries suspended using AI and returned to traditional paper-based elections. In case of use of algorithms in the voting process, the first issue is that the voters must not be able to prove to anyone how they voted, and the system itself must not allow identification of a voter with her or his vote. Likewise, there is a need to ensure the **secrecy** of ballots, so to ensure that receipts or codes provided to voters to verify the vote was recorded as cast. There is a number of potential risks, such as flows in design of system or possibility of outside hacking. In particular, the automated voting process is the transfer of large amounts of information from one point to another. Of course, traditional voting system does not fully guarantee the security, but the key difference from electronic voting is that the interference with the process can be recognized by an average citizen. There should be effective measures incorporated to deprive the system from illegal external access as elections and referendums are meant to address vital issues for the public, and any change in the data will also have irreversible consequences for the society. The optimal solution for security policy shall include provisions on technical and technological solutions for the fast restoration of the system in case of system failure and the preservation of the results of the voting. Similar to the confidentiality of votes, the critical issue is to provide the integrity and public confidence towards the AI-driven results during counting and reporting results. Thus, an independent body has to assess the counting process of votes.

The equality of the vote is the main principle of electoral rights. The key aspect of the law of equality is that no voter will be able to cast more votes than another, nor will citizens be prevented from participating in voting. While voting technologies are used, the main objective is to prevent any person from casting more votes than is established by law and must avoid any votes from being subtracted from the system. The use of technology in the voting process that discriminates against certain groups of voters or discourages them from participating would not be in accordance with law.[49] When new systems are used with traditional paper-based voting, the voters should receive equivalent means of voting not to endanger the equality of the vote. With electronic voting, voters get easier access and chance to participate in elections, when deprived of accessing polling stations, living outside their home country. Though, electronic

[49] OSCE Ministerial Council, Decision No. 5/03, "Elections", (2 December 2003).

voting cannot become the exclusive mean as less computer-literate voters may have problems operating systems.

The cornerstone of any election process is transparency, as candidates and observers should have the opportunity to observe the work of election authorities at all levels, and especially the voting, counting and tabulation processes. When AI systems are introduced to the election process, observers need to have additional access in order to be confident that the election is in full accordance with the law and with democratic principles. The 2003 Maastricht Ministerial Council Decision No. 5/03 underlined the importance of the accountability of those involved in an election process to the electorate.[50] The key objective to provide accountability is keeping detailed minutes of how voters and administration interact with the system. The minutes have to be confirmed by an independent auditor.

The consequences of AI interference with electoral processes can be observed in case of "gerrymandering," which is the manipulating map-drawing process of electoral district boundaries to gain the advantage in elections for a particular political candidate or party. During the process, the methods of "packing" and "cracking" are used. "Packing" refers to packing unwanted voters into minimum numbers of electoral districts to decrease their representation in other places, while "cracking" spread unwanted voters in many places as possible to outnumber them. The US case-law prohibits racial gerrymandering, while political gerrymandering is considered to be legal. As it was exemplified many times, AI and algorithms are tailor-made for data processing, profiling, and calculation of probabilities, which is the main requirement for gerrymandering. [51]As was noted, racial gerrymandering is illegal, unlike political gerrymandering. The issue is that artificial intelligence can use political affiliation as a proxy for race. For instance, in 2018 House of Representatives Midterm Election in the USA, 90% Black voters voted for a Democratic candidate.[52] So, AI can easily use this correlation for proxy discrimination.

The operation of AI also may create "filter bubbles"- fully automated echo chambers in which individuals only see pieces of information that confirm their own opinions or match their profile.[53] The actual impact of "filter bubbles" and targeted misinformation on the formation of political opinion is difficult to determine accurately, political opinion is difficult

[50] Ibid.
[51] Ibid
[52] Jordan, E., How Computers Turned Gerrymandering Into a Science (6 October,2016) available at https://www.nytimes.com/2017/10/06/opinion/sunday/computers-gerrymanderingwisconsin.html
[53] Recommendation CM/REC of the Committee of Ministers on standards of e-voting (6 October, 2017) *available at* *https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f*

to determine accurately.[54] The curation and manipulation of online content on social media platforms occurred during U.S. elections, researchers reportedly manipulated the Facebook platform to influence users voting behavior by telling them how their friends had said they had voted, without users' knowledge, and were able to convince a statistically significant segment of the population to vote in the congressional mid-term elections on 2 November 2010.[55] In this way, Facebook and other dominant online platforms have the ability to influence elections. Social bots emulate the activity of human users by keeping their artificial nature disclosed. Research into the extent to which the presence of social media bots affected political discussion around the 2016 U.S. Presidential election suggests that it can negatively affect democratic political discussion rather than improving it, which in turn can potentially alter public opinion and endanger the integrity of the election process.[56] The nature of representative democracy comprises free and fair elections in which residents can determine their conscience, released of manipulation. As stated earlier, AI threatens to undermine fair elections if it continues to be methodically used to manipulate voters and promote extreme narratives. However, these tools can be used to support democracy and increase civic engagement. An ethical approach to AI can serve to acquaint and assist an electorate.

Electronic voting system is used also in Armenian realms. In particular, Article 62 of the Electoral Code of Republic of Armenia regulates the proceedings of the organization of voting in diplomatic and consular representations. The provisions of this Article are applicable to military servants seconded for a long-term study abroad and the employees of legal entities registered in RA. In particular, electors who are on diplomatic service and consular representations and members of their families residing abroad…may participate in elections of the National Assembly by voting electronically in the manner and within time limits prescribed by the Central Electoral Commission. Electronic voting may be held after the end of the time limit established for registration of the electoral lists for the political parties running in elections of the National Assembly, but no later than five days before the voting day. The decree N 32-N of CEC prescribes that CEC no later than ten days after receiving the list of voters by e-voting system, provide electronically encoded ballots to the MFA, the MOD, and Head of legal entity to send the voters.[57] The law provides detailed and scrutinized proceedings

[54] Nguyen, Tien T., "The Effect of Using Recommender Systems on Content Diversity", p. 677–686 *available at* *http://doi.acm.org/10.1145/2566486.2568012*

[55] Jonathan Zittrain, Engineering an election, Harvard Law Review Forum Vol. 127, 335 – 339 (2014).

[56] Bessi, Alessandro, and Emilio Ferrara. Social bots distort the 2016 U.S. Presidential election online discussion, FIRST MONDAY, Volume 21, no 11, 7 (November, 2016) *available at: http://journals.uic.edu/ojs/index.php/fm/article/view/7090/5653 (last visited on 25 September 2017).*

[57] Decree N 32-N of CEC of RA (6 May, 2012) *available at* *https://www.elections.am/majoritarian/election-24103/district-32/*

to ensure the security of voting. In particular, the system is designed in manner to ensure the accessibility of voters, equal suffrage, transparency and public confidence. One of the main issues during e-voting is to ensure the appropriate identification of a voter. The suggestion is to establish the mechanism when the e-voting system will be capable of taking a photo of voters and of identifying him with the ID information on the database. The described system is used by financial organizations for remote identification of customers as the Law on Combating money laundering and terrorism financing states that " The reporting entity shall define and apply risk management policies and procedures for authentication while establishing a business relationship with a customer and conducting a proper business review".[58]

Furthermore, the possible solution to ensure the security of e-voting can be monitoring the process by private companies since the organization of elections and referendums through electronic voting intends the use of expensive technologies, which is considerably costly for the State. In particular, it is more likely that the organization of elections and referendums through e-voting will be more effortless for organizations that have relevant experience, specialists, and technical equipment rather than for State at the expense of the state budget. In order to increase the efficiency of control, a licensing mechanism can be introduced. In particular, the amendment to the Law on Licensing can be made. Thus, the organization of elections and referendums through electronic voting can be classified as a type of licensed activity, as a result of which the State will acquire additional practical tools to control the activity of companies. In particular, the suggestion is while applying for a license, among the documents submitted to the competent authority by the person applying for a permit have to present a security policy for the organization of e-voting. Amongst others, the security policy should envisage provisions on effective restoration and preservation of voting results in case of system failure during voting. Furthermore, the suggestion is to contemplate the responsibility of the organizers of e-voting to publish instructions on the platform for voters. Finally, the calculation of the voting results must be public. Voters should be able to monitor on the platform the rates of votes distribution. Furthermore, the law can envisage the preservation of data on the outcome of elections for a fixed time limit for probable recalculation.

So, e-voting in an efficient tool in the prospect of affordability and resource-saving. Nevertheless, when enforcing the model, the core issue is the employment of technical, technological, and legal mechanisms that minimize the above-mentioned risks. For instance, the system should be able to depict all options for voting without any prejudice. Likewise, the

[58] Law on Combating money laundering and terrorism financing of RA, HO-80-N (June 21, 2008)

counting of votes shall be public. The voters need to be capable of survey throw platform the distribution of votes.

Conclusion

The conducted research has shown that AI, in all likelihood, will advance on developing and providing a vital impetus in prospect. The outlined issue was to assess whether the current regulations are effectively responding to the challenges or whether new human rights regimes of institutional governance are needed to warrant that risks can be purposefully addressed in practice. Nevertheless, there are numerous reasons why existing rights discourse and enforcing tools may need reconsideration if they are to implement adequate protection. So, the research revealed that the growing power of AI would require to reconceive human rights in new ways, as well as to develop a different vernacular for rights discourse – one that recognizes the central role of socio-technical configurations in affording and constraining the freedoms and capabilities that people enjoy. The scope of existing rights evolved in a pre-networked age. Therefore, the living instruments may fail to provide adequate protection.

In the framework of research it was acknowledged that AI content moderation systems could potentially control freedom of expression. Furthermore, algorithms risk shifting actual content for public discussion while refining the speech to excrete hateful content. The suggested solution for the issue is the application of "regulation by design" approach by AI-developers as the human oversight over these systems is paramount in all stages of development and employment of systems. This strategy aims to create more accountable and privacy-friendly AI content moderation systems. Moreover, the noteworthy fact is that there is no legal framework to shape the effects of AI on the freedom to speech. The recommended solution for the issue is the development of dispute resolution and enforceability standards in conformity with the rule of law. They can be incorporated in the European Convention on Human Rights and other human rights documents. Thus, the probability of human oversight in case of complaints regarding the use and impacts of algorithms for content regulation can provide a vital protection net for the rights and freedoms of affected users.

Further discussion was focused on the impact of AI on the right to private and family life. It was noted that the capacity of algorithms to promote the accumulation of data gathered from a digital search of users might produce unpredictable outcomes for the data subject. Then

the conducted research showed that GDPR and Convention 108 set a significant safeguard for illegal data collection and processing. Furthermore, the discussion on how governments use AI to contain and combat the pandemic showed that when systems can favor society when they are deployed in conformity with the principles of transparency and legitimate aim. The conclusion is that States must deprive the population from the risk of trivialization of mass surveillance, stressing the importance of the principle of accountability and necessity of risk assessment procedures.

In the light of research on how AI impacts prohibition of discrimination has shown that non-discrimination statutes typically focus on discrimination based on protected characteristics, such as race, gender, language, religion, political, or other opinions. Since non-discrimination law leaves gaps, the recommendation is the development of additional sector-specific rules and regulations to protect people against newly invented classes of discrimination. Therefore, the regulations will enforce States and private companies to mitigate and prevent discrimination risks of the use of AI systems for groups that have an increased risk of their rights being disproportionately impacted by it.

The analysis of the use of AI in the judicial system revealed that it can be useful from the perspective of reasonable time requirement and promote legal certainty with the possibility of doing in-depth research. Meanwhile, it can harm the independence and impartiality of the process, and negatively affect equality of arms principles. During the discussion, it was revealed that the European Ethical Charter on the use of AI in judicial systems and their environment developed vital regulation for the use of AI in the judicial system, but still, they are not binding for the parties. Thus the suggestion is to adjust the provisions of the European Ethical Charter to the current regulations of the European Convention of Human Rights. So, the European Court of Human Rights will be the competent body to communicate the cases of violations of the right to a fair trial.

The assessment on how AI impacts the rights to the free election has illustrated that one of the main issues during e-voting is to ensure the appropriate identification of a voter. The suggestion for this point was the establishment of the mechanism when the e-voting system would be capable of taking a photo of voters and of identifying him with the ID information on the database. Another recommendation is to pass the organizational and monitoring power of e-voting to private companies. The State can establish control on private companies by amending the Law on Licensing and envisaging a specific class of licensing for the organization of e-voting. Thus, the organization of electronic voting will be classified as a type of licensed activity, and the State will be capable to control the operation of companies. In

particular, the suggestion is to envisage the provision that a company applying for the license, among other documents submitted to the competent authority, has to present a security policy for the organization of e-voting. Amongst others, the security policy should envisage provisions on effective restoration and preservation of voting results in case of system failure during voting. Furthermore, the suggestion is to contemplate the responsibility of the organizers of e-voting to publish instructions on the platform for voters. Finally, the calculation of the voting results must be public to ensure public confidence towards the AI-driven results. Voters should be able to monitor on the platform the rates of votes distribution. Furthermore, the law can envisage the preservation of data on the outcome of elections for a fixed time limit for probable recalculation. The probable solution to provide accountability and transparency of e-voting is keeping detailed minutes of how voters and administration interact with the system. The minutes have to be confirmed by an independent auditor.

Finally, considering the velocity and scale at which technologies can operate, and the substantial hazard that infringements may erode the common socio-technical foundations that are fundamental for freedom, democracy, and human rights the suggestion is to consider mapping risks and opportunities arising from the development of AI and create a legal framework which will adequately address the imposed challenges on human rights and create a preventive strategy. The document can be in the form of a new Convention on Human Rights in a Networked Digital Age, which will be in conformity with standards of human rights, democracy, and the rule of law. It will be envisaged both for public and private actors and will contain accountability and oversight regimes.

BIBLIOGRAPHY

Web sources

1. Universal Declaration of Human Rights (10 December, 1948).
2. European Convention on Human Rights (European Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, 4 November 1950).
3. International Covenant on Civil and Political Rights (16 December,1966).
4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January, 1981).
5. Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, (13 February 2019).
6. Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 177),(4 November, 2000).
7. Council Directive 2000/43/EC of 29 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (June, 2000).
8. U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L,7, (23 March, 2017).
9. General Data Protection Regulation (GDPR) (5 May, 2016).
10. Council of Europe, European Court of Human Rights Guide on Article 6, Right to a fair trial, criminal limb (31 December, 2013).
11. Council of Europe, European Court of Human Rights Guide on Article 6, Right to a fair trial, civil limb, (31 December, 2018).
12. European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, European Commission for the efficiency of justice (4 December, 2018).
13. Artificial Intelligence, European Perspective (2018).
14. Wagner, B. "Study On The Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implication", Council of Europe, Committee of Experts on internet intermediaries (MSI-NET) (2017).

15. UNHRC, Report of the Working Group on the Universal Periodic Review (2018).
16. The Global Principles on Protection of Freedom of Expression and Privacy (2017).
17. Directive 2000/31/EC June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000).
18. OSCE Ministerial Council, Decision No. 5/03, "Elections" (2 December, 2003).
19. Recommendation CM/Rec 6 of the Committee of Ministers to Member states on measures to promote and respect for freedom of expression and information with regard to internet filters (2008).
20. Recommendation CM/REC of the Committee of Ministers on standards of e-voting (6 October, 2017).

Books and journal articles

1. Gina, N. P., Talking to Bots: Symbiotic Agency and the Case of Tay, International Journal of Communication 10 (2016).
2. Edwina L. Rissland, Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning (1990).
3. Jordan, E. How Computers Turned Gerrymandering Into a Science (6 October, 2016).
4. Nguyen, Tien T., "The Effect of Using Recommender Systems on Content Diversity" (2014).
5. Jonathan Zittrain, Engineering an election, Harvard Law Review Forum Vol. 127 (2014).
6. Bessi, Alessandro, and Emilio Ferrara. Social bots distort the 2016 U.S. Presidential election online discussion, FIRST MONDAY, Volume 21, no 11, 7 (November, 2016).
7. Hugh Collins and Tarunabh Khaitan, Indirect Discrimination Law: Controversies and Critical Questions (2018).
8. A Theory of Discrimination Law (2015).
9. T.J. Buocz, Artificial Intelligence in Court – Legitimacy Problems of AI Assistance in the Judiciary (2018).
10. L. Edwards, & M. Veale, "Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions?", IEEE Security & Privacy (2017).
11. Darren, B. China's hi-tech war on its Muslim minority. Retrieved from Guardian (April 11, 2019).

12. Paul, M. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. Retrieved from New York Times (April 14, 2019).