PRIVACY IN THE AGE OF ARTIFICIAL INTELLIGENCE

GULKHANIM SURKHAYLI[1]

Abstract

Artificial intelligence is now ubiquitous. The use of artificial intelligence can both benefit society and violate human rights. These technologies collect, analyze, and sometimes transmit large amounts of personal data. This data predicts human behavior in advance. Some programs, such as spam filters or online shopping offers, may seem harmless, but others can have more significant effects and potentially pose threats to our privacy. Extensive government surveillance of citizens and outsiders infringes on privacy. Giant search engines, social media networks, and e-commerce businesses have adopted a business model that routinely and seriously abuses personal information. In recent years, this trend has developed further. Authorities and civil society need to understand the consequences, dangers and promises of artificial intelligence. In this article, we have explored artificial narrow intelligence and its impact on human rights, particularly the right to privacy. The legal nature of artificial intelligence and its potential impact on the right to privacy is the subject of this article. The subject of this article is the rapid development of artificial intelligence today and the reconciliation of conflicts that arise in the implementation of human rights through the application of artificial intelligence. First, we illuminate the discussion by providing basic technical definitions, then we examine the main directions of the impact of artificial intelligence on the right to privacy, and describe the current challenges. All this is done to better understand the results of artificial intelligence. Finally, we offer some initial offers for legal solutions that can be pursued by civil society organizations and other stakeholders engaged in AI campaign activities. We support the development and use of artificial intelligence in accordance with human rights norms and legal requirements in the relevant fields. We first offer a review of the impact of these developments on people's right to privacy, as well as map the regulatory framework and outline the roles and responsibilities of the various actors in the sector. Based on what is said in this article, we believe that it is important to do more research and focus on the impact of artificial intelligence on human rights. Furthermore, at this point, we call on governments to take the following measures: there are various human rights issues that arise with the many applications and types of artificial intelligence. Existing laws should be reviewed and, if necessary, updated to eliminate the effects of risks to human rights, particularly the right to privacy. The creation, use, study and improvement of artificial intelligence should be subject to minimum criteria such as respect for international human rights standards and its preservation. To understand the multitude of scenarios in which AI will affect human rights, it is important to collect and highlight examples of AI's impact. Another approach could be to include transparent and explainable AI algorithms to the design of AI systems so that individuals understand how their data is being used and can exercise their privacy rights. Ultimately, the key to resolving the conflict between the demands of the times and the right to privacy in the age of artificial intelligence is to strike a balance between the two values, recognizing that they are both important and necessary for a healthy, progressive society. We hope to contribute to such an understanding by publishing this article.

Keywords: *artificial intelligence, machine learning, right to privacy, data protection, privacy, non-discrimination, transparency, accountability.*

I. Introduction

The capability of artificial intelligence (AI) to recognize patterns and progressively "derive the intimate from the available" gives rise to a number of concerns regarding privacy in the context of AI [21]. Processing massive quantities of data is required for the capacity to function properly.

The right to privacy can be impacted in a variety of ways depending on the implementation or utilization of AI, including the following:

[1]Advocate, the member of the Bar Association of the Republic of Azerbaijan / gulyaxalilova@yahoo.com

- Sensors that produce and gather immense quantities of data with no awareness or permission of the individuals in their neighbourhood are frequently included in artificial intelligence-powered commercial products and self-driving technologies;
- AI techniques are currently applied to profile individuals with the help of population-scale data;
- AI techniques are being deployed to recognize individuals who want to stay unidentified. AI instruments are getting utilized to deduce and produce sensitive information about humans relying on their insensitive data;
- AI techniques are being used to arrive at subsequent choices employing such data, a certain number of which significantly impact the lives of individuals; and furthermore.

Investigating an impact of these innovative intrusions into privacy is important for the following reasons: privacy is essential to the use of a wide variety of human rights, including the freedom of expression and the freedom of association; privacy is also essential to the exercise of personal autonomy and freedom of choice [30]; and privacy is essential to the exercise of larger societal norms [22].

II. Utilization of the AI technologies

Products for consumers, such as smart house devices, networked vehicles, and mobile applications, are frequently designed with exploiting data in mind. This includes the use of consumer information. Consumers are frequently confronted with an instructional imbalance regarding the nature and quantity of the data that is generated, processed, or shared by the products, networks, and sites that they use. It is becoming more and more crucial to educate people in general about the manipulation of personal data as we continue to introduce more intelligent and networked gadgets into our residences, places of employment, public areas, and even our own bodies.

Identification and tracking applications based on artificial intelligence may be employed to recognize persons within multiple platforms, in their residences, at their places of employment, and outdoors. This makes it possible for people to be tracked. For instance, even though personal data is typically anonymized within databases, AI might be used to de-anonymize this data, calling into question the differentiation between private and not private data, that forms the foundation of the present data privacy legislation [10]. Individuals can be monitored and recognized in additional ways, including through the use of technology that recognizes their faces [4]. It also has a possibility of altering people's expectations regarding their ability to remain anonymous while in public spaces.

Even more impressive, machine learning algorithms are able to recognize approximately 69% of the demonstrators who were covering their features with hats and headscarves [7]. In the setting of law enforcement, recognition of facial features can give officers the ability to recognize individuals without the need for probable reason, reasonable doubt, or any additional formal criteria that would otherwise be necessary for law enforcement to acquire identity using conventional means. This can be a significant benefit to law enforcement.

Extremely private information might be inferred or forecasted employing machine learning techniques, and this can be done via non-sensitive types of data as input. Typing patterns on the keyboard of a computer may be used to infer a person's mental condition, including their confidence level, level of anxiousness, level of melancholy, and level of fatigue [3]. When seemingly unconnected data, such as activity records, phone parameters, location data, or social network likes, are used to make inferences about private data that is sensitive, such as information about an individual's medical condition, sexual orientation, ethnic background, or views on politics, this practice is known as profiling, and it may end up in serious threats to privacy as well as discrimination.

Everyone and every group are profiled in order to divide, score, categorize, evaluate, and position them. Applications powered by AI utilize data to automatically divide, score, categorize, evaluate, and place people, regularly with no permission or knowledge, and usually without having the ability to dispute the results or effectiveness of those procedures. For example, in 2016, IBM advocated the application of AI to differentiate between "authentic" immigrants and other kinds of migration [18]. In addition, machine learning is playing an increasingly important part in ranking

systems, which are used to determine eligibility for various benefits, such as credit, jobs, housing, and welfare services.

Systems with artificial intelligence might be employed to formulate or influence conclusions regarding individuals or their surroundings, theoretically according to classification. These decisions can be made about individuals or their surroundings as well. Major issues concerning privacy, autonomy, and the morality associated with these modifications are raised when considering a setting that is aware of the user's interests and can adjust itself accordingly to the assumed areas of interest. As we progress towards networked places like smart towns or augmented and virtual reality, personalization, not only in terms of information, but additionally of our understanding of the world, will develop into a more and more essential aspect of how we live [19].

The manner in which the word "AI" is used in regulation and policy conversations to mean a wide variety of programs, applications, and techniques makes it more difficult to have fruitful discussions about AI policy and concerns regarding privacy. When artificial intelligence (AI) is brought up in an extensive sense, there is an inclination for people to presume that the technology at hand presents issues that are so fundamentally novel that none of the currently current regulations, laws, or standards are adequate or suitable. This is because there is an inclination for AI to be considered in such a general manner. The "other side" of this debate is to call for the governance of technological innovation in and of itself, independent of how or where it is implemented.

In order to avoid falling for any of these falsehoods, it is necessary to investigate the ways in which previously established ideologies, such as laws concerning human rights, data protection, industry privacy laws, and scientific ethics, are connected to the various uses and techniques of artificial intelligence.

In the following paragraphs, we will describe how multiple of these established structures can be applied, as well as the areas in which they are lacking. In addition, we will talk about a variety of AI-specific efforts that are explicitly focused on protecting the confidentiality of users. Some of these efforts are specialized, while others tend to be more broad.

The most basic right to privacy is recognized by the legislation governing international human rights. As an example, Article 12 of the Universal Declaration of Human Rights (UDHR) declares that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence …. Everyone has the right to the protection of the law against such interference or attacks" [6].

Any violation of a person's right to privacy is not only required to be in compliance with legislation [26], but it additionally needs to be essential and in the appropriate amount. This is a requirement under international law governing human rights [27]. To the degree that states create or employ AI in a way that violates the right to privacy, those actions need to be submitted to the three-part test of legitimacy, necessity, and proportionality. This scrutiny is required whenever governments build or utilize AI in a way that violates the right to privacy.

Advocates and officials who use the international system of human rights are gradually recognizing and acknowledging the effect that novel types of data processing have on basic freedoms, which include the right to privacy. One of these rights is the right to data portability, which allows individuals to move their data from one location to another. Concerning profiling, for example, which could include making use of artificial intelligence (AI) tools to derive, deduce, or forecast information about people for the aim of assessing or evaluating certain factors about them, the United Nations Human Rights Council pointed out with worries 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 the right to privacy". This statement was made in reference to the fact that "automatic processing of personal data for individual profiling" [28].

In addition, worldwide human rights organizations have been making progress toward the recognition of the right to anonymity within the context of the rights to privacy, as well as freedom of thought and expression. It has repercussions for the artificial intelligence that is utilized to recognize people on the net, in their residences, and in public areas. For example, the UN Special Rapporteur on Freedom of Expression has frequently recognized this connection and emphasized that governmental intervention with confidentiality ought to be exposed to the three-part test of legitimacy, necessity, and

proportionality, just like all other interventions to these liberties. In addition, the UN Special Rapporteur on Freedom of Expression has made it clear that this test must be applied to any additional intervention with those rights [17].

When it comes to the research, development, and implementation of artificial intelligence, data protection frameworks come into play to the degree that personal data (as specified by the frameworks) becomes involved [29]. As a result, data protection frameworks currently restrict how artificial intelligence (AI) tools can process personal data, even though there is no specific reference to AI in these frameworks. The regulatory structures that are in place in different parts of the world may differ from one another, but they all share the goal of safeguarding the personal information of individuals and the recognition that such safeguards are an essential component of the individual's constitutionally protected right to privacy.

The EU General Data Protection Regulation (GDPR), which became effective on May 25, 2018, necessitates a valid reason for processing data. In addition to the fundamental values of equality, accountability, and transparency, the GDPR also encompasses the basic principles of purpose restriction and data minimization [7]. These fundamental principles are significant for the expansion, use, and utilization of artificial intelligence (AI) systems.

In addition, the GDPR places restrictions on the application of automated decision-making in specific contexts and mandates that individuals receive information regarding the occurrence of automated decision-making, the reasoning involved, as well as the importance and anticipated repercussions of the processing for the person in question. This information must be supplied to the person [7]. When it comes to matters that are legally or otherwise significantly impactful, the law imposes a blanket restriction on decisions that are made exclusively by automatic means, with a few limited exclusions[1].

In particular, the General Data Protection Regulation (GDPR) describes profiling as a method of using automatic methods to analyze or make projections about people [7]. This description acknowledges that personal data can be generated by machine learning applications and other types of monitoring in addition to the traditional methods [7].

In conclusion, the General Data Protection Regulation (GDPR) includes a wide variety of requirements that promote the development of less privacy-invasive technologies. Some of these rules possess implications for artificial intelligence. The goal of the requirement that data protection be built in from the start and be the default setting is to include privacy safeguards into the process of designing how data is processed [20].

Data Privacy Impact Assessments (DPIA), which are instruments that organizations use to cope with risks related to privacy, become obligatory for numerous privacy-invasive AI and machine learning programs that come under the purview of data protection law and come with significant expected risks, such as the processing of sensitive data. These programs fall into the category of falling under the purview of data protection law and come with serious predicted risks.

Data protection serves an essential function in protecting the right to privacy[2], but it is unable to tackle all of the privacy threats that emerge from the various implementations and deployments of artificial intelligence (AI). The scope of data protection is restricted to the preservation of information that pertains to an individual who can be recognized or located (even indirectly). This does not cover the privacy of organizations or other invasions of privacy which may not involve personal data. Likewise, this does not cover other types of privacy violations [16].

Although regulations such as those in the GDPR dealing with automated decision-making and profiling are extremely important, they can only have an impact on a limited number of applications of AI in automated decision-making [4] or profiling [13]. Furthermore, data protection frameworks often contain exclusions for national security, which restricts rights and protections in essential privacy-

[1]Article 22 of GDPR only applies to decisions "based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

[2]In 2011, the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression issued a report similarly noting that 'the protection of personal data represents a special form of respect for the right to privacy.' U.N. Doc. A/HRC/17/27, ¶ 58 (May 16, 2011).

invasive uses of AI, such as governmental eavesdropping. This is the case because national security is a legitimate concern.

In nations that have data protection structures, industry privacy regulations serve as a complementary layer of safeguarding personal information. The European Union's (EU) suggested ePrivacy Regulation, for example, addresses the privacy and confidentiality of communications and, as such, has consequences for powered by AI commercial goods such as digital companions. This regulation encompasses the privacy and confidentiality of communications. A person has the right, under French administrative law, to be given a justification for any administrative judgments that were made about them using a computer algorithm [12]. The clause pertains solely to administrative decisions, despite the fact that it is more general and thorough than the provisions on automatic decision-making in the GDPR.

Sectoral privacy legislation also plays an essential part in countries that do not have a universal data protection structure, such as the USA. In this country, all implementations of artificial intelligence are required to conform to established laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [14]. The city of New York has introduced a law that will create a committee to investigate the city's "automated decision systems" with the objective to render them better and more accessible for examination. The goal of this endeavor is to render the processes more transparent. This will extend to computerized algorithms that direct the distribution of resources such as public housing as well as food stamps. Other instances of such resources include police personnel and firehouses.

The application of sectoral legislation may additionally have an essential part of dealing with further context and domain particular problems posed by AI, such as those posed by driverless vehicles, for example. On the other hand, not all of the present privacy legislation in different industries are capable of effectively shielding individuals from the novel privacy risks presented by AI applications. Plenty of alternate credit-assessment instruments, such as those that depend on machine learning techniques for scoring, for example, have been successfully able to escape inclusion under the United States Fair Credit Reporting Act [15].

Artificial intelligence has the potential to make industry regulatory data less efficient. As an example, even strict regulation of healthcare records generally fails to tackle the reality that internet histories or credit card data can be used to deduce, assume, or forecast medical information. This is because these types of data are not considered health data.

Ethical guidelines for artificial intelligence are presently being developed by industry organizations, standards groups, and government agencies; some of these guidelines are specific, while others are more general.

For example, the Global Initiative on Ethics of Autonomous and Intelligent Systems of the IEEE has devoted a portion to the topic of privacy that is titled “Personal Data and Individual Access Control in Ethically Aligned Design”. This section focuses on the ethical considerations related to the collection and use of personal information.

One example of a sector-specific ethic code that includes a particular principle on the privacy of data is the German Ethics Code for Automated and Connected Driving, which seeks to resolve the conflict between data-driven business models and user restrictions on their freedom and control over their personal information [5].

There are numerous ethical issues that are specific to AI or its application in a specific discipline or setting; however, some of these obstacles are not always exclusive to AI. For example, there is a wealth of published material on business and human rights [30], in addition to the moral implications of big data research [10], a few of which may be instructive with regard to the potential dangers that AI poses to individuals' privacy. It is essential to emphasize that the global framework for human rights is applicable to non-state applications of artificial intelligence as well [9].

Distinct ethical and legislative privacy concerns are raised by various forms of artificial intelligence (AI) and their respective spheres of application. For example, the application of machine learning to recognize “terrorist” suspects presents a distinct set of privacy difficulties compared to the processing of data collected by driverless vehicles. This absence of definitional precision presents a

challenge, as different kinds of AI and various application sectors bring up unique ethical and regulation concerns.

People are typically incapable of fully understanding what types of data and the amount of data their electronics, systems, and platforms produce, analyze, or exchange with one another. When more and more intelligent and networked gadgets are introduced into people's residences, places of employment, public spaces, and even their bodies, the desire to educate people regarding the manipulation of their personal data becomes a growing concern. The use of artificial intelligence (AI) for purposes such as monitoring, or following, and recognizing individuals across machines as well as in public locations, exacerbates this imbalance in the current environment.

Some implementations of artificial intelligence can be obscure to people, authorities, or even the programmers of the system themselves, rendering it hard to question or investigate results. This can make it challenging to dispute or investigate outcomes. In this regard, it is crucial to differentiate among the following types of opacity: (1) opacity that is deliberate business or state secrecy; (2) opacity due to technical lack of education; and (3) opacity resulting from the features of machine learning methods and the scale necessary for using them usefully. In this setting, it is essential to differentiate between all sources of opacity [8]. Even though there are technological options to improve the comprehension or transparency of certain systems to benefit various stakeholders [1], an important obstacle remains in situations in which this is not feasible and in which adverse effects can be either critical to safety or human rights critical.

Recognition, classification, and automatic decision-making that are powered by AI can result in consequences that are unjust, discriminating, or prejudiced. This may be the case due to inconsistencies or biases in the data collected [23]. It is possible to incorrectly categorize, incorrectly identify, or pass unfavorable judgment on people, and these types of mistakes or prejudices may disproportionately impact certain categories of people. Precise projections may shed light on vulnerable characteristics that can be used to differentiate between individuals. On the contrary, incorrect data or data that has been systematically skewed in a certain direction can be fed into profiles, which may result in conclusions that are prejudiced or discriminating.

Certain applications of artificial intelligence, especially the use of machine learning, muddle the distinction between private and nonpersonal data (or PII (personally identifiable information) and non-personally identifiable information (non-PII) in the United States), which forms the basis upon which data protection and privacy laws are organized all over the world. Re-recognizing and de-anonymization are two of the terms that fall under this category. Data that is originally not personally identifiable (also known as non-PII or publicly available information) can transform into personally identifiable information (also known as PII) in a different setting or at a different moment in a period of time, which presents a unique risk for industry legislation. A comparable difficulty pertains to confidential personal info. The use of machine learning for profiling can deduce, assume, or forecast sensitive data out of non-sensitive data, which may compromise additional protections for private data that is sensitive.

We are in favor of the advancement and use of AI so long as it is done so in accordance with human rights norms and legal requirements in the relevant domains. Policy and technological solutions in this field need to satisfy the suggestions that were laid forth in this paper as artificial intelligence systems become progressively incorporated into a greater number of important social activities.

III. Conclusion

We have offered a preliminary review of the effects that these advancements have on people's rights to privacy, as well as mapped the regulatory framework and outlined the roles, obligations, and obligations that are owed by different participants in the sector. In addition to this summary, we hope that this work will give a concrete start toward developing strong civil society structures for activity and advocacy. We want to make certain that the organizations who are utilizing, developing, and managing AI are deemed responsible and respect international human rights standards, therefore we wrote this paper.

According to what is said in this article, we are of the opinion that it is essential to do more research on and keep an eye on the effect that AI has on human rights. Yet, at this juncture, we urge governments to take the following actions:

Examine whether or not the present structures and regulations are adequate: There are a variety of ethical and regulatory human rights concerns that are raised by the many applications and varieties of artificial intelligence (AI). Current laws need to be reexamined, and if required, updated, to address the implications of emerging and novel risks to privacy and freedom of speech. This is important to guarantee that these laws continue to protect persons from the dangers presented by artificial intelligence (AI).

In addition, we make the following requests of states and businesses:

The creation, utilization, study, and advancement of AI ought to be subjected to the minimal criterion of respecting, encouraging, and safeguarding international human rights standards. This has to be done in order to guarantee the preservation of international human rights standards. This ought to involve establishing knowledge of what defines AI human rights critical systems and making sure that laws and regulations, codes of conduct, ethical codes, and self-regulating and technological requirements meet the criteria established by international human rights. In addition, this ought to involve developing an awareness of what makes up "AI human rights essential systems".

Ensure accountability and transparency: Corporate, technical, and government entities must make space for worthwhile multi-stakeholder engagement, including players from civil society, in establishing technical standards, rules, and industry guidelines for artificial intelligence (AI) systems, as well as technology policy and industry standards, in order to guarantee open procedures and legitimate results. Particularly, voluntary structures need to be complemented with stringent accountability and monitoring systems in order to be effective.

In addition, we urge members of civil society to:

Continue your efforts to guarantee that any potential negative impacts on basic rights, such as the freedom of speech and privacy, are mitigated to the greatest extent possible. In order to do this, a comprehensive knowledge of the technology, the parties responsible for its development, and the environment where it is used is required.

Collect and bring attention to the research of "human rights critical" cases. AI: It is essential to gather and emphasize case studies that show the influence of AI in order to have a comprehension of the multiplicity of scenarios in which AI is going to have an effect on human rights. These case studies must include illustrations from different countries all around the world.

It is necessary to emphasize the necessity to construct knowledge-exchange initiatives and allow cooperative strategy formulation across different civil society organizations. In addition, it is crucial to foster expertise alliances and networks within civil society. Up to this point, academic institutions and private businesses have been in the vanguard of efforts to advance the discussion around the implications of AI for society. It is essential to amplify the voices of people engaged with technology in the public interest, despite the fact that actors from civil society serve an essential role in these discussions.

REFERENCES:

1. Datta, S. Sen, & Y. Zick, 'Algorithmic transparency via quantitative input influence: Theory and experiments with learning systems', In Security and Privacy (SP), 2016 IEEE Symposium, pp. 598-617.
2. Electronic Privacy Information Center (EPIC) and 45 organisations, Letter to Senators Grassley and Leahy and Representatives Goodlatte, Chaffetz, Conyers, and Cummings regarding the FBI's Use of Facial Recognition and Proposal to Exempt the Bureau's Next Generation Identification Database from Privacy Act Obligations, 2016.
3. Epp, M. Lippold& R.L. Mandryk, Identifying emotional states using keystroke dynamics' in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems., May 2011, pp. 715-724.

4. F.Kaltheuner, & E. Bietti, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR', Journal of Information Rights, Policy and Practice, vol 2(2), 2018.
5. Federal Ministry of Transport and Digital Infrastructure, Ethics Commission, Automated and Connected Driving, June 2017. URL:https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commissionreport.pdf?__blob=publicationFile (last access 20.12.2023).
6. G.A. Res. 217 (III) A, UDHR, art. 12 (Dec. 10, 1948).
7. General Data Protection Regulation (GDPR) of the European Union, 2016/679.
8. J. Burrell, 'How the Machine 'thinks': Understanding Opacity in Machine Learning Algorithms', Big Data and Society, 3(1), 2016.
9. J. Metcalf, & K. Crawford, 'Where are human subjects in big data research? The emerging ethics divide', Big Data & Society, 3(1), 2016p.2053951716650211; Zook, M. et al, 'Ten simple rules for responsible big data research', PLoS computational biology, 13(3), 2017, p. e1005399.
10. J.P. Achara,,G. Acs, and C. Castelluccia,'On the unicity of smartphone applications' at the 14th ACM Workshop on Privacy in the Electronic Society, October 2015, pp. 27-36.
11. Kaye, 2015. A/HRC/29/32, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. UN General Assembly, May 22.
12. Loi pour uneRépublique numérique (Digital Republic Act, Loi n 2016-132).
13. M. Hildebrandt., and, B.J. Koops, 'The challenges of ambient law and legal protection in the profiling era', The Modern Law Review, 73(3), 2010, pp.428-460.
14. M. Hurley, & J. Adebayo, 'Credit Scoring in the Era of Big Data', Yale JL & Tech., 18, 2016, p. 148.
15. M. Veale., L. Edwards, 'Enslaving the Algorithm', op.cit.
16. M. Veale., L. Edwards., H. Bear, (draft, Jan 2018 for PLSC Europe). Better seen and not (over) heard? Automated lipreading systems and privacy in public spaces.
17. Office of the U.N. High Commissioner for Human Rights, Report on encryption, anonymity, and the human rights framework, U.N. Doc. A/HRC/29/32 (22 May 2015).
18. P. Tucker, Refugee or Terrorist? IBM thinks its software has the answer, Defense One, 27 January 2016.
19. Privacy International, 'Smart Cities: Utopian Vision, Dystopian Reality', October 2017.
20. R. Binns, 'Data protection impact assessments: a meta-regulatory approach' International Data Privacy Law, 7(1), 2017, pp 22-35; L. Edwards, & M. Veale, 'Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?', IEEE Security & Privacy, 2017.
21. R. Calo, Artificial Intelligence Policy: A Primer and Roadmap, 2017.
22. R.C.Post,., 'The social foundations of privacy: Community and self in the common law tort', California Law Review, 1989, pp. 957-1010.
23. S. Barocas, & A. Selbst, 'Big data's disparate impact', Cal. L. Rev., 104, 2016, p. 671.
24. S. Walker, Face recognition app taking Russia by storm may bring end to public anonymity, The Guardian, 17 May 2016.
25. T. Payton and T. Claypoole, Privacy in the age of Big data: Recognizing threats, defending your rights, and protecting your family, Rowman & Littlefield, 2014.
26. U.N. Human Rights Committee, General Comment No. 16 (Article 17 ICCPR), 8 Apr. 1988, para 3.
27. U.N. Human Rights Committee, Toonen v. Australia, Comm. No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (31 Mar. 1994), para. 8.3.
28. U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L,7, 23 Mar. 2017, para 2.
29. UK Information Commissioner, Discussion paper Big Data, artificial intelligence, machine learning and data protection.

URL:https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (last access 20.12.2023).

30. UN Guiding principles on business and human rights: implementing the United Nations "Protect, Respect and Remedy" framework, 2011.

SÜNİ İNTELLEKT DÖVRÜNDƏ ŞƏXSİ TOXUNULMAZLIQ HÜQUQU

GÜLXANIM SURXAYLI[1]

Annotasiya

Süni intellekt indi hər yerdə mövcuddur. Süni intellektin istifadəsi həm cəmiyyətə fayda verə, həm də insan hüquqlarını poza bilər. Bu texnologiyalar böyük həcmdə şəxsi məlumatları toplayır, təhlil edir və bəzən də ötürür. Bu məlumatlar insan davranışını əvvəlcədən proqnozlaşdırır. Spam filtrləri və ya onlayn alış-veriş təklifləri kimi bəzi proqramlar zərərsiz görünə bilər, lakin digərləri daha əhəmiyyətli təsirlərə malik ola və potensial olaraq şəxsi toxunulmazlığımıza təhlükələr yarada bilər. Hökumətin vətəndaşlara və kənar şəxslərə qarşı geniş monitorinqi şəxsi həyatın toxunulmazlığına xələl gətirir. Nəhəng axtarış sistemləri, sosial şəbəkələr və e-ticarət fəaliyyətini həyata keçirən müəssisələr şəxsi məlumatlardan istehlakçılar üçün aşkar olmayan şəkildə müntəzəm və ciddi şəkildə sui-istifadə edən biznes modelini mənimsəmişlər. Son illər bu tendensiya daha da inkişaf etmişdir. Hakimiyyət orqanları və vətəndaş cəmiyyəti süni intellektin nəticələrini, təhlükələrini və vədlərini dərk etməlidirlər. Bu məqalədə süni dar intellekti, onun insan hüquqlarına, xüsusən də şəxsi toxunulmazlıq hüququna təsirini araşdırdıq. Süni intellektin hüquqi təbiəti və onun şəxsi toxunulmazlıq hüququna təsir etmə ehtimalı bu məqalənin obyektidir. Bu məqalənin mövzusu bu gün süni intellektin sürətli inkişafı və onun tətbiqi ilə insan hüquqlarının həyata keçirilməsində ortaya çıxan münaqişələrin uzlaşdırılmasıdır. Əvvəlcə əsas texniki tərifləri təqdim etməklə müzakirəni işıqlandırırıq, sonra süni intellektin şəxsi toxunulmazlıq hüququna təsirinin əsas istiqamətlərini araşdırır, mövcud problemləri təsvir edirik. Bütün bunlar süni intellektin nəticələrini daha yaxşı başa düşmək üçün edilir. Sonda biz vətəndaş cəmiyyəti təşkilatları və süni intellekt kampaniyası fəaliyyəti ilə məşğul olan digər maraqlı tərəflər tərəfindən izlənilə bilən hüquqi həllər üçün bəzi ilkin tövsiyələr təklif edirik. Müvafiq sahələrdə insan hüquqları normalarına və qanuni tələblərə uyğun olaraq süni intellektin inkişafı və istifadəsinin tərəfdarıyıq. Biz, ilk öncə, bu irəliləyişlərin insanların şəxsi toxunulmazlıq hüququna təsirinin nəzərdən keçirilməsini təklif etmişik, həmçinin tənzimləyici bazanın xəritəsini tərtib edib sektorun müxtəlif iştirakçılarının üzərinə düşən rolları, öhdəlikləri təsvir etmişik. Bu yazıda deyilənlərə əsasən, biz hesab edirik ki, süni intellektin insan hüquqlarına təsiri ilə bağlı daha çox araşdırma aparmaq və ona diqqət yetirmək vacibdir. Bundan əlavə, bu məqamda hökumətləri aşağıdakı tədbirləri görməyə çağırırıq: Süni intellektin çoxsaylı tətbiqləri və növləri ilə ortaya çıxan müxtəlif insan hüquqları problemləri var. Mövcud qanunlar yenidən nəzərdən keçirilməli və tələb olunarsa, insan hüquqlarına, xüsusən şəxsi toxunulmazlıq hüququna qarşı yaranan risklərin təsirlərini aradan qaldımaq üçün yenilənməlidir. Süni intellektin yaradılması, istifadəsi, öyrənilməsi və təkmilləşdirilməsi beynəlxalq insan hüquqları standartlarına hörmət, onun qorunub saxlanması kimi minimal meyarlara tabe olmalıdır. Süni intellektin insan hüquqlarına təsir edəcəyi ssenarilərinin çoxluğunu başa düşmək üçün süni intellektin təsirini göstərən nümunələri toplamaq vəonları vurğulamaq vacibdir. Başqa bir yanaşma, süni intellekt sistemlərinin dizaynına, şəxsi toxunulmazlıq hüququnun qorunmasına təşviq edən şəffaf və izah edilə bilən süni intellekt alqoritmləri daxil edilə bilər ki, fərdlər öz məlumatlarından necə istifadə edildiyini başa düşsünlər və şəxsi toxunulmazlıq hüquqlarını həyata keçirə bilsinlər. Nəhayət, süni intellekt dövründə dövrün tələbləri ilə şəxsi toxunulmazlıq hüququ arasındakı münaqişənin həllinin açarı iki dəyər arasında tarazlığı saxlamaq,

[1] Azərbaycan Respublikası Vəkillər Kollegiyasının üzvü / gulyaxalilova@yahoo.com

onların sağlam irəliləyən cəmiyyət üçün həm vacib, həm də zəruri olduğunu dərk etməkdir. Ümid edirik ki, bu məqalənin nəşri ilə belə bir anlayışa töhfə verəcəyik.

Açar sözlər: *süni intellekt, maşın öyrənməsi, şəxsi toxunulmazlıq hüququ, məlumatların qorunması, ayrı-seçkiliyin olmaması, şəffaflıq, hesabatlılıq.*

КОНФИДЕНЦИАЛЬНОСТЬ В ЭПОХУ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ГУЛЬХАНЫМ СУРХАЙЛИ[1]

Резюме

Искусственный интеллект (ИИ) сейчас распространён повсеместно. Использование искусственного интеллекта может как принести пользу обществу, так и нарушить права человека. Эти технологии собирают, анализируют, а иногда и передают большие объёмы персональных данных. Эти данные заранее предсказывают поведение человека. Некоторые программы, такие как спам-фильтры или онлайн-магазины, могут показаться безобидными, но другие могут иметь более серьезные последствия и потенциально представлять угрозу нашей конфиденциальности. Обширная государственная слежка за гражданами и посторонними нарушает конфиденциальность. Гигантские поисковые системы, социальные сети и предприятия электронной коммерции приняли бизнес-модель, которая регулярно и серьезно злоупотребляет личной информацией. В последние годы эта тенденция получила дальнейшее развитие. Власти и гражданское общество должны понимать последствия, опасности и перспективы искусственного интеллекта. В этой статье мы изучили искусственный узкий интеллект и его влияние на права человека, особенно право на неприкосновенность частной жизни. Правовая природа искусственного интеллекта и его потенциальное влияние на право на неприкосновенность частной жизни являются предметом данной статьи. Предметом данной статьи является стремительное развитие искусственного интеллекта сегодня и урегулирование конфликтов, возникающих при реализации прав человека, посредством применения искусственного интеллекта. Сначала мы освещаем дискуссию, предоставляя базовые технические определения, затем исследуем основные направления влияния искусственного интеллекта на право на неприкосновенность частной жизни и описываем текущие проблемы. Все это сделано для того, чтобы лучше понять результаты искусственного интеллекта. Наконец, мы предлагаем некоторые первоначальные предложения по юридическим решениям, которые могут быть реализованы организациями гражданского общества и другими заинтересованными сторонами, участвующими в кампаниях по искусственному интеллекту. Мы поддерживаем разработку и использование искусственного интеллекта в соответствии с нормами прав человека и требованиями законодательства в соответствующих областях. Сначала мы предлагаем обзор влияния этих событий на право людей на неприкосновенность частной жизни, а также наносим на карту нормативно-правовую базу и описываем роли и обязанности различных участников сектора. Основываясь на том, что сказано в этой статье, мы считаем, что важно провести больше исследований и сосредоточиться на влиянии искусственного интеллекта на права человека. Кроме того, на данном этапе мы призываем правительства принять следующие меры: существуют различные проблемы с правами человека, возникающие в связи со многими приложениями и типами искусственного интеллекта. Существующие законы следует пересмотреть и, при необходимости, обновить, чтобы устранить последствия рисков для прав человека, особенно права на неприкосновенность частной жизни. Создание, использование, изучение и совершенствование искусственного интеллекта должно регулироваться минимальными критериями, такими как уважение международных

[1] Член Коллегия Адвокатов Азербайджана / gulyaxalilova@yahoo.com

стандартов прав человека и их сохранение. Чтобы понять множество сценариев, в которых ИИ будет влиять на права человека, важно собрать и осветить примеры воздействия ИИ. Другой подход может заключаться во включении прозрачных и объяснимых алгоритмов ИИ в разработку систем ИИ, чтобы люди понимали, как используются их данные, и могли осуществлять свои права на конфиденциальность. В конечном счете, ключом к разрешению конфликта между требованиями времени и правом на неприкосновенность частной жизни в эпоху искусственного интеллекта является достижение баланса между двумя ценностями, признавая, что, они одновременно важны и необходимы для здорового, прогрессивного общества. Мы надеемся внести свой вклад в такое понимание, опубликовав эту статью.

Ключевые слова: *искусственный интеллект, машинное обучение, право на неприкосновенность частной жизни, защита данных, недискриминация, прозрачность, подотчетность.*

Məqalənin redaksiyaya daxil olma tarixi: 24.01.2024
Çapa qəbul tarixi: 15.05.2024