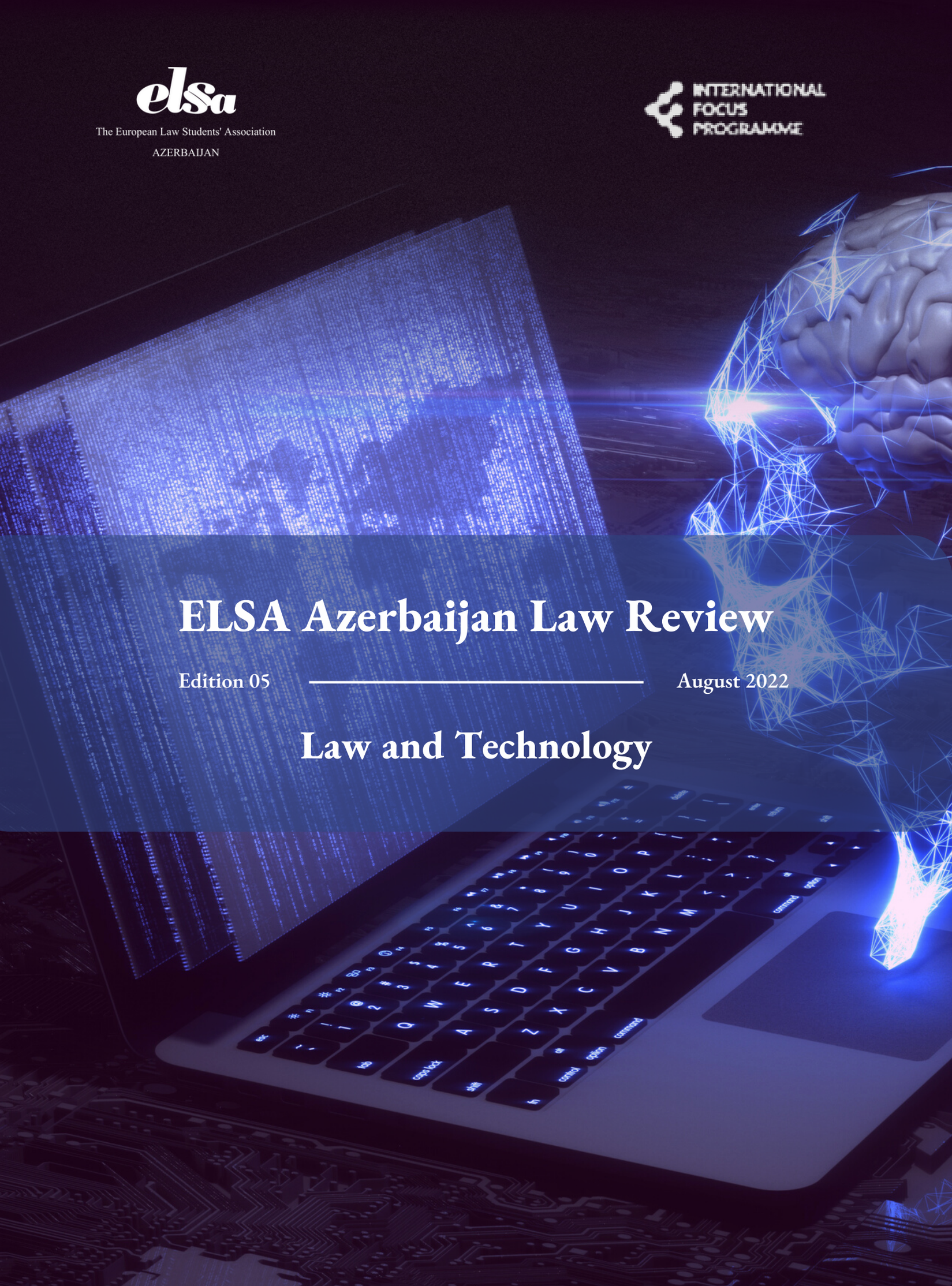
elsa
The European Law Students' Association
AZERBAIJAN

INTERNATIONAL FOCUS PROGRAMME



ELSA Azerbaijan Law Review

Edition 05 — August 2022

Law and Technology

ELSA HAQQINDA

The European Law Students' Association, ELSA, is an international, independent, non-political and non-for-profit organisation comprised of and run by and for law students and young lawyers. Founded in 1981 by law students from Austria, Hungary, Poland, and West Germany. ELSA is today the world's largest independent law students' association. ELSA is present in 43 countries.

ELSA's members are internationally minded individuals who have an interest in foreign legal systems and practices. Through our activities, such as seminars, conferences, law schools, moot court competitions, academic competitions, legal writing, legal research, and the Student Trainee Exchange Programme, our members acquire a broader cultural understanding and legal expertise.

ELSA has gained a special status with several international institutions. In 2000, ELSA was granted Participatory Status with the Council of Europe. ELSA has Consultative Status with several United Nations bodies: UN ECOSOC, UNCITRAL, UNESCO & WIPO.

Our Purpose:
To contribute to legal education, foster mutual understanding, and promote social responsibility of law students and young lawyers.

Our Vision:
"A just world in which there is respect for human dignity and cultural diversity".

Since 2010, ELSA Azerbaijan has been one of 43 National Groups that integrate ELSA International.

ABOUT ELSA

Avropa Hüquqşünas Tələbələri Assosiasiyası, ELSA, hüquq tələbələri və gənc hüquqşünaslardan ibarət və onlar tərəfindən idarə olunan beynəlxalq, müstəqil, qeyri-siyasi və qeyri-kommersiya təşkilatıdır. Təşkilat 1981-ci ildə Avstriya, Macarıstan, Polşa və Qərbi Almaniyadan olan hüquq tələbələri tərəfindən yaradılmışdır. ELSA bu gün dünyanın ən böyük müstəqil hüquq tələbələri birliyidir və 43 ölkədə fəaliyyət göstərir.

ELSA üzvləri xarici ölkələrin hüquq sistemləri və təcrübələri ilə maraqlanan şəxslərdir. Onlar təşkilat tərəfindən təşkil olunan seminarlar, konfranslar, hüquq məktəbləri, səhnələşdirilmiş məhkəmə müsabiqələri, akademik müsabiqələr, hüquqi yazı, hüquqi araşdırma üzrə layihələr və tələbə təcrübə mübadilə proqramları kimi fəaliyyətlər vasitəsilə daha çox biliklər və hüquqi təcrübə əldə edirlər.

ELSA bir sıra beynəlxalq qurumlarda xüsusi statusa malikdir. Belə ki, 2000-ci ildə ELSA-ya Avropa Şurasında iştirakçı statusu verilmişdir. Birləşmiş Millətlər Təşkilatının UN ECOSOC, UNCITRAL, UNESCO & WIPO kimi qurumlarında isə ELSA konsultativ statusa malikdir.

ELSA-nın məqsədi Avropanın müxtəlif ölkələrindən olan hüquq tələbələri və gənc hüquqşünasları eyni təşkilatda birləşdirməklə onlar arasında mənəvi-əxlaqi inteqrasiyaya, elmi biliklərin paylaşılmasına nail olmaq, onları sosial məsuliyyətə təşviq etməkdir.

ELSA-nın şüarı:
"İnsan ləyaqətinə və mədəni müxtəlifliklərə hörmətin mövcud olduğu ədalətli bir dünya".

2010-cu ildən etibarən ELSA Azərbaycan ELSA Beynəlxalqda təmsil olunan 43 ölkədən biridir

ELSA AZƏRBAYCAN HÜQUQ JURNALI

ELSA Azərbaycan Hüquq Jurnalı Avropa Hüquqşünas Tələbələr Assosiasiyası (ELSA) Azərbaycan tərəfindən elektron formada nəşr olunan, illik, hüquq tələbələri tərəfindən redaktə edilən və rəydən keçən hüquq jurnalıdır. Jurnal 2015-ci ildə yaradılıb və onun ilk buraxılışı 2016-cı ildə nəşr olunub.

ELSA Azərbaycan Hüquq Jurnalının məqsədi hüquq tələbələri və gənc hüquqşünasların hüquqi yazı və araşdırma bacarıqlarını inkişaf etdirmək, onların qabaqcıl hüquqi düşüncələrini cəmiyyətə çatdırmaq, həmçinin oxucularına aktual mövzularda hazırlanmış kontent təqdim etməklə elmi fikrin formalaşması və inkişafına öz töhfəsini verməkdir.

Jurnal həmçinin, hüquq tələbələrini hüquqi ədəbiyyat oxumağa və məqalələr yazmağa həvəsləndirməyi hədəfləyir.

Dünyanın hər yerindən tələbələr (bakalavr, magistr və ya doktorant), hüquqşünaslar və müəllimlər öz məqalələrini dərc olunması üçün ELSA Azərbaycan Hüquq Jurnalına göndərə bilərlər.

ELSA AZERBAIJAN LAW REVIEW

The ELSA Azerbaijan Law Review is an annual, student-edited, and peer-reviewed law journal published by the European Law Students' Association (ELSA) Azerbaijan. The journal was established in 2015 and its first edition was published in 2016.

The mission of the Law Review is to create a forum for the analysis and discussion of contemporary legal issues by serving as an avenue for the network to publish its academic work. It aims to provide law students and young lawyers, as well as the wider legal profession, with a source of critical commentary that is outside the scope of the typical legal curriculum.

Law Review also targets to motivate law students to read academic literature and write academic articles, to provide them with appropriate information related to highly important and topical discussions taking place in civil society, and to deliver young lawyers and students' articles to society.

Students (LL.B, LL.M, or Ph.D.), professors, scholars, and practitioners from all over the world are welcome to send their articles to ELSA Azerbaijan Law Review.

Editorial Board

Editor-in-Chief

Academic Reviewers

(in alphabetical order)

Article Editors

Fidan Abishsoy

Inci Seyidova

Laman Samadzade

Interview Editors

Ali Mammadov

Maleyka Jafarli

Narmina Huseynzade

Technical Editors

Gulshan Javadova

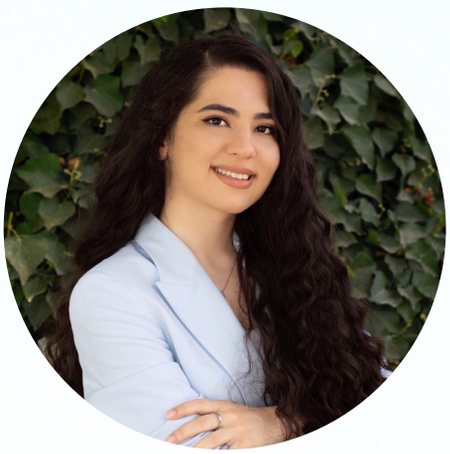
Maleyka Jafarli

Sevil Hasanli

Design Editor

Fidan Namazova

Redaksiya



Səbinə Zülfiyeva

2021/2022 fəaliyyət ili üzrə ELSA Azərbaycan Hüquq Jurnalının Baş redaktoru və ELSA Azərbaycanın Akademik Fəaliyyətlər üzrə vitse-prezidenti

Hörmətli oxucu,

ELSA Azərbaycan Hüquq Jurnalının 5-ci buraxılışını sizə böyük məmnuniyyətlə təqdim edirəm.

ELSA şəbəkəsi 2021/2022 fəaliyyət ilində "Beynəlxalq Fokus Proqramı" çərçivəsində hüquq və texnologiya arasındakı əlaqəyə xüsusi diqqət yetirdiyindən, biz də bu buraxılışı xüsusi mövzu üzrə nəşr etmək qərarına gəldik. "Hüquq və Texnologiya" mövzusuna uyğun seçilmiş mövzuda hüquq tələbələri və gənc hüquqşünaslar tərəfindən göndərilən hər bir məqaləyə görə minnətdarıq. Bu buraxılışda ən yaxşı 4 məqalə seçilərək dərc edilmişdir. Məqalələri seçilmiş müəllifləri ürəkdən təbrik edir, digər tələbə və hüquqşünasları növbəti buraxılışlar üçün məqalələr yazmağa dəvət edirəm.

Bu buraxılışda həmçinin, Azərbaycandan və dünyanın müxtəlif ölkələrindən "Hüquq və Texnologiya" sahəsində ixtisaslaşmış şəxslərlə müsahibələr yer alır. Dəvətimizi qəbul edib öz təcrübəsini oxucularımızla bölüşən bütün müsahiblərimizə təşəkkür edirəm.

Hər buraxılışda olduğu kimi bu buraxılışda da ELSA Azərbaycan Hüquq Jurnalı Redaksiya Heyətinin dəstəyi olmadan hazırlana bilməzdi. Bütün Redaksiya Heyəti üzvlərinə jurnala verdikləri töhfələrə görə səmimi-qəlbdən təşəkkür edirəm.

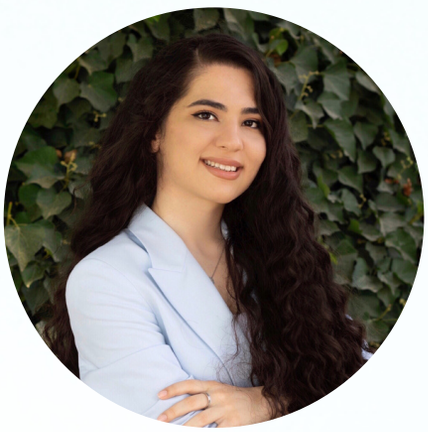
Bütün Redaksiya Heyəti üzvləri və ELSA Azərbaycan Milli İdarə Heyəti adından isə jurnalın Akademik rəyçilərinə dərin minnətdarlığımızı bildirirəm. Məqalələrə rəy verilməsi və seçilməsi prosesini həyata keçirməklə, onların bu buraxılışın akademik keyfiyyətinin yüksəldilməsində çox böyük rolu olmuşdur.

Ümid edirik ki, ELSA Azərbaycan Hüquq Jurnalının bu buraxılışı sizin hüquqda texnologiyanın rolu ilə bağlı daha çox məlumatlı olmağınıza kömək edəcək və onu oxumaqdan bizim onu sizin üçün hazırlamaqdan zövq aldığımız qədər zövq alacaqsınız.

ELSA-nın "İnsan ləyaqətinə və mədəni müxtəlifliyə hörmətin mövcud olduğu ədalətli bir dünya" şüarı ilə estafeti növbəti Redaksiya Heyətlərinə ötürərək, onlara və növbəti buraxılışın müəlliflərinə uğurlar arzulayıram.

Ən xoş arzularla,
Səbinə Zülfiyeva

Editorial



Sabina Zulfiyeva

Editor-in-Chief of ELSA Azerbaijan Law Review and Vice President in charge of Academic Activities of ELSA Azerbaijan 2021/2022

Dear Reader,

It is with great pleasure that I present to you the 5th edition of the ELSA Azerbaijan Law Review.

Through International Focus Programme, the ELSA Network focuses on the interplay between law and technology. Therefore, we decided to publish this edition on a specific topic.

With this in mind, we are grateful for the articles we received, written by graduates and undergraduates on "Law and Technology". In this edition, the best 4 articles were selected and published. I wholeheartedly congratulate the authors whose articles have been selected and encourage other students and professional lawyers to write and send articles for the upcoming editions.

This edition also includes interviews with legal technology professionals from Azerbaijan and different countries of the world. I would like to thank all of our interviewees for accepting our invitation about sharing their experiences with our readers.

As with every publication, the ELSA Azerbaijan Law Review would not be realised without the support of certain individuals. First and foremost, I would like to sincerely thank the whole Editorial Board for their dedication and hard work. They were invaluable in carrying out the publication of this edition of the ELSA Azerbaijan Law Review.

On behalf of the whole Editorial Board and ELSA Azerbaijan, we would like to express our gratitude to our Academic Reviewers. By undertaking the review and selection process of the articles, their academic contribution helped ensure the high academic quality of the publication.

We hope the ELSA Azerbaijan Law Review will assist you in becoming more interested and informed about legal technology and that you enjoy reading this edition as much as we enjoyed putting it together for you.

I wish the greatest of success to the Editorial Boards and authors of the future as we pass the baton, bolstered in our commitment to the vision of ELSA: "A just world which there is respect for human dignity and cultural diversity".

Best wishes,
Sabina Zulfiyeva

Table of Contents

Articles

Interviews

Dr. Veronika Haberler MAS, MLS

Dr. Veronika Haberler, MAS, MLS, has been a leading innovator in the field of European legal technology since she co-founded the Austrian start up LeReTo in 2014. Haberler, a doctor of sociology with a master degree in legal studies, won a Women of Legal Tech Award in 2018 and was shortlisted for the Digital Female Leaders Award in 2020. She published scientific research on how the Austrian Supreme Court comes to its judgements and is also co-editor of the first Austrian, as well as German, legal tech legal law collection (besides Univ-Prof Dr Nikolaus Forgó and Markus Hartung, published by facultas). Dr. Haberleris a sought-after speaker at conferences across Europe. She develops, together with her team at LeReTo, new and innovative ways to bring law, data and users together, forging new paths and creating new technologies for new ways of working.

Hello, Veronika. Thank you for accepting our interview offer.

Hello to you, too, and thanks for having me. I am ready to start, if you are.

What is open data? First and foremost, we would want to hear your perspectives on open data and how it can affect future developments in legal technology. What is the value of open data and how can it help people get access to the justice system?

As you probably know, the term "open data" was first used by NASA in the 1970s to foster a policy for the international use of US satellites. The concept itself, namely that data should be made public, to be used freely for science and education, was already promoted in the 1950s. Already at that time, people recognized that it was necessary to standardize metadata in order to allow interoperability.

Today, analysts assess the global economic value of open data at approximately EUR 50 billion per year. I personally think the value must be significantly larger, though. Let's bear in mind that open data and open data use cases strongly contribute to political and judicial transparency for decades. Transparency is necessary for all democratic processes, as it allows participation, namely informed participation.

For the judicial system, it was one of the core achievements of the French Revolution 1789 that courts and judges are no longer holding their hearings and passing their decisions behind closed doors. Also, that reasons for decision must be stated, which allows – generally speaking – an appeal or otherwise control or supervision of this state authority. That way, transparency can also be seen as a quality guarantee. And today, accessible data on how courts decide certain matters will make a lawsuit more predictable for people.

Before utilizing open data, what considerations about the data's quality should you make?

The primary concern should, in my opinion, rather be: Are the desired data available at all? My country, Austria, is a real pioneer with public legal data as since 1997, court decisions (in a structured data quality) are made available to the public for free. That means almost all Supreme Court, Constitutional Court, Supreme Administrative Court decisions, but also lots of second instance courts'

decisions, all federal and provincial laws back to the year 1780, hundred thousands of enactments, directives, etc. But sadly, this is not at all the case in other countries and even Austria could do better.
Quality concerns are, compared to the availability, of secondary concern, because when data are accessible, to work and interpret it, means to also consider possibly awkward quality problems there may be. And of course, there can be such. Mostly data scientists struggle with missing values or a lack of consistency in data coding schemes.
Typically, the most relevant elements of a first instance decision would not be a super-scientific legal assessment, but rather precise fact findings. And those would, again typically, contain several elements that are personal data and that might be hard to scrape without affecting the data quality. And here we have the drawback already, namely that proper anonymization of complex multi-lateral personal data is a huge challenge. I sense there is still a lot of work to be done here.

Do you believe that there is a possibility that open data might be abused? If so, how should it be protected or regulated by the law?

There is a possibility of an evil use case with everything or almost everything. You can take an innocent YouTube chemistry course and probably figure out how to build explosives with it. When it comes to open data from the legal domain, there are especially sensitive areas. Just to mention criminal prediction algorithms that can perpetuate bias and discrimination. Another example would be the possible infringement of other fundamental rights by data that are accessible too easily and without any restrictions. Is it really in the best interest of all of us if you could stream every divorce proceeding 24/7 and post about it in real time on social media? So, we need to have mindful approaches that allow keeping in balance the fundamental rights of public court hearings, the data collection and their documentation, and an individual's right to be forgotten. Or think of the protection of business secrets, the protection of private life, and so on.

Now the point is data protection, so we are interested in hearing your perspectives concerning the General Data Protection Regulation (GDPR) and the role it plays in the context of data protection.

For the EU, namely for the integrity of Europe's businesses and the protection of citizens, the GDPR was an enormous step forward. I am a big supporter of standardized rules for important matters, and even would welcome a joint tax and fiscal policy. And I believe that the importance of an honest and transparent way of collecting people's personal data has in the meantime become clear for most. But the way in which the actual implementation was made by many, like drafting lengthy standardized data protection declarations that are, to be frank, illegible, appears not to be true to the idea behind it.
As for most matters, individual decisions will be made by local and supranational courts, leading to a more precise idea of how to do it. In that context, I think the role that data protection activists like Max Schrems have played, cannot be emphasized enough.

For lawyers, how might automation and artificial intelligence make open data possible and useful?

Automation is a process that does not necessarily be an IT project. It means scrutinizing your own workflows and procedures, and analyzing what can be made either more efficient or more effective. Of course, where automation potential has been discovered, that's where legal tech tools come into play. There is a broad variety of what can be done open data in that connection! We at LeReTo, a legal tech company that I co-founded in 2014, started with narrow AI analysis of texts to auto-link citations, starting with publicly available open data databases. Later, we went into legal network (citation) analysis, subject matter identification and other advanced

applications, like dictionaries integration, semantic deep searches, similarity comparison, etc. The possibilities are endless, really. Our tool was developed together with a team of litigators, so we could go for user-centered design right from the start.
What tool can be useful for what kind of legal practitioner, of course, depends on the individual requirements. I know that's a typical lawyer's answer, but so true: who writes hundreds of very similar contracts a year has other requirements than a practitioner who does thousands of, for example, air passenger rights cases.

Innovative solutions may be developed in tandem when data are more openly available for usage and analysis by legal aid groups, attorneys, and legal technology businesses to analyze. Open data for legal technology advancements has various advantages. Do you believe there are any drawbacks to this strategy?

I think the opportunities outnumber the potential threats by far. Open data, especially legal open data, needs to be safe for the data subjects, of course, which is why court decisions are typically only published and made accessible in an anonymized form. That can be a true challenge. For example, for proper machine learning, let's say we need at least 500, better 1000, comparable first instance decisions.

How has technology impacted the law from the past to the present time? From your perspective, what are the most important alterations?

There are two arguments that come to mind. One is that with the concepts of historic Roman law, most European legal phenomena can be fully understood, apprehended and applied. Austria's Civil Code, for example, comes from 1813 and were there no special rules for today's technology, a good lawyer could plausibly cover all requirements by analogy. Another matter is public law, regulatory rules. Just think about the recent discussions on how to prevent the circumvention of sanctions with cryptocurrencies and how to discourage people from investing into blockchain apps that are perceived as damaging the environment. Or think about the supply chain rules coming into force in 2023. Without a globalized and digital world, neither would there be such norms, nor could they ever be implemented. To sum it up, the effect of tech on law is enormous, but that's also valid the other way, with all the gov tech/legal tech/regulatory tech, etc. apps.

To help our readers have a better understanding of legal technology, we'd love to hear your suggestions.

Legal tech is here not to replace legal professionals, but to help them do their tasks better, faster, or both. It starts with general basic tech like a secure cloud space for a digital client record. The range goes from if-then-chatbots or automated document management to forensic software, assisting with larger due diligence assignments or claims settlement algorithms. It all has only just begun, but after all, it has actually begun now.
From a consumer's perspective, numerous digital assistants help you make your life easier when there are legal matters that appear too small to go to a lawyer: reclaiming overcharged rent, collecting small insurance claims, reimbursements for flight delays, etc. All of them generate new business that does not harm to the traditional legal sector at all. And all of them contribute to more justice, in the end. And is that not a good thing?

Thank you very much for talking to us today, Veronika!

It was an interesting journey. Thank you for having me, and my best wishes for your projects.

Privacy protection and its possibility on social media

Rahil Mammadov

He is pursuing the second year of master's studies in the European Business Law programme at Lund University, holder of the Swedish Institute Scholarship for Global Professionals, 2020-2022.

Abstract

Social media is an integral part of our daily life. The global digitalization policy, as well as the coronavirus pandemic, have particularly accelerated the process of social media penetration into our personal space. With the ever-increasing role of social media in our lives, privacy is becoming a tool for both social media representatives and third parties who are able to acquire information from various social media platforms. Privacy is new within social media and needs more detailed study and regulation. Given the important role of privacy for each social media user, this paper analyzes the concept of privacy, social media and privacy on social media, privacy policy on social media under international and European law, privacy protection and its possibility on social media.

Introduction

In recent years, with the entry into the era of digitalization, the role of the need to regulate privacy on social media has increased. This outcome is clearly influenced by the sudden increase in the role of online platforms, both aimed at social and commercial activities. This paper analyzes privacy on social media from different legal aspects by considering the theoretical and practical approach, and influential court decisions, moreover, it discusses the possibility and effectiveness of privacy on social media, while considering its positive and negative challenges.

Concept of privacy, social media, and privacy on social media.

Before starting to analyze privacy on social media, privacy and social media should be discussed separately.

Social media platforms are aimed at building the connection between people and help them to connect based on shared interests, political views, or activities.[1] Regardless of gender, race, nationality, language, origin, property and official status, place of residence, attitude to religion, beliefs, and other circumstances, people can freely use social media.

It should be noted that it is rather difficult to define the concept of privacy, as it can vary depending on different foundations of society and regulation methods in different countries. As the most generally accepted definition, it can be noted that privacy is the right to make certain fundamental decisions concerning deeply personal matters free from government coercion, intimidation, or regulation.[2] What is more, privacy was characterized by the Supreme Court of the United States as the individual's "right to be left alone".[3] Thus, privacy is individual in nature and depends on the specific perception of the individual, which may differ in connection with religion, generally accepted norms and customs in a particular society, etc.

Privacy on social media can be defined as the level of protection of any personal information that a social media user owns in that social media platform.[4]

[1] Abdullah Abdulabbas Nahi Al-Rabeeah, Faisal Saeed, 'Data Privacy Model for Social Media Platforms', Institute of Electrical and Electronics Engineers (2017): 1

2] privacy. (n.d.) West's Encyclopedia of American Law, edition 2. (2008). Retrieved December 21, 2021 from https://legal-dictionary.thefreedictionary.com/privacy

[3] S. Warren, Brandeis L.D, 'The Right to Privacy', Harvard Law Review 4 (1890): 193

[4] Dae-Hee Kim, Hettche, M. and Clayton, M. J. 'The Privacy Paradox and Calculus Among Millennials: An Empirical Study of Privacy Attitude-Behavior Congruence', AMA Marketing & Public Policy Academic Conference Proceedings, (2015). Retrieved December 23, 2021 from https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=119960827&site=eds-live&scope=site

Such personal information may be covered by the laws of the country where the social media user is active or residing. This controversy is again related to the recent rise in the role of privacy on social media.

Statistics show that about 50% of those surveyed keep their social media accounts in private mode, whereas the remaining half choose to use them publicly.[5] This survey also showed that 71% of those surveyed had detailed the privacy policy of the social media platform and took steps to set specific privacy settings.[6] This statistical information shows how people are aware of the need to consider privacy policies and applying appropriate measures.

According to the proposed theories, privacy on social media can be divided into two types. These are issues caused by the data holders and caused by others. An example of the issues caused by data holder may be posting a personal photo publicly on a social network without reading the privacy policy and harming one's own privacy by arranging media of oneself with insufficient safety or deliberation.[7] Expanding danger to privacy protection comes from other media sources posted by social media users. The amount of information that has been posted is massive and cannot be overseen or sorted physically. Users cannot even see and understand how far the scope of one's private information is spread.[8] This theory partially covers the subjects of privacy on social media, which makes it possible further to analyze the possibility of privacy on social media.

Privacy policy on social media under international and European law.

Having considered privacy from a theoretical and partly empirical point of view, it is important to briefly consider its regulation in various legal systems, especially in the framework of international and European law.

A right to privacy has been recognised by many countries and nowadays the number of such countries is rising. The right to privacy is protected under Article 12 of the Universal Declaration of Human Rights, which provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation".[9] This provision does not play a significant role from a practical point of view, that is, it is not covered by a strict enforcement and protection mechanism.

The right to privacy is also established in Article 8 of the European Convention on Human Rights, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence".[10] The European Court of Human Rights (ECHR) said that "the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press."[11] The ECHR also states that "notwithstanding therefore the significant development of the Internet and social media in recent years, there is no evidence of a sufficiently serious shift in the respective influences of the new and of the broadcast media (...) to undermine the need for special measures for the latter."[12]

[5] Peter Suciu, 'There Isn't Enough Privacy On Social Media And That Is A Real Problem', Forbes. (2020). Retrieved December 23, 2021 from https://www.forbes.com/sites/petersuciu/2020/06/26/there-isnt-enough-privacy-on-social-media-and-that-is-a-real-problem/?sh=37eed1b344f1

[6] Ibid

[7] Rainie, L., Smith, A., Schlozman, K. L., Brady, H., & Verba, S., 'Social media and political engagement', Pew Internet & American Life Project, (2012): 19

[8] Ibid, 19

[9] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12

[10] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8

[11] Editorial Board of Pravoye Delo and Shtekel v. Ukraine, no. 33014/05, 5 May 2011, para 63

[12] Animal Defenders International v. the United Kingdom [GC], no. 48876/08, ECHR 2013, para 119

This differing position of the ECHR leads to the conclusion that, within the framework of the protection of human rights, privacy on social media cannot be clearly established as it relies on the interpretation of the ECHR depending on the legal framework of the Member States.

The General Data Protection Regulation (GDPR) is considered as the most effective and clearly compiled legal act which regulates privacy and security law in the European Union (EU).[13] However, the practice of the European Court of Justice (ECJ) has significantly influenced the regulation of the right to privacy within the EU, providing for non-EU countries the need to regulate the law in accordance with the provisions of the GDPR even outside the EU.

In Schrems I case, the complaint was pointed at restricting Facebook from further exchanging information from Ireland to the United States, given the alleged involvement of Facebook USA in the PRISM mass surveillance program.[14] The ECJ ruled that companies moving personal user data from the EU to other jurisdictions will have to provide the same protections given inside the Union.[15] In Schrems II's judgment, the CJEU declared the Privacy Shield Decision of the European Commission invalid on account of invasive US surveillance programmes, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal.[16] These decisions of the ECJ play an essential role in strengthening the protection of the right to privacy and have shown the importance of EU policy in the field of regulation and protection of this right.

Thus, the EU was able to create a strict and serious format for protecting the right to privacy, as well as its mechanism, which, over time, began to spread throughout the world.

Privacy protection and its possibility on social media.

Privacy protection can be ensured by various types of actions, such as identity theft, surveillance, unintentional fame, stalking, etc. With the development of online platforms and their increasing role in everyday life, it becomes difficult to identify new causes of privacy violations on social media.

To protect privacy on social media, rights within that platform and analyzing the privacy policy of the social media platform should be taken into account. In addition, it is important to determine whether the actions on social media are public or have access to persons restricted by the subject. However, many examples can be cited when it is quite difficult to preserve personal data, which casts doubt on even the effectiveness of the current legal regulation in this area. One such example is the possibility of acquiring personal data online by any third party about any person residing in Sweden and having a social security number. This website, called “hitta/se”, is operated by the state and provides an opportunity for anyone to get information about one’s residence, mobile number, and other personal information by writing the name and surname of that person.

Therefore, it is necessary to take into account both the practical and legal consequences of actions of data privacy holders in the framework of social media. In addition, it is important to adopt the practice of different countries, especially the EU Member States, in the field of privacy regulation and establish its common boundaries.

[13] GDPR, ‘What is GDPR, the EU’s new data protection law?’, Retrieved December 24, 2021 from https://gdpr.eu/what-is-gdpr/

[14] Columbia University Global Freedom of Expression, ‘Schrems v. Data Protection Commissioner’. (2021) Retrieved December 24, 2021 from https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/

[15] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] C:2015:650

[16] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] C:2020:559

Conclusion.

Privacy is still new in social media platforms since the growth happening of that sector which needs more attention and guidelines.[17]

The analyzed legal acts and practical issues give a basis to believe that privacy is still possible on social media, however, given certain mistakes in the regulatory area, it is important to strengthen control and establish the limits of the application of privacy on social media.

Bibliography

Books and articles:

1. Abdullah Abdulabbas Nahi Al-Rabeeah, Faisal Saeed, 'Data Privacy Model for Social Media Platforms', Institute of Electrical and Electronics Engineers (2017)
2. S. Warren, Brandeis L.D, 'The Right to Privacy', Harvard Law Review 4 (1890)
3. Dae-Hee Kim, Hettche, M. and Clayton, M. J. 'The Privacy Paradox and Calculus Among Millennials: An Empirical Study of Privacy Attitude-Behavior Congruence', AMA Marketing & Public Policy Academic Conference Proceedings, (2015). Retrieved December 23, 2021 from https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=119960827&site=eds-live&scope=site
4. Peter Suciu, 'There Isn't Enough Privacy On Social Media And That Is A Real Problem', Forbes. (2020). Retrieved December 23, 2021 from https://www.forbes.com/sites/petersuciu/2020/06/26/there-isnt-enough-privacy-on-social-media-and-that-is-a-real-problem/?sh=37eed1b344f1
5. Rainie, L., Smith, A., Schlozman, K. L., Brady, H., & Verba, S., 'Social media and political engagement', Pew Internet & American Life Project, (2012)

Legal acts and cases:

1. Animal Defenders International v. the United Kingdom, no. 48876/08, ECHR 2013
2. Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] C:2020:559
3. Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] C:2015:650
4. Editorial Board of Pravoye Delo and Shtekel v. Ukraine, no. 33014/05, ECHR 2011
5. Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)
6. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

Internet sources:

1. Columbia University Global Freedom of Expression, 'Schrems v. Data Protection Commissioner'. (2021) Retrieved December 24, 2021 from https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/
2. GDPR, 'What is GDPR, the EU's new data protection law?', Retrieved December 24, 2021 from https://gdpr.eu/what-is-gdpr/
3. Privacy. (n.d.) West's Encyclopedia of American Law, edition 2. (2008). Retrieved December 21, 2021 from https://legal-dictionary.thefreedictionary.com/privacy

[17] Al-Rabeeah, Saeed (n 1) p. 5

Fariz Cəfərov

Fariz Cəfərov Azərbaycan Respublikasının Prezidenti yanında Vətəndaşlara Xidmət və Sosial İnnovasiyalar üzrə Dövlət Agentliyinin (ASAN Xidmət) tabeliyində fəaliyyət göstərən "Elektron Hökumətin İnkişafı Mərkəzi" publik hüquqi şəxsin direktoru vəzifəsində çalışır. Təhsil və peşəkar təcrübəsindən irəli gələrək, o, myGov, ASAN Bridge, ASAN Ödəniş, ASAN Viza kimi 50-dən çox ümummilli dövlət xidmətləri layihəsinin ərsəyə gətirilməsində iştirak etmiş və dövlət xidmətlərinin göstərilməsinə yenilik gətirmək üçün qabaqcıl beynəlxalq təcrübələrin tətbiqinə təşəbbüs göstərmişdir.
2021-2022-ci illər üçün Avropa Komissiyası tərəfindən maliyyələşdirilən və texnologiya sahəsində dörd aparıcı Avropa universiteti (Madrid Texniki Universiteti, Milan Texniki Universiteti, Tallin Texniki Universiteti və Erlanqen-Nürnberq Universiteti) tərəfindən dəstəklənən "Dövlət Xidmətləri üçün Süni İntellekt" magistr (AI4Gov) proqramının ilk iştirakçılarından biridir.
Bundan əlavə, Fariz Cəfərov, Corc Vaşinqton Universitetinin Layihə idarəetməsi, Duke Universitetinin Adaptiv Strategiyanın İdarə Edilməsi sahələri üzrə magistr sertifikatlarının, eləcə də İT xidmətlərinin idarə edilməsi üzrə beynəlxalq səviyyədə tanınmış "ITIL Foundation" sertifikatının sahibidir.

Hörmətli Fariz bəy, müsahibə təklifimizi qəbul etdiyiniz və dəyərli vaxtınızı ayırdığınız üçün təşəkkür edirik.

Müsahibə üçün mən də sizə öz təşəkkürümü bildirirəm.

Oxucularımızın Sizi daha yaxından tanıması üçün hazırkı fəaliyyətiniz haqqında qısa məlumat verə bilərsiniz?

2013-cü ildən Azərbaycan Respublikasının Prezidenti yanında Vətəndaşlara Xidmət və Sosial İnnovasiyalar üzrə Dövlət Agentliyinin (ASAN Xidmət) müxtəlif strukturlarında çalışmışam. 2018-ci ildən isə Dövlət Agentliyinin tabeliyində fəaliyyət göstərən Elektron Hökumətin İnkişafı Mərkəzinin (EHİM) direktoru olaraq çalışıram. Paralel olaraq müxtəlif vaxtlarda fərqli universitetlərdə tədrislə məşğul olmuşam. Hazırda ADA Universitetində Elektron Hökumət üzrə Dövlət İdarəçiliyi fənnini tədris edirəm.
EHİM olaraq isə ölkədə dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, inteqrasiyası, yeni rəqəmsal layihələrin yaradılması, elektron dövlət xidmətlərinin göstərilməsi işlərilə məşğuluq. Mərkəz müasir informasiya texnologiyalarından istifadə etməklə dövlət qurumları tərəfindən bütün vətəndaşlara e-xidmətlərin göstərilməsini təmin edir.

2022-ci il ərzində Elektron Hökumətin İnkişafı Mərkəzi hansı layihələri həyata keçirmişdir və keçirməyi planlaşdırır?

2022-ci il layihələrin inkişafı və yeni layihələrin formalaşması nöqteyi-nəzərindən olduqca produktiv ildir. Bu ilin mart ayından etibarən Rəqəmsal icra hakimiyyəti - rih.gov.az portalı bütün respublikanı əhatə etməyə başladı. Hazırda rih.gov.az portalı Bakı və regionlar da daxil olmaqla 77 yerli icra hakimiyyətini əhatə edir. Layihə icra hakimiyyətlərində qərar qəbuletmə üzrə çevikliyin artırılması, rəqəmsal savadlılıq səviyyəsinin yüksəldilməsi, vahid məkandan xidmətlərə çıxışın təmin edilməsi, vətəndaşların vaxtına qənaət edilməsi, müraciət prosesinin asanlaşdırılması, habelə

yerli icra hakimiyyətlərinin fəaliyyətində çeviklik və səmərəliliyin təmin edilməsi məqsədilə yaradılıb.

Öz mütəxəssislərimiz tərəfindən yaradılan "ASAN Bridge" Milli Məlumat Mübadiləsi Sistemi vasitəsilə qurumlara 2022-ci il ərzində 181 milyondan çox məlumat ötürülüb. Bura 50 qurumun 92 sistemi inteqrasiya edilib. Hələ neçə-neçə inteqrasiya üzərində iş gedir. Bu, yenicə yaranmış sistem üçün böyük uğurdur.

Bu il həmçinin, qurum və şirkətlərin mövcud və ya yarana biləcək təhlükə, eləcə də risklərdən qorunması məqsədilə onların əməkdaşlarına kibertəhlükəsizlik davranış testlərini və maarifləndirmə tədbirləri, təlimləri özündə ehtiva edən "Kibergigiyena" platformasının tətbiq edilməsi ilə yadda qaldı.

EHİM bu il Şamaxı rayonunda əməkdaşlarının innovasiya yönümlü potensiallarının aşkarlanması, əməkdaşlar arasında komanda ruhu və quruculuğu, ideya formalaşdırma bacarıqlarının inkişaf etdirilməsi məqsədilə çox uğurlu "DIGITAL IDEA CAMP – Govtech həlləri" adlı hakaton keçirdi.

Bununla yanaşı, 2022-ci ildə EHİM tərəfindən ölkəmiz üçün çox böyük mənəvi əhəmiyyət daşıyan "Yolumuz Qarabağa" portalı texniki olaraq ərsəyə gətirildi. Bu gün portalın dayanıqlılığı, mütəmadi olaraq sisteminin təkmilləşdirilməsi işləri Mərkəz tərəfindən aparılır. Bildiyiniz kimi "Yolumuz Qarabağa" layihəsi, Azərbaycan Respublikasının 44 günlük Vətən müharibəsi zamanı işğaldan azad etdiyi ərazilərə səfərlərin təşkilini ehtiva edir.

"myGov" elektron hökumət portalında bu ildən yeni növ arayışlar istifadəyə verilib. Ümumiyyətlə, bir çox qurumlar bu ildən arayışları "myGov" üzərindən vətəndaşlara təqdim edir.

Hal-hazırda Dövlət Şəhərsalma və Arxitektura Komitəsinin icazələrlə bağlı yeni sistemi tərəfimizdən hazırlanır və bu ilin sonunadək sistemin yeni dizaynda istifadəyə verilməsi nəzərdə tutulur.

Həmçinin qeyd etmək istəyirəm ki, "myGov", "ASAN Login", "DXR", "ASAN ödəniş" və e-gov.az portalını özündə birləşdirən vahid dövlət xidmətləri portalının yaradılması planlaşdırılır. Ümumiyyətlə, EHİM tərəfindən idarə olunan bütün layihələrdə yeniliklər vardır.

Həmçinin qeyd etmək istərdim ki, cari ildən EHİM dövlət xidmətlərinin dizaynı, sadələşdirilməsi istiqamətində bu sahədə böyük nüfuzu olan Böyük Britaniya, Sinqapur və Kanada kimi ölkələrin aidiyyatı qurumları ilə çox sıx əməkdaşlıq edir, qarşılıqlı təcrübə mübadilələri aparır. Bu, elektron dövlət xidmətlərinin standartlarının formalaşmasına öz böyük töhfəsini verir.

Fiziki və hüquqi şəxslər "Elektron hökumət" (www.e-gov.az) portalından nə üçün istifadə etməlidirlər? Bu portal onlara hansı üstünlükləri təqdim edir?

e-gov.az portalında hazırda 37 qurum tərəfindən elektron xidmətlər göstərilir. Portalın istifadəçi sayı 1 milyon 400 minə yaxındır. Portal dövlət qurumları tərəfindən göstərilən elektron xidmətləri vahid məkanda birləşdirərək vətəndaşlara 7/24 xidmət göstərir. Yəni elektron xidmətlər zaman və məkan anlayışını yox edir. İndiki zamanda hər birimiz üçün çox önəmli olan vaxta qənaət edərək xidmət almaq üçün əvəzolunmazdır. Portaldan həm fiziki şəxslər, həm də hüquqi şəxslər onlara lazım ola biləcək xidmətlərdən yararlana bilirlər.

Qeyd edim ki, e-gov.az portalına artıq "ASAN Login" ilə də daxil olmaq mümkündür və şəxsi kabinetdən "myGov"a birbaşa keçid imkanı təmin edilib. Artıq istifadəçilər bir kliklə portal vasitəsilə qurumlar tərəfindən təqdim edilən informativ və interaktiv xidmətlərlə yanaşı "myGov"dakı şəxsi məlumatlarına və buradakı arayış və digər xidmətlərə keçid edə bilirlər.

Yaxın zamanlarda elektron sənədlərin hüquqi qüvvəyə minməsindən sonra isə kağız sənədlərin dövriyyədən çıxması, istənilən yerə istənilən nöqtədən sənədlərin elektron təqdim olunması, heç bir sənədin fiziki şəkildə daşınmaması artıq bizi daha üst səviyyə rəqəmsallaşmağa aparacaq.

Vətəndaşlara təqdim olunan elektron xidmətlər ilə bağlı onların narazılıq və şikayətləri adətən nələr ilə bağlı olur? Bu halların aradan qaldırılması üçün hansı təkmilləşdirilmələr aparılır?

Müasir dövrdə texnologiyanın sürətli inkişafı istifadəçilərin rahatlığını təmin etmək, zamanın tələbinə uyğunlaşmaq kimi istəkləri daha da artırır. Belə bir dövrdə ən böyük tələb müasir texnologiyalardan istifadə etməklə vətəndaşların xidmətlərə daha əlçatan olmasını təmin etməkdir.
Biz EHİM olaraq daim vətəndaşların fikir və təkliflərini müxtəlif üsullarla öyrənməkdə maraqlıyıq. Bunun üçün istər onlayn, istərsə də fiziki olaraq sorğular keçirilir, "108" Çağrı Mərkəzindən gələn sorğular, EHİM-in bütün sosial media hesablarından daxil olan vətəndaş müraciətləri, e-poçt ünvanı və rəsmi məktub vasitəsilə daxil olan bütün sorğu və müraciətlər mütəmadi olaraq araşdırılır və nəzərə alınır. Biz daim vətəndaşların narahat olduğu mövzuları müəyyən edərək analiz edir və bütün bunlar əsasında təkmilləşdirmə işləri aparırıq. Biz bütün şikayətlərə imkan kimi baxırıq, çünki məhz onları araşdırarkən yeni fikir və ideyalar əmələ gəlir. Məsələn, "ASAN Login" sistemində yaradılan videoqeydiyyat buna misal ola bilər. Əvvəllər sistemində qeydiyyat yalnız vətəndaşın öz adına olan mobil nömrə və şəxsiyyət vəsiqəsinin FİN-i ilə mümkün idi. Vətəndaşlardan, xüsusən də xanımlardan bu istiqamətdə qeydiyyatdan keçmədə çətinliklərlə bağlı müraciətlər alırdıq. Müəyyən olurdu ki, bir çox vətəndaşların istifadə etdikləri mobil nömrə öz adlarına deyil və bu səbəblə də "ASAN Login"də qeydiyyatdan keçə bilmirlər. Bu tipdə çoxsaylı müraciətləri təhlil etdikdən sonra "ASAN Login" sistemində video ilə qeydiyyat imkanı yaratdıq və vətəndaşlara təqdim etdik. Artıq sistemdə qeydiyyatdan keçən zaman vətəndaşlardan mobil nömrənin öz adına olması tələb olunmur. Daha müasir üztanıma texnologiyası ilə qeydiyyatdan keçə bilirlər. Yəni təqdim etdiyimiz layihələrdə vətəndaşların fikirləri ("e-participation") və istifadə rahatlığı ("user-friendly"), təklifləri nəzərə alınır. Çünki işimiz vətəndaşlara xidmət göstərmək, onların işini asanlaşdırmaqdır.
Bundan başqa biz məşhur portalları, sosial şəbəkələri izləyib onların funksionallıqlarını və insanlara verdiyi istifadəçi rahatlığı konsepsiyalarını öz portallarımızda vətəndaşlara təqdim edirik. Məsələn, səs vasitəsilə şikayətin göndərilməsi, notifikasiyaların vətəndaşların öyrəşdiyi dizayn və yerdə yerləşdirilməsi, portalın rəng seçimi və s. buna misal ola bilər.

Bir çox hallarda dövlət qurumları tərəfindən vətəndaşların elektron qaydada təqdim etdiyi sənədlərin notariat qaydasında təsdiq edilmiş kağız daşıyıcılarda da təqdim olunması tələb olunur. Sizcə, sənədləşmə işlərində tam elektronlaşma prosesi nə zaman başa çatacaq?

Ümumiyyətlə, elektron hökumət quruculuğu böyük bir ekosistemdir. Bura rəqəmsal identifikasiya, şəbəkə infrastrukturu, vətəndaşların iştirakı, normativ hüquqi baza, qurumların sağlam və dayanıqlı sistemlərinin olması və s. kimi 12 komponent daxildir. Bütöv ekosistemin mövcud olması üçün hər bir komponentin inkişafı olduqca vacibdir.
Hal-hazırda "ASAN Bridge"-dən dövlət qurumlarına birbaşa məlumatlar ötürüldüyünə görə artıq növbəti mərhələlərdə kağız sənədlər tamamilə aradan qaldırılacaq və data əsaslı idarətetmə modeli tətbiq olunacaq.
Rəqəmsal keçid dövrünü yaşayan Azərbaycanda "myGov" üzərindən verilən arayışların dövlət və özəl sektorda tanınması üçün qanunvericiliyə dəyişikliklə bağlı təşəbbüslər də edilib, yaxın zamanda bu istiqamətdə də yeniliklərin olması gözlənilir. Bu məsələlər öz həllini tapdıqdan sonra bu istiqamətdə daha yaxşı nəticələr əldə etməyimiz mümkün olacaq.
Bu gün bütün dünyada qanunvericiliyə dəyişikliklərin

olunması texnologiyanın inkişafından daha aşağı sürətlə gedir. EHİM olaraq biz rəqəmsallaşma istiqamətində pilot layihələr edir, texniki tərəfdən layihə və xidmətləri mümkün və istifadəyə yararlı etdikdən sonra praktiki cəhətdən hüquqi əsasının təmin edilməsi üçün təkliflər veririk.

Rəqəmsallaşmanın sürətlənməsi, texnologiyanın inkişafı fonunda kiber hücumlar da gündən-günə artmaqdadır. Bu hücumlardan qorunmaq üçün məlumatların təhlükəsizliyinin təmin edilməsi istiqamətində hansı yeniliklərdən istifadə olunur?

Bilirsiniz ki, qlobal mühitdə texnologiya inkişaf etdikcə, bütün həyat hadisələri rəqəmsallaşmağa başlayıb. Bu cür sürətli rəqəmsal transformasiya zamanı, təbii ki, kibertəhdidlərin də artma sürəti yüksəkdir. Artıq ölkəmizdə də bu məsələlərə həssas yanaşılmağa başlanılıb. Müvafiq olaraq dövlət tərəfindən də aidiyyatı tədbirlər görülür.
EHİM olaraq biz də məlumatların qorunmasına çox həssas yanaşırıq. Məsələn, qurum olaraq məlumatların şifrələnərək göndərilməsinə, saxlanılmasına ciddi önəm verilir və "log"lara daim nəzarət olunur.
İcazəsiz istifadəçilərin həssas məlumatlara daxil olmasının qarşısını almaq üçün düzgün istifadəçi identifikasiyası üsullarına malik olmaq lazımdır. Ancaq tək güclü şifrələrin olması kifayət deyil. Ən təhlükəsiz üsullar - biometrika, daxili iki faktorlu autentifikasiya üsullarına önəm verilməlidir.
EHİM tərəfindən kritik infrastrukturlarda həssas məlumatların qorunması üçün qurulmuş sistemlərə daimi nəzarət edilir. Sistemlər hər biri fərqli zonalarda və serverlərdə saxlanılır, ehtiyat üçün arxiv planları qurulur, bütün məlumatların saxlandığı sistemlər və arxivlərin ehtiyat nüsxələri alınır. Fərdi məlumatların saxlanmasında beynəlxalq standartlar tətbiq olunur. Təhlükəsizlik nəzarətləri - informasiya təhlükəsizliyi üzrə beynəlxalq standart, ödəniş sistemlərində məlumatların təhlükəsizliyi standartı, GDPR (ümumi məlumatların qorunması haqqında qanun) standartı tətbiq olunur.

Kibertəhlükəsizlik sahəsində vətəndaşların fərqinə varmadığı, doğru bildikləri yanlışlar nələrdir? Onlar kiber hücumlardan müdafiə olunmaq üçün onlar nələrə diqqət etməli, hansı qabaqlayıcı tədbirləri görməlidirlər?

2022-ci ilin statistikasına əsasən internet mühitdə hər 39-cu saniyədə kiberhücum baş verir. İstifadə etdiyimiz elektron poçt ünvanları 94% virus hücumlarını özündə ehtiva edir. Məlumat sızıntısının əsas səbəblərindən biri isə kibertəhlükəsizlik haqda məlumatsız olan insanlardır. Bu gün insanların sosial şəbəkələrdə öz fərdi məlumatlarını, eləcə də günlük həyat hadisələrini açıq şəkildə paylaşması, mənbəyi məlum olmayan linklərdə öz məlumatlarını daxil etməsi və sair kimi artıq bir çoxları tərəfindən norma qəbul edilən və ya vərdiş edilən fəaliyyət əslində kibertəhlükəsizlik nöqteyi-nəzərdən çox yanlış addımlardır.
Tanımadığınız mənbədən gələn hər bir link, sizə verilmiş olan fləş kartlar, "crack" proqramların yüklənilməsi, bunlar hər biri təhlükə mənbəyidir. İnsanları aldadaraq məlumat oğurlama üsulları arasında ən geniş yayılmış metod bildiyiniz kimi fişinqdir. Fişinq hücumlarının əsas məqsədi insanlara müəyyən linklər göndərməklə onları saxta, lakin real veb səhifəyə bənzər səhifələrə yönləndirmək, hesab məlumatlarının həmin saxta səhifəyə daxil etməsini təmin etməkdir. Bu üsulla qarşı tərəf hesab məlumatlarını çox asanlıqla ələ keçirə və istifadəçinin xəbəri olmadan ondan istifadə edə bilər. Bu kimi hallarla qarşılaşmamaq, məlumat sızıntısının qarşısını almaq üçün vətəndaşların mütəmadi olaraq kibergigiyena sahəsində maarifləndirilməsinə ehtiyac var. Biz mütəmadi sosial şəbəkələrimizdə, eləcə də EHİM-in təqdimatında "ASAN Radio"da yayımlanan "Rəqəmsal Azərbaycan" verilişində bu barədə vətəndaşlarımızı maarifləndirir və ekspertləri dəvət edərək tövsiyələr veririk.

Ölkəmizdə "Kiber Gigiyana" sahəsində vətəndaşlar arasında, eləcə də dövlət və özəl təşkilatlarda, təhsil müəssisələrində mövcud vəziyyətin təhlili istiqamətində hansı tədbirlər görülür və görülməsi planlaşdırılır?

Rəqəmsal transformasiya və texnoloji inkişaf dövlət və özəl sektor əməkdaşlarının kibertəhlükəsizlik tədbirlərinə daha həssas yanaşmasını tələb edir. Ölkəmizdə kibergigiyena sahəsində mühüm addımlar atılmaqdadır.

EHİM, Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti və "B.EST Solutions" şirkəti tərəfindən kibergigiyena üzrə əməkdaşlıq platformasının yaradılmasına dair əməkdaşlıq müqaviləsi imzalanıb. Müqavilə müvafiq platformanın istifadəsi, idarə edilməsi, informasiya təhlükəsizliyinin təşviqi və müvafiq təbliğat işlərinin aparılmasını əhatə edir.

Məlumatların qorunması və informasiya təhlükəsizliyinin təmin edilməsi zəruri avadanlıqlarla yanaşı, həm də internet və məlumatlardan istifadə zamanı təhlükəsizlik qaydalarına riayət edilməsini zəruri edir.

Əməkdaşlıq çərçivəsində qurum və şirkətlərin mövcud və ya yarana biləcək təhlükə, eləcə də risklərdən qorunması məqsədilə kibertəhlükəsizlik haqqında maarifləndirmə tədbirlərinin və təlimlərin keçirilməsi nəzərdə tutulub. Layihənin icrası çərçivəsində qurum və şirkətlərin əməkdaşlarının kiberhücum nümunələri əsasında hazırlanmış simulyasiya testlərinə yanaşmaları və hazırlıqları müəyyən ediləcək. Təlim və testlər NATO tərəfindən mükafatlandırılmış Estoniyanın kibertəhlükəsizlik şirkəti – "CybExer"in proqram təminatı vasitəsilə həyata keçirilməsi nəzərdə tutulub.

Həmçinin, vətəndaşlar da kibergigiyena.az portalına daxil olaraq "Özünü sına" bölməsindən öz kibergigiyena biliklərini yoxlaya bilərlər.

Layihə və testlər "Teknofest"dəki stendimizdə də vətəndaşlar tərəfindən böyük maraqla qarşılandı. Onlar monitorda öz biliklərini yoxlayaraq elə yerindəcə nəticəsi ilə tanış olurdular.

Biz öz əməkdaşlarımızın da bu istiqamətdə ayıq-sayıqlığını və maariflənməsini təmin etmək üçün addımlar atırıq. Məsələn, EHİM-in İnformasiya təhlükəsizliyi şöbəsi tərəfindən təlimlər keçirilir, kibertəhlükəsizlik sahəsində əməkdaşların davranışlarının yoxlanılması üçün test və nəticələri analiz edilir.

Bəs əhalinin rəqəmsal savadlılığının artırılması istiqamətində regionlarda hansı ictimai maarifləndirmə layihələri həyata keçirilir?

Rəqəmsal savadlılığın artırılması istiqamətində ilkin addımlarımızı Bakı şəhərində atmışıq. Aydın məsələdir ki, paytaxtla bölgələr arasında rəqəmsal savadlılıq baxımdan böyük fərq var. Aradakı bu fərqi azaltmaq, xidmətlərimizin bölgə vətəndaşlarının da istifadəsi üçün ötən ildən müvafiq addımlar atmağa başladıq.

Bölgələrdə rəqəmsal savadlılığı artırmaq üçün EHİM tərəfindən daha öncə Bakıda həyata keçirilən "Rəqəmsal Hökumət" Təşviqat Proqramını Şamaxı şəhərində tətbiq etməyə başladıq. Şəhərin sosial aktiv gənclərindən ibarət böyük auditoriyaya bir neçə günlük təlimlər keçirilib. Paralel olaraq rəqəmsal könüllülər yetişdirilib, könüllülər vətəndaşları maarifləndirməyə hazırlanıb, təlimdən sonra könüllülərin bilikləri yoxlanılıb. Layihənin növbəti mərhələsində isə həmin könüllülər Şamaxıda ASAN xidmətə yaxınlaşan, növbə gözləyən vətəndaşları elektron dövlət xidmətləri, rəqəmsal xidmətlər, mobil tətbiqlər və s. haqqında maarifləndirib. Bu layihənin paralel olaraq digər rayonlarda da keçirilməsi nəzərdə tutulub.

Həmçinin qeyd edim ki, EHİM indiyədək media nümayəndələrinin rəqəmsal savadlılığının artırılması üçün 3 dəfə " Rəqəmsal Jurnalistikaya doğru" layihəsini həyata keçirib. Proqrama bölgələrdən olan media nümayəndələri də qatılıblar. Bu layihə ilə vətəndaşların maarifləndirilməsinə medianın dəstərilə nail olmağa çalışmışıq. Layihə çərçivəsində 100-dən çox jurnalist rəqəmsal maarifləndirmə proqramını uğurla bitirib.

Regionlarda rəqəmsal xidmətlərin inkişafı baxımından ”Rəqəmsal icra hakimiyyəti” layihəsi – rih.gov.az da böyük əhəmiyyət daşıyır. Righ.gov.az portalının ilk tətbiq edildiyi Gəncə şəhərində, Quba və Masallı rayonlarının hər birində sosial aktiv vətəndaşlara, eləcə də seçilmiş könüllülərə xidmətlərdən istifadə ilə bağlı təlimlər keçirilib. Vətəndaşları maarifləndirmək üçün rəqəmsal könüllülər hazırlanıb. 2022-ci ilin yanvar ayından etibarən fəaliyyətə başlayan könüllülər hər 3 bölgədə ASAN xidmətə yaxınlaşan, növbə gözləyən vətəndaşları portalın funksionallıqları, qeydiyyatdan keçmə və xidmətlərə müraciətlə bağlı vətəndaşları maarifləndiriblər. Ümumilikdə isə könüllülər vasitəsilə 2022-ci ilin yanvar ayından bu günədək həmin bölgələrdə 20000-ə yaxın vətəndaş maarifləndirilib.
Qarşıda bu istiqamətdə yeni layihələrimiz olacaq.

Sonuncu sualımız Avropa Şurasının yeni yaradılmış Süni Zəka üzrə daimi komitəsilə bağlıdır. Komitənin fəaliyyət istiqamətləri nələrdən ibarətdir? Sizcə, Komitənin fəaliyyəti Azərbaycana süni intellektin tətbiqi üzrə hansı yenilikləri gətirəcək?

11 sentyabr 2019-cu il tarixində 1353-cü iclasında Avropa Şurası Nazirlər Komitəsi Süni İntellekt üzrə Komitəni (CAHAI) yaratdı. Komitənin əsas məqsədi çoxtərəfli məsləhətləşmələr əsasında, Avropa Şurasının insan hüquqları, demokratiya və qanunun aliliyi standartlarına əsaslanan süni intellektin inkişafı, dizaynı və tətbiqi üçün hüquqi bazanın formalaşdırılmasıdır.
Azərbaycan olaraq biz də Komitədə digər üzv dövlətlərlə birgə bərabərhüquqlu təmsil olunuruq. Komitənin iclaslarında beynəlxalq təşkilatların nümayəndə heyətləri, eləcə də, Avropa Şurasına üzv 41 dövlətin iştirakçısına Azərbaycanda rəqəmsal hökumət istiqamətində aparılan işlər, süni intellekt vasitəsilə dövlət xidmətlərinin təkmilləşdirilməsi və bu sahədə ölkəmiz tərəfindən əldə olunan uğurlar barədə daim məlumat verilib.
Komitədə təmsilçiliyimiz Azərbaycan üçün də bu sahənin inkişafı və süni intellektin müasir tətbiqetmə imkanlarına töhfə verməyə təbii ki müsbət təsirini göstərir və belə də davam edəcək.
Xüsusilə vurğulamaq istərdim ki, EHİM olaraq 2020-ci ilin aprelində “Rəqəmsal idarəetmədə süni intellekt” mövzusunda beynəlxalq konfrans və data yarışması keçirdik. Konfransın adı “AIFORDIGIOV” (Artificiail Intelligence for Digital Governance) idi. Konfrans çərçivəsində 20-dən çox ölkəni təmsil edən 50-dən çox tanınmış spiker, beynəlxalq təşkilatların nümayəndələri, mühəndislər, süni intellekt üzrə mütəxəssislər və futuristlər bir araya toplanaraq süni intellekt sahəsində dövrümüzün ən vacib məsələlərini müzakirə etdilər.
Bu gün Mərkəzimizin süni intellekt həllərinin istifadə edildiyi layihələrinə “ASAN Login”, “ASAN Viza”, “ASAN Bot” və digərlərini nümunə gətirmək olar. Həmçinin, EHİM-də Data labaratoriyası departamenti fəaliyyət göstərir ki, burada mütəmadi olaraq dövlət xidmətlərində süni intellektin tətbiqi istiqamətində araşdırmalar aparılır və müvafiq olaraq tətbiq edilir. Əminəm ki, bu gün Azərbaycanda süni intellektin tətbiq edildiyi bir çox layihələr, xidmətlər vardır. Ölkəmizin son illər bu sahədəki inkişafı həqiqətən sevindiricidir.

GDPR VƏ İNTERNET RESURSLARINDAN İSTİFADƏ KONTEKSTİNDƏ UŞAQ HÜQUQLARI

Siyavuş Bağırov

Müəllif Bakı Dövlət Universitetinin hüquqşünaslıq ixtisası üzrə bakalavr ikinci kurs tələbəsidir.

Texnologiyaların sürətli inkişafı ilə əvvəlki dövrlərdən fərqlənən XXI əsrdə insan hüquqlarının müdafiəsi əsas müzakirə predmetlərindən biridir. Xüsusi həssaslığı ilə seçilən uşaqların hüquqlarının qorunması yönündə təminat mexanizmlərin təhlili bir sıra problemlərin həllinə yönəlsə də, qanunlara edilmiş dəyişikliklər və ya müəyyən sahə üzrə hüquq mənbələrinin azlığı yeni maneələr formalaşdıra bilməkdədir. Bu məqalədə Ümumi Məlumat Mühafizəsinin Tənzimlənməsi (General Data Protection Regulation, bundan sonra GDPR[1]) adlı sənəd təhlil edilməklə onun müsbət və ziddiyyətli tərəfləri açıqlanır, həmçinin başda Birləşmiş Millətlər Təşkilatı Uşaq Hüquqları Konvensiyası (bundan sonra UHK) olmaqla digər hüquq mənbələri ilə qarşılıqlı müqayisəsi aparılır. Məqalədə texnoloji inkişafın uşaqların həyatı və hüquqlarına təsirləri də ətraflı izah edilir.

Açar sözlər: Uşaq hüquqları, Ümumi Məlumat Mühafizə Tənzimlənməsi, Beynəlxalq hüquq, Uşaq Hüquqları Konvensiyası, Avropa hüququ, Texnologiya hüququ.

GİRİŞ.

Cəmiyyət və dövlətin inkişaf tarixinə nəzər yetirdikdə insan hüquqlarına müxtəlif dövrlərdə müxtəlif münasibətin mövcud olması qənaətinə gələ bilərik. Belə fərqlənmənin əsas qaynağının başda dövlət idarəçilik forması, əxlaq və hüquq düşüncəsi olmaqla bir çox amillərin təsiri olması şübhəsizdir. Qeyd edilənlər sırasında hüquq düşüncəsini xüsusilə vurğulamaq lazımdır, çünki 'o, hüquqa sadəcə olaraq münasibət olmayıb, ... hüquqa tənqidi münasibətlə yanaşaraq onu qiymətləndirir'.[2] Mövzu üzrə hüquqa və qanunvericiliyə tənqidi münasibətlə yanaşaraq, fikrimizcə, ziddiyyətlərin aradan qaldırılması mümkündür.

İnsan hüquqları müəyyən sistem kimi düşündükdə, uşaq hüquqları onun sistemaltı elementi kimi mühüm əhəmiyyət kəsb edir. Uzun müddət ərzində formalaşmış konsensusu da nəzərə alaraq onların xüsusi diqqət və qayğıya ehtiyac duyduqları qeyd edilməlidir. Uşaq hüquqları insan hüquqları daxilində spesifikliyi ilə seçilir. Bunu bir-biri ilə sıx əlaqədə olan üç əlamət ilə səciyyələndirmək olar:

- Uşaq hüquqlarının spesifikliyinin birinci əlaməti tarixi amillərlə bağlıdır. Hesab edirəm ki, qədim zamanlardan 1924-cü ilədək müddəti əhatə edən birinci dövr sırf uşaq hüquqlarını tənzimləyən mənbənin olmaması ilə seçilir. Uşaqlara ibtidai icma quruluşunda daha diqqətcil və həssas münasibət mövcud olsa da, patriarxallığın təsiri və ardınca ilkin dövlətlərin formalaşması nəzərdən qaçmır. Burada müxtəlif məişətlərdə fərqli yanaşmaların fərqinə vara bilərik, məsələn bir-birinə qonşu sayılan Afina və Spartada uşaqlara verilən təhsil və psixoloji təsir fərqli idi. 'Spartadan fərqli olaraq Afina daha liberal və demokratik ictimai quruluşa sahib olduğuna görə təhsil sistemi baxımından fərqli bir quruluşa malik idi'.[3] Təhsildəki fərqlər növbəti zamanlarda

[1] Ətraflı məlumat üçün: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[2] M.F.Məlikova. "Hüquq nəzəriyyəsi", Bakı, "Elm və təhsil nəşriyyatı", 2019, 448 s. Səh. 303.

[3] D.Ç.Dikyol. "Antik Yunanda bir eğitim modeli: Sparta". Mediterranean Journal of Humanities, VI/2 (2016), səh 194. Ətraflı məlumat üçün: http://proje.akdeniz.edu.tr/mcri/mjh/6-2/MJH-12-9-Derya_CIGIR_DIKYOL.pdf (son baxış 16 fevral 2022-ci il).

hüquq düşüncəsində ziddiyyətlərə gətirib çıxara bilər. 1924-cü ildə Uşaq Hüquqları haqqında Cenevrə Bəyannaməsi qəbul edildi. 1959-cu ildə bəyannamənin daha təkmil və əhatəli versiyası hazırlanmış, 1989-cu ildə BMT Uşaq Hüquqları Konvensiyası (UHK) üçün bazis olmuşdur. UHK-nın qəbul edilməsi, zənnimizcə, inqilabi olmuş və onun əsasında ölkələrdə uşaq hüquqları haqqında qanunlar[4] qəbul edilmişdir. Sırf uşaq hüquqları ilə bağlı olmasa da, 1966-cı il Beynəlxalq Paktlarında onların hüquqlarının mühafizəsi ilə əlaqədar normalara yer verilmişdir.

- Spesifikliyin ikinci əlaməti bioloji amillərdir. Aydındır ki, bir qayda olaraq, uşaqların bioloji inkişafda olmasına görə fiziki zəifliyi bəzi işləri görə bilməmələrinə səbəb olur. Həmçinin, əfsuslar olsun ki, xüsusilə, zəif inkişaf etmiş ölkələrdə və (ya) müxtəlif rayonlarda uşaq əməyinin istismarı hallarına rast gəlinir. UHK-nın mövqeyinə baxsaq, görə bilərik ki, 'uşaqların iqtisadi istismardan və onların sağlamlığı üçün təhlükə törədən...yaxud onun sağlamlığına və fiziki...inkişafına ziyan vura biləcək hər hansı işin yerinə yetirilməsindən müdafiə hüquqları var' (maddə 32). Uşaqların məcburi əməyinin qadağan edilməsi haqqında 182 nömrəli Konvensiya 1989-cu ildə Beynəlxalq Əmək Təşkilatı tərəfindən qəbul edilmişdir.
- Sonuncu və üçüncü əlamət sosio-psixoloji təsirlərdir ki, ilk ikisi ilə vəhdət təşkil edir. 32-ci maddədə həmçinin onların sosial, mənəvi və əxlaqi inkişafına zərbə vurma ehtimalı olan işlərdən müdafiə hüququ göstərilmiş, 6-cı maddədə onların inkişafa olan hüquqlarını təmin etmək konvensiya iştirakçısı olan dövlətlər üçün öhdəlik kimi qəbul edilmişdir.

Əlamətlərin təhlili uşaqların xüsusi həssas kateqoriya olmasının sübutudur və istər dövlətlər, istərsə də təşkilatlar qanunvericilik fəaliyyətində rəhbər tutmalıdır. Texnoloji inkişaf mühitində uşaq hüquqlarının mühafizəsi özlüyündə yeni çətinlik və öhdəlikləri gətirir. UHK-nın 16-cı maddəsinin göstərişini (toxunulmazlıq hüququ) diqqətə alaraq, məsələnin tənzimlənməsi üçün bir sıra tədbirlərin təşkili imperativ hal almışdır. Vurğulanmalıdır ki, dövlətlərlə yanaşı beynəlxalq təşkilat qismində BMT, Avropa Şurası və Avropa İttifaqı uşaqların dijital erada hüquqlarının qorunması üçün qətiyyətli addımlar atmışdır. Sırf uşaq hüquqları ilə bağlı olmasa da, 1995-ci ildə qəbul edilmiş "Şəxsi Məlumatların Emalı və Bu Məlumatların Sərbəst Hərəkəti haqqında" Avropa Parlamentinin və Şurasının Direktivi[5] (bundan sonra Direktiv) region səviyyəsində rezonans doğurdu. Ehtiyacları qarşılamadığına və reallıqla uzlaşa bilmədiyinə görə illər sonra GDPR Direktivi əvəz etdi. Sələfi ilə müqayisədə tənzimlədiyi ictimai münasibətlər dairəsi daha geniş olsa da, GDPR-in mübahisə ediləsi yönləri heç də az deyil.

Yaşla bağlı normanın UHK-dəkindən fərqlənməsi, internet resurslarından istifadə zamanı onlara daxil olmaq üçün razılıqda üzləşilə biləcək problemlər, mənəviyyatı təhdid edə biləcək tərkiblərlə mübarizə GDPR-i müzakirə predmetinə çevirir. GDPR adıçəkilən problemlərin həllində effektiv mənbə rolunu oynayır mı? Yoxsa düzəliş edilməli və reallığa uyğunlaşdırılmalı məqamlar çoxdur?

GDPR-İN ZİDDİYYƏTLİ YÖNLƏRİ.

a. Yaş məsələsi və ondan irəli gələn valideyn səlahiyyətləri

[5] Nümunə olaraq, 1998-ci ildə Azərbaycan Respublikasında uşaq hüquqları haqqında qanun (№ 499-IQ) qəbul edilmişdir. Qanunun preambulasında UHK-yə və digər beynəlxalq sənədlərə istinad var. Ətraflı məlumat üçün: http://www.e-qanun.az/framework/3292 (son baxış 16 fevral 2022-ci il).

[6] Ətraflı məlumat üçün: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 (son baxış 17 fevral 2022-ci il)

İstər Avropa İttifaqı hüdudlarında, istər Avropanın digər ölkələrində, istərsə də müxtəlif regionlarda internet resurslarının davamlı inkişafı ilə uzlaşa biləcək və fərdi məlumatların qorunmasına təminat verən qanunvericilik mənbələrinin azlığı GDPR qəbul edildikdə diqqətləri ona yönəltdi. Valideynlərin əksəriyyətinin və kommersiya qurumlarının əks qütblərdə dayandığı mövzu yaş problemi idi. Direktivdə yaşla bağlı tənzimləmə yox idi. Bu baxımından GDPR-in rolunu qənaətbəxş saymaq olar. Lakin məlumatların emalı üçün razılıqla bağlı müəyyən edilmiş yaş həddinə münasibət eyni olmadı. GDPR-in 8-ci maddəsində təsbit edilmişdir ki, 'uşağın ən azı 16 yaşı olduqda onun şəxsi məlumatlarının emalı 6.1-ci maddənin "a" bəndi[6] əsasında uşağa bilavasitə informasiya cəmiyyəti xidmətlərinin təklifi yönəldikdə qanuni hesab edilir. Uşağın yaşı 16-dan az olduqda, bu cür emal yalnız uşaq üzərində valideynlik məsuliyyətinin sahibi tərəfindən razılıq verildiyi və ya icazə verdiyi dərəcədə qanuni olacaqdır. Üzv dövlətlər bu məqsədlər üçün qanunla daha aşağı yaş müəyyən edə bilər, bir şərtlə ki, bu yaş 13 yaşdan aşağı olmamalıdır'.

Yaşla bağlı bu cür tənzimləmənin tənqidçiləri hesab edirlər ki, 16 yaş etalonu heç bir konkret analizə əsaslanmır. 'Başqa sözlə, 13-16 yaş həddinin arxasında dayanan məntiqin nə olduğunu bilmədiyimiz üçün onun təsirini və təyin olunmuş məqsədə uyğunluğunu təhlil edə bilmirik'.[7] Belə olduqda uşaqlarla bağlı dəyişikliyin legitimliyə və sosial reallığı əks etdirməsi sual altına düşür. Hesab edirəm ki, bu hal təfsir və tətbiqdə çətinliklər yarada bilər. Unutmaq olmaz ki, bir sıra dövlətlərin bir ittifaqda cəmlənməsində məqsəd millətlər arasında harmoniya yaratmaq və onlararası ziddiyyətləri mümkün olduqca həll etməkdir. Mövzuya istinadən, Avropa İttifaqı müqaviləsinin 3 (3)-cü maddəsində uşaq hüquqlarının mühafizəsinə təşviq təşkilatın məqsədlərindən biri kimi təsbit edilmişdir.

Üzv dövlətlər müxtəlif yaş hədləri müəyyən etdikləri təqdirdə mövcud harmoniya təmin edilə bilərmi? Məsələn, təsəvvür edək ki, 3 qonşu və üzv dövlət Almaniya, Polşa və Çexiya müvafiq olaraq yaş həddini 13, 15 və 16 olaraq müəyyən etdilər. Subyekt 13 yaşı tamam olmuş Çex vətəndaşıdır və o, hazırda Polşa ərazisindədir, üstəlik hansısa Almaniyaya məxsus informasiya cəmiyyəti xidmətləri məlumat emalı ilə bağlı təklif irəli sürür. Belə halda həll üsulu GDPR-də göstərilməmişdir. Nəticə etibarilə, bütün üzvlər üçün standart və vahid yaşın müəyyən edilməməsi **birinci ziddiyyətdir.**

UHK-nın 1-ci maddəsinə əsasən, 'hər bir insan 18 yaşa çatanadək bu Konvensiyanın məqsədlərinə görə uşaq sayılır'. Konvensiyanın 16-cı maddəsi isə toxunulmazlıq hüququna birbaşa diqqət ayırır: 'Hər hansı bir uşaq onun şəxsi həyatı, ailə həyatı...yazışma sirri hüququnun həyata keçirilməsinə özbaşına və ya qeyri-qanuni surətdə müdaxilə obyekti, yaxud onun şərəf və ləyaqətinə qeyri-qanuni qəsd obyekti ola bilməz'. İki müddəanın paralel təhlili nəticəsində açıq şəkildə görünür ki, 15 yaşlı fərdin (nümunə kimi) şəxsi məlumatlarına müdaxilə və ya onun öz şəxsi məlumatlarından istifadə etmək yolu ilə müəyyən informasiya xidmətindən istifadə etməsinə məqsədli maneə yaratmaq (məsələn, valideynlərin qəsdən onlara icazə/razılıq verməməsi) beynəlxalq normaya ziddir.

Bir daha vurğulayırıq ki, Aİ-yə üzv dövlətlər həm də UHK-nı ratifikasiya etmişlər. Təsəvvür edək, UHK-nın 1 və 16-cı (18 yaş); GDPR-in 8.1-ci (16 yaş) maddələri təfsir edildiyi təqdirdə ikililik yaranacaq. Qlobal və regional qanunların yaş məsələsində uzlaşmaması **ikinci ziddiyyət hesab olunur** və uşaq hüquqları müddəalarının yanlış tətbiqinə səbəb ola bilər.

[7]GDPR-in 6-cı maddəsi "Emalın qanuniliyi" adlanır. Onun I hissəsi məlumatların prosesləşdirilməsinin qanuni hallarını müəyyən edir, (a) bəndi isə subyektin onun məlumatlarının bir və ya bir neçə xüsusi məqsəd üçün işlənilməsinə razılıq verməsindən bəhs etməkdədir.

Bir sıra ekspert rəylərinə diqqət yetirsək, onlar GDPR-də 16 yaşın çox yüksək həddi olduğu qənaətindədirlər. 'Siyasətçilərin 8-ci maddənin layihəsini tərtib etmə tərzində çatışmazlıq, praktiki səviyyədə qiymətləndirmək bacarığıdır ki, əgər uşaqlar bir fərd kimi ciddi qəbul edilərsə, onların insan hüquqlarına hörmət onların maraq və ehtiyaclarının tez bir zamanda valideynləri ilə uyğunlaşdırılmadığı anlamına gələ bilər'.[8] Bu fikrin tərəfdarları XXI əsrin öncəki dövrlərdən fərqli olduğu qənaətindədirlər və düşünürlər ki, uşaqlar əvvəlki qədər valideynlərindən asılı olmamalıdırlar. Asılılığın azaldılmasını isə resurslara azyaşlıların çox rahat əlçatımlılığı ilə əlaqələndirirlər. Qəbul edildiyi ilk vaxtlarda GDPR-ə gənclərin münasibətini tədqiq edən araşdırmada bu cümləyə rast gəlirik: '8-ci maddə gələcəyə toxunmağa çalışan siyasət resepti kimi görünür və keçmişin qərəzlərini əks etdirməkdən başqa heç nə etmir'.[9] Ekspert rəylərinin əksəriyyətinin və sosial sorğuların nəticəsinin təhlili göstərir ki, internet istifadəçilərinin sayında uşaqların bir həssas kateqoriya kimi çəkisinin artması 16 yaş tənzimləməsi ilə uzlaşmır. Bu, **üçüncü** ziddiyyətdir.

GDPR 8.1-ci maddəsində göstərilmiş "icazə" və "razılıq" (given or authorized) terminləri arasında qanunvericinin maddi və ya texniki olaraq fərqləndirici izah verməməsi qeyri-müəyyənlik yaradır.[10] Problem öz aktuallığını sadəcə bu kontekstdə deyil, həm də uşağın internetdən istifadə etməsi zamanı da qoruyur. Zənn edirəm ki, bu iki termin bir-birinə çox yaxın olsa da, onları bərabərləşdirə bilmərik. Praktiki baxımından "icazə" və ya "razılığ"ın bir-birindən fərqləndirilməsi çətindir və onları bir-birindən ayıra bilməyən (onların fərqləndiyini bilməyən və ya bu mövzuda bu iki terminin olmasını ağlına belə gətirməyən) vətəndaş üçün fərqli hüquqi nəticələrə gətirib çıxara bilər. Hesab edirəm ki, qanunverici bu ziddiyyətin həlli üçün müvafiq tədbirlər görməlidir.

Sonuncu ziddiyyət praktiki nəzarətin kifayət qədər problemli olması və istənilən nəticəni verə bilməməsidir. 'Nəzarətçi mövcud texnologiyanı nəzərə almaqla, belə hallarda razılığın uşaq üzərində valideyn məsuliyyəti sahibi tərəfindən verildiyini və ya icazə verdiyini yoxlamaq üçün ağlabatan səy göstərməlidir' (GDPR 8.2). "Ağlabatan səy" ifadəsi konkret deyil. Bu cür "səy" tövsiyə və ya göstərişlər formasında əks etdirilə bilər, ümumi strategiyaları əks etdirən sənəddə cəmlənə bilər. Lakin bu tövsiyələr nə dərəcədə tamlığı əks etdirəcək? Əvvəla, onlayn sistemə daxil olmuş uşaq ona yönəldilmiş sorğuya yalan cavab verə bilər. Məsələn, 11 yaşlı uşaq sistemdəki 18 yaş və yuxarı üçün nəzərdə tutulan xidmətə giriş sorğusuna məqsədli yanlış cavab verə bilər (tutaq ki, 19 yaşı qeyd edə bilər). İkincisi, 16 yaşadək uşaqlar üzərində icazə/razılıq səlahiyyətinə malik valideyn(lər) qəsdən müvafiq xidmətdən istifadəni məhdudlaşdıra bilər, halbuki övladı üçün ciddi əhəmiyyət kəsb edirdi, fəqət daxili münasibətlərdəki problemə əsasən, belə addım ata bilər. Üçüncüsü, Aİ məkanında savadlılıq səviyyəsi normadan yüksək olsa da, bu hər kəsin icazə/razılıqla bağlı qanunvericiliyi bildiyi və ya ən azından xəbərdar olduğu mənasına gəlmir. Qeyd etdiyimiz amilə görə valideyn ümumiyyətlə razılıq verməkdən imtina edə bilər. Daha pis halda isə məlumatları olmayan şəxslərdən valideyn səlahiyyətlərinə sahib ola biləcək şəxs qismində sui-istifadə edə bilərlər. Dördüncüsü, uşaqlar internet xidmətlərindən sadəcə evlərində istifadə etmirlər. Nəzərə almalıyıq ki, uşaqların internetə qoşulacaqları məkanlar çoxluq təşkil edir (məktəblər və s.). Belə olan hallarda müvafiq səlahiyyətin kimdə olması suallar doğurur.

[8] Đorđe Krivokapić, Jelena Adamović. "Impact of General Data Protection Regulation on children's rights in digital environment". Annals FLB – Belgrade Law Review, Year LXIV, 2016, No. 3, səh. 208.

[9] Joseph Savirimuthu. "EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids?" The London School of Economics and Political Science. Ətraflı məlumat üçün: https://blogs.lse.ac.uk/medialse/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/ (son baxış 19 fevral 2022-ci il).

[10] A.Pals, "GDPR from a youth perspective", (son baxış 19 fevral 2022-ci il) https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=687738.

Valideynlərin 16 yaşadək uşaqlar üzərində icazə/razılıq vermək hüquqlarından sui-istifadə etməsi ilə müəyyən hədlərdə mübarizə aparmaq üçün qeyd edilmiş xidmətlər ona birbaşa təklif edilə bilər, lakin belə xidmətlərin dairəsi kifayət qədər məhduddur. 'Birbaşa uşağa təklif olunan profilaktik və ya məsləhət xidmətləri ilə bağlı GDPR preambulasında nəzərdə tutulan istisna bu məsələni kifayət qədər lazımi aydınlıqla həll etmir'.[11] İstifadəçilərin sayında uşaqların çəkisini əks etdirən cədvələ diqqət yetirək:

Dünyada 18 yaşdan aşağı internet istifadəçilərinin faizi (2015-ci il və 2017-ci il üzrə)	~ 33 %
Aİ məkanında 18 yaşdan aşağı internet istifadəçilərinin faizi (2015-ci il üzrə)	~ 20 %
Aİ üzvləri arasında uşaqların internetə müxtəlif (kompüter və ya mobil/digər) vasitələrlə daxil olması faizi üzrə ən yüksək I və II ölkə (müvafiq olaraq İtaliya və Bolqarıstan) – (2019-cu il üzrə)	93 % (mobil) ---- 83 % (mobil) 48 % (kompüter)
Müvafiq olaraq İtaliya və Bolqarıstan üzrə ən azı həftəlik onlayn oyuna daxil olan uşaqların cins amili əsasında faizi (2019-cu il üzrə)	64% (o), 28% (q) 84% (o), 62% (q)
Onlayn məlumatların doğruluğunu yoxlaya bilməyəcəklərini söyləyən uşaqlar faizi (müvafiq olaraq İtaliya və Bolqarıstan, 2019 üzrə)	53% 48%
Məktəb və ya kollecdə ən azı həftəlik internetə qoşulan uşaqların yaş amili əsasında faizi (müvafiq olaraq İtaliya və Bolqarıstan, 2019 üzrə)	21%-25% (9-11 yaş) 38%-58% (12-14 yaş) 64%-74% (15-17 yaş)

Cədvəldə də yer verildiyi kimi müxtəlif cihazlar vasitəsilə 18 yaşdan aşağı şəxslərin internetə daxil olmaq faizi ən yüksək iki ölkəsində məktəb və kolleclərdə internetə qoşulmaq faizi heç də aşağı deyil. Məsələn, sonuncu sütunla yuxarıda qeyd etdiyimiz ziddiyyətləri əlaqələndirərək Bolqarıstan məktəb və kolleclərində razılıq/icazə texniki-nəzarət prosesində xüsusilə ciddi problemlərin olduğu qənaətinə gələ bilərik.

GDPR-in 8.3-cü maddəsi diqqətdən qaçmamalıdır. Orada '1-ci bənd (8.1 nəzərdə tutulur – müəllif qeydi) uşağa münasibətdə müqavilənin etibarlılığı, formalaşması və ya təsiri ilə bağlı qaydalar kimi üzv dövlətlərin ümumi müqavilə hüququna təsir göstərmir' norması öz əksini tapmışdır. Buna baxmayaraq, 'üzv dövlətlərin GDPR 8.1-ci maddəsi üzrə uzlaşmada çətinlik çəkə biləcəkləri qeyd edilir'.[18]

b. "Görünməzlik"dən hipergörünməyə

Dijital mühitin sürətli formalaşmasının mənfi tərəflərindən biri "görünməzlik" problemidir. İnternet resurslarının aktiv və ya qismən aktiv istifadəçisi olan uşaqların müxtəlif məqsədlər saxta profillərin imkanlarından yararlanmaları tendensiyası artmaqdadır. Müxtəlif sosial şəbəkələrdə qarşılaşılan hallar göstərir ki, adətən uşaqlar iki profildən istifadə edirlər, biri həqiqiliyi ilə seçilir, digəri isə onların müxtəlif maraqlarına xidmət edir. Məsələn, üçüncü şəxsləri narahat etmək, sadəcə olaraq tanınmalarını istəməmək, müəyyən məqsədlər üçün başqalarının hesablarını "gizli nəzarət"-də saxlamaq, valideynlərinin qoyduğu qadağaların pozulması halında onların cəzalarından qorxaraq onlayn oyunlar oynayan uşaqların başqa adlardan istifadə etmək və lazım olduqda təkzib üçün tutarlı sübutu olmaq və s.

Ümumiyyətlə, saxta profillərin aşkara çıxarılması, onların tənzimlənməsi kifayət qədər çətindir. Hesab edirəm ki, çətinliyin birinci səbəbi elə informasiya anlayışının hədsiz genişliyi ilə bağlıdır. 'Bu anlayış həddən çox genişdir və ümumi elmi mənada bu dərəcədə genişliyə haqq qazandırmaq mümkün olsa da, dəqiqlik və birmənalılıq tələb edən hüquqşünaslıq üçün elə də məqsədəuyğun deyil'.[19] Unutmaq olmaz ki,

[11] İstinad nöm.8, səh. 211.
[12] S. Livingstone, J. Byrne, J. Carr, "One in three: internet governance and children's rights", The Global Commission on Internet Governance, Paper Series, 22/2015.
[13] "When Free isn't", eNASCO Report, 59, (dekabr 2015-ci il üçün). https://www.unicef.org/media/48601/file (son baxış 20 fevral 2022-ci il, səh 3. - 2017-ci il üçün).
[14] GKO Summary Report, "Growing up in a connected world". UNİCEF Office of Research, 2019, səh. 6.
[15] İstinad nöm.15, səh. 8.
[16] İstinad nöm.15, səh. 12.
[17] İstinad nöm.15, səh. 20.
[18] İstinad nöm.8, səh. 214.
[19] Z.A.Əsgərov. "Konstitusiya hüququ". Dərslik, yenidən işlənmiş ikinci nəşr. Bakı, Bakı Universiteti nəşriyyatı, 2011, 760 s. Səh. 189.

informasiya dedikdə sadəcə müəyyən məlumat bazası başa düşülmür, eyni zamanda informasiya sisteminə giriş, məlumatlardan faydalanmaq da bu terminin bir parçasıdır. Mövzumuza uyğun olaraq, UHK-nın 17-ci maddəsi uşaqların kütləvi informasiya ehtiyatlarından istifadə etmək hüququnu müəyyən edir və dövlətlər bir sıra məqsədlər üçün (uşaqların sosio-psixoloji inkişafı və s.) onların bu hüquqlarının realizəsinə təminat verir. Məhz bu təminat əvvəldə qeyd etdiyimiz saxta profillərin yaradılması üçün sui-istifadə mühiti yaradır. Saxta profillərlə mübarizədə zənn edirəm ki, dövlətlər xüsusilə, beynəlxalq təşkilatların işləyib hazırlayacağı nizamlama alqoritminə ciddi ehtiyac duyurlar.

"Görünməz" uşaqları gözləyən təhdidi onların özləri çox vaxt düşünmürlər. Uşaq psixologiyasına istinadən, onların daha çox onlayn oyunlara yönəldiyi qənaətinə gəlirik. Uşaqlar isə oyunlarda uğur qazanmaq üçün çox vaxt onlara təqdim edilmiş xidmətləri qəbul edirlər. Əksəriyyət xidmət şərtlərini ümumiyyətlə oxumur və bununla da "görünməz" məqsədlər sahibi uşaqlar öz məlumatlarını sistemə daxil edərək hipergörünən vəziyyətdə qalırlar. 'Eyni zamanda, uşaqların problemləri üçün ənənəvi oflayn həll yolları da çətinləşir, çünki uşaqlar şirkətlər üçün həddindən artıq görünsələr də, onların oyunları, dostluqları və problemləri onların rifahı üçün fəal şəkildə maraqlanan hər kəs üçün yeni görünməzdir'. [20]

Hipergörünmə uşaqları bir sıra təhlükələrin hədəfinə çevirir. Onların məlumatları, brauzerlərdə, sosial tətbiqlərdə axtarışlarını əks etdirən tarixçələri və digər məxfi informasiyalar çox asanlıqla reklam ləvazimatına çevrilir, bununla da şirkətlər və digər subyektlər pul qazanırlar. GDPR hipergörünmə ilə mübarizədə istənilən səviyyədə effektiv deyil.

Tənzimləmə sənədində fikrin və informasiya ifadəsinin (mad. 85), rəsmi sənədlərə ictimai girişin (86), milli identifikasiya nömrəsinin (87), məşğulluq kontekstində emal (88), ictimai maraq, statistik, tarixi, elmi tədqiqatlarla bağlı təminat və istisnalar (89), məxfilik öhdəliyi (90), kilsə və dini təşkilatların məlumatlarının qorunması (91) "spesifik məlumat emalı" fəslinə daxil edilsə də, bu fəsildə uşaqlarla bağlı məlumatların emalı ilə bağlı konkret maddənin olmaması məqbul hesab edilmir. Həmçinin, mütləq şəkildə bir maddədə bütün problemləri həll edəcək normanın hazırlanması real olmasa da, qismən tənzimləmənin olması uşaqların dijital mühitdə hüquqlarının müdafiəsi üçün regional səviyyədə ciddi addım ola bilərdi.

GDPR-İN MÜSBƏT YÖNLƏRİ.

Çoxsaylı tənqid və ziddiyyətli məqamlara baxmayaraq GDPR-in spesifik əhəmiyyətini qeyd etməliyik. Əvvəla, GDPR-in uşaqların hüquqlarına aid normaya yer verməsi müsbət qiymətləndirilməlidir. İronikdir ki, 4-cü maddədə uşaq anlayışı verilməsə də, uşaq hüquqlarının əhəmiyyətini qanunverici dərk etdiyindən ona sənəddə yer verir. İkincisi, əvvəldə də qeyd etdiyimiz kimi 1995-ci il Direktivində yaşla bağlı məsələyə yer verilmirdi. Qüsurlu da olsa, GDPR onunla bağlı normanı əks etdirdi və qəbul olunduğu ilk vaxtlarda insanların marağının səbəbi də bu idi. O cümlədən, Aİ-də GDPR qədər internet problemini tənzimləyən normativ-hüquqi akt yox idi. Uşaq hüquqlarının önəmi təkcə 8-ci maddədə deyil, preambulada da əks edilmişdir.

Üçüncüsü, GDPR pozuntulara görə məcburiyyət tədbirlərini və onların hansı halda tətbiq edilməli olduğunu da müəyyən edir. GDPR şəxsi toxunulmazlıq hüquqlarının pozuntusuna görə məsuliyyət və tənbeh tədbirləri ilə bağlı ayrıca fəsil (VIII fəsil, 77-84-cü maddələr) ayırmışdır. 83.4-cü maddədə bu maddənin

[20] Livingstone, Sonia. "Realizing children's rights in relation to the digital environment". European Review. ISSN 1062-7987 (In Press), 2020. Səh. 6.

ikinci bəndinə[21] uyğun olaraq 10.000.000 avroya qədər və ya öhdəlik halında əvvəlki maliyyə ilinin ümumi dünya miqyasında illik dövriyyəsinin 2%-i qədər inzibati cərimələrə səbəb olan hallar qismində 8-ci maddə üzrə nəzarətçi və prosessorun öhdəliklərini pozması qeyd edilir. Dördüncüsü, GDPR-də uşaq hüquqlarının fundamenti olan 8.1-ci maddə 17-ci maddə üzrə əsaslardan biri kimi müəyyən edilmişdir. Məlumatın aid olduğu subyektin nəzarətçidən onun məlumatlarını ləngitmədən silməyi tələb etmək hüququnu əks etdirən 17-ci maddədən uşaqların məlumatlarına yer verilməsi sevindiricidir. Beşincisi, GDPR Direktivə nisbətdə 'informasiya xidməti provayderləri üzərində sərt qaydalar qoyduğundan yeni biznes modelləri ona əsasən şəkillənəcək'.[22] Göründüyü kimi GDPR həm uşaq hüquqlarının mühafizəsini vurğulayır, həm də informasiya xidmətlərini həyata keçirən subyektlərlə uşaq hüquqları arasında balansı qorumağa çalışır.

NƏTİCƏ.

Uşaq hüquqlarının dijital mühitdə tənzimlənməsi ilə bağlı ciddi ziddiyyətləri olsa da, zənn edirəm ki, GDPR qlobal səviyyədə UHK-dən sonra ikinci, regional səviyyədə isə birinci mövqedə durur. Direktiv dönəmin reallığı ilə ayaqlaşa bilmədiyi üçün əvəz edilmişdi. GDPR-ı isə qənaətbəxş saymaq olar.
Hələ də mövzunun tədqiqatçıları başda olmaqla Aİ vətəndaşları GDPR-da bir sıra dəyişikliklər ediləcəyi ümidindədirlər. Çünki yaşla bağlı vurğuladığımız məqamlar hazırda olmasa da belə, gələcək üçün ciddi problemlər yarada bilər. Xüsusilə, başlıca məqsədlərindən biri hüdudları daxilində xalqların harmoniyasını təmin etmək olan Avropa İttifaqı üçün təhdid dərəcəsinə qalxa bilər. GDPR-in 16 yaşı etalon kimi müəyyən edərək 13 yaşdan aşağı olmaması şərti ilə üzv dövlətlərə onun əsasında qanunları hazırlamalarını tövsiyə etməsi ilk baxışdan yaxşı görünə bilər, fəqət internet istifadəçisi olan uşağın informasiya xidmətini həyata keçirən subyektlə fərqli üzv dövlətdən olması özlüyündə problemdir. Uşaqların informasiya xidmətlərindən istifadəsinin qarşısını öz hüquqlarından sui-istifadə edərək alan valideynlərlə mübarizədə mütəxəssislərin alqoritmlər işləyib hazırlamaları zəruridir.
Mövzuya optimist yanaşdıqda GDPR 17-ci maddəsində 8.1-ci maddənin əsaslardan biri kimi müəyyən edilməsini vurğulamaq lazımdır. Ümid edirəm ki, istər Avropada, istər digər regionlarda müvafiq aktlar qəbul edildikdə bu Tənzimləmənin müsbət yönlərindən istifadə edəcəkdir.

[21] GDPR-in 83.2-ci maddəsində inzibati cərimənin tətbiq edilib edilməməsi zamanı nəzərə alınmalı şərtlər öz təsbitini tapmışdır. Göstərilir ki, 83-cü maddədəki inzibati cərimələr 58.2-ci maddənin a-h və j bəndlərinə (müvafiq səlahiyyətli orqanın tam səlahiyyətə sahib olduğu məsələlər) əlavə və ya onların əvəzinə tətbiq edilir. GDPR 83.4-də əks olunmuş "nəzarətçi" (controller) və "prosessor" (processor) ifadələrinin izahı 4-cü maddədə göstərilmişdir. Ona istinadən, birinci termin fərdi məlumatların emalının məqsəd və vasitələrini təkbaşına və ya başqaları ilə birlikdə müəyyən edən fiziki və ya hüquqi şəxs, dövlət orqanı, agentlik və ya digər orqan; ikinci isə fərdi məlumatları nəzarətçi adından emal edən fiziki və ya hüquqi şəxs, dövlət orqanı, agentlik və ya digər orqan deməkdir.
[22] İstinad nöm.8. Səh. 218.

Marc Rotenberg

Marc Rotenberg is Founder and President of the Center on AI and Digital Policy (CAIDP.ORG). The mission of the Center is "to promote a better society, more fair, more just — a world where technology promotes broad social inclusion based on fundamental rights, democratic institutions, and the rule of law." The Center is engaged in a wide range of AI policy activities, including research, analysis, training, and advocacy. The Center published Artificial Intelligence and Democratic Values, the first report to evaluate and rank national AI policies and practices. The research team includes more than 200 participants from over 40 countries.
Marc Rotenberg is also the lead author of the forthcoming Law of Artificial Intelligence (2023). He served on the OECD AI Group of Experts and helped draft the OECD AI Principles. Healso helped draft the Universal Guidelines for AI, a widely endorsed human rights framework for AI policy. Marc Rotenberg is a graduate of Harvard College, Stanford Law, and Georgetown Law, and an Adjunct Professor at Georgetown Law. He has published widely in academic and popular journals. He is the author of leading reference books on privacy law, open government, and AI policy.

Hello, Mr. Rotenberg. Thank you for accepting our interview offer. Please tell us a little bit about the Center for AI and Digital Policy.

We established the Center for AI and Digital Policy to focus public attention on the impact of Artificial Intelligence and to advocate for democratic values. Our mission is "to promote a better society, more fair, more just —a world where technology promotes broad social inclusion based on fundamental rights, democratic institutions, and the rule of law."
We established a research network of over 200 participants in 50 countries. We run AI policy clinics, provide advice for national governments and international organizations, and publish annually "Artificial Intelligence and Democratic Values," the first report to rate and rank national AI policies and practices.
And I am now working on the first U.S. casebook on The Law of Artificial Intelligence, which we hope will be available in 2023.

Concerns exist over how AI will affect democratic principles. UNESCO released a draft recommendation on the ethics of artificial intelligence in 2020 that established ten guiding principles. Regarding one of them, fairness, we have a question for you. How should fairness be implemented in artificial intelligence, in your opinion?

The UNESCO Recommendation for AI Ethics was adopted by 193 countries in 2021. It is the most comprehensive approach to AI governance so far. Fairness is one of the foundational principles. The aim is to ensure that when decisions are made by AI systems about people they are fair and just. To ensure fairness, there are several related principles – explainability, transparency, and contestability. Taken together these principles help ensure that individuals understand a decision, have the ability to examine the basis of the decision and are also able to challenge an adverse decision. These are the essential elements to ensure fairness in AI systems.

There are some crucial components in the European White Paper on AI, such as the person's right not to be subject to an automated decision in the first place. Do you think preventing discrimination by removing the individual's protected characteristics is possible? To what extent can or should law address concerns of algorithmic bias?

Since the issuance of the White Paper in 2020, the EU has moved forward with the proposed EU Artificial Act that would establish a right, in certain circumstances, not to be subject to an automated decision. As to whether it is possible to remove a person's protected characteristics from automated decision-making, that is a difficult question as there are proxies, such as postal codes, that mirror the protected characteristics. But there are techniques, including impact assessments that can help identify and mitigate these risks. It is important to identify and correct algorithmic bias.

Data is now stored in massive data centers as billions of smartphones and other gadgets capture and transfer data across high-speed worldwide networks. As artificial intelligence advances, the opportunity to utilize personal information in ways that infringe on privacy concerns grows. How is AI regulated for data protection? What authority is responsible for this?

This is a key challenge. Most countries have data protection laws that regulate the collection and use of personal data. But AI techniques have introduced new challenges, such as machine learning, that data protection laws did not anticipate. So, the goal will be to build on current data protection laws and establish new safeguards for the use of AI systems. In some countries, it is anticipated that the Data Protection Agency will be responsible for overseeing AI systems. In other countries, there may be offices with specific responsibility for this task. In all instances, it will be important to ensure that these supervisory authorities are independent, sufficiently funded, and enforce the legal standard to ensure that AI systems are human-centric and trustworthy.

Climate change and environmental issues are worldwide priority topics. The UNESCO Recommendation underlines the need for resource efficient AI technologies to ensure that AI becomes a more effective instrument in the fight against climate change and environmental challenges. In this regard, what do you think about AI's current influence on the environment?

There is a real concern today about the energy consumption of large AI models and also crypto currencies. Some of the models for Natural Language Processing are approaching a trillion parameters. A recent study indicated that training a single AI model can emit as much carbon as five cars over many years. At the same time, AI techniques may help identify new challenges to sustainability and promote efficiencies in the industrial economy. So, the aim will be to create AI systems with a light carbon footprint. And there are recent breakthroughs that suggest this will be possible.

Today, the problem of algorithmic transparency is one of the most important ones concerning AI policy. How much of a role does GDPR have in this issue?

One of the key articles in the GDPR (Article 15) establishes a right of access to “meaningful information about the logic involved.” Similar language is found in the EU Data Protection Directive which preceded the GDPR, and the modernized Council of Europe Convention on Privacy (“108+”). These provisions all have a common purpose – to establish a legal right to algorithmic transparency.
In our evaluation of national AI policies and practices, we give favorable scores to those countries that have

established a legal right to algorithmic transparency. So, countries that are subject to the GDPR or other similar laws for algorithmic provisions, rank more highly the AI and Democratic Values index.

Now that we have reached this point, I would want to tackle this issue from a different angle. Should artificially intelligent robots, if they have developed emotions, be granted the same legal protections as humans? What do you think?

No. Of course, there are many excellent movies about how robots become sentient and fight for their freedoms. And I enjoy those movies! But back in the real world, we need to be careful not to diminish human responsibility for the devices we create. And it will be tempting to transfer both authority and responsibility to autonomous devices as their actions increasingly mirror human activity. But I believe that would be a tragic mistake. As the American inventor Thomas Edison once said, "what we create with our hand, we should control with our head."

Is it humans who influence technology or technology which impacts humans? Which of the following best describes your thoughts about this situation?

There is obviously a dialectic as we shape our world and are, in turn, shaped by the world we create. But I object to those who say that because of the impact of technology certain outcomes are necessarily pre-determined. The technology determinists have argued for example that we must deploy AI systems because AI will necessarily become more widespread and make better decisions than humans. They have even suggested that AI will decide for us what is important. That argument is deeply flawed. For an essay in Issues in Science and Technology, I described that view as "a dangerous invitation to disarm the human intellect." I believe in the centrality of human reason. Technology influences the future, but it does not determine the future. That is our responsibility.

You have significant experience in teaching law school students about law and tech for many years. So we are curious about what you would say is the best advice for our readers about that topic.

I would make several suggestions. First, be curious. This is a fascinating field filled with change and innovation, but also complex problems. Examine all dimensions. Don't accept simple answers. Second, be independent and keep an open mind. It is too easy to make popular comments that everyone endorses. Do the hard work of research and analysis. Form your own opinions. My last advice is to be skeptical but not cynical. It is good to think critically, ask hard questions, and expect good answers. But do not assume the worst or become a fatalist. Legal institutions create opportunities to solve hard problems through reason and evidence. In my career, I have had many successes with innovative cases at the intersection of law and technology.

Thank you very much for talking to us today, Mr. Rotenberg!

Thank you for the interview! And please visit us at caidp.org.

Dr. Keith Barrows

Keith is a practicing attorney in the US, advising corporate and individual clients on blockchain, cryptocurrency, and artificial intelligence matters, as well as wealth transfer strategies, non-profit governance, and fundraising. His firm's website is www.kobarrowslaw.com
He earned a doctoral degree in Educational Leadership from Liberty University, a juris doctor degree from Widener Commonwealth School of Law, and a Bachelor of Arts degree from Lycoming College.

Hello, Dr. Barrows. Thank you for accepting our interview offer. Please, tell us a bit about your journey to where you are now?

My journey into law practice began when I was inspired to explore the law when I was much younger, I watched the movie "The Verdict" with Paul Newman, and really became enamored with the idea of being an attorney. I think everyone needs to have an inspiration or a healthy motive to become an attorney and stick with it for their career. Seriously though, I began my legal career in the US military as a member of the Judge Advocate General's Corps in the US Army. Most of my career has been primarily in non-profits and with individuals who had complex wealth planning needs.

Over the course of my career, I've been fortunate to have been exposed to some great companies, individuals and families as an attorney. I've worked with non-profit organizations and their donors structuring legacy gifts, and I've been able to help families navigate the complexities of wealth transfer planning for generational transfer.

In the last five years, I began focusing on artificial intelligence initially and then moved into blockchain and cryptocurrency law. All three of those aspects of the law are still developing rapidly, so quickly in fact that it is a challenge for lawyers and regulators to keep abreast of the innovation and growth of those fields. At the moment, I think there are many more questions than answers.

What in particular do you find fascinating about legal tech?

The thing I like best about legal tech and the issues surrounding it is the innovative nature of the businesses in tech, and how broadly it is affecting the practice of law. I suppose that's been true over the past several decades anyway, that new business innovation has driven legal practices to develop new legal theories and accompanying legal structures. I believe it is happening more rapidly now, especially in business formation with the advent of DAOs and cryptocurrencies for example. This is one area of the law that to me at least, is super-interesting.

Not only is the practice of law in relation to clients rapidly changing as lawyers advise entrepreneurs and investors, but how we practice law has changed in particular with the rise of big data and artificial intelligence. One example is on how eDiscovery takes place using AI capable software and systems, another is how arbitration has been affected by the availability of data. In eDiscovery, litigators can now search through

mountains of records using AI much more rapidly than before, with the same accuracy as humans or better. Naturally, there are problems associated with using AI that are being worked out, like algorithmic bias, but the promise of AI in making legal processes more efficient and reliable is there.
There are several large-scale arbitration projects underway around the world, where legal systems are seeking to use data to encourage "fair" resolution of disputes between parties that is faster, cheaper and of course less labor intense than litigation, or even in person arbitration. It will take some time before people might accept that a "bot" is going to resolve a dispute submitted to arbitration, but the more experience businesses and individuals have in using data in arbitration the more likely widespread adoption will occur. India is one country that is leading the way in using AI in arbitration and it will be fascinating to see if the promise of AI comes true.

How do you think the next generation of lawyers should approach using tech in their careers?

The next generation is already probably pretty well advanced in using legal tech just by the nature of smart technology access through phones, pads, tablets, etc. One area that the next generation will probably lead is the use of cloud technology and smart contracts. Many law firms are already using cloud-based technology to manage caseloads and clients, and I assume that will continue to proliferate. The next generation of lawyers will come to the practice of law using technology in their personal lives that is superior to the technology they find in their professional lives. One simple example is the use of digital signatures, where that has become the norm in many use cases in our lives with our phones and computers, but there are many jurisdictions around the world that do not accept digital signatures, and many for good reason. Another use case is in identity verification, where companies are using AI-enabled technology on a blockchain to conduct KYC and AML identity verification. The companies use a person's passport or other government issued identification with a photo, along with publicly available data, and real-time facial recognition or photo analysis to confirm a person's identity. This is extremely valuable given the otherwise often anonymous nature of blockchain and cryptocurrency. I think that the next generation will have an opportunity to lead in the adoption of legal tech in their practices.

As a Blockchain & Crypto lawyer, could you tell us a little bit about this area of law and its opportunities and development trend?

The current issues facing lawyers in both blockchain and crypto law practices are very similar. Most issues clients are facing relate to regulation of both blockchain and crypto assets, like coins and NFTs. There's a rising issue related to intellectual property surrounding NFTs right now, and whether an NFT can be subject to copyright protection and trademark protection. The transfer of NFTs is fairly straightforward, but the transfer of the associated copyright protection has been often neglected and overlooked. Similarly, the question of trademark protection is being adjudicated currently through trademark filings in numerous jurisdictions and litigation.

Opportunities for growth are going to abound for many years. There are always going to be regulatory and compliance issues that need to be navigated by clients, especially when a client is operating in multiple jurisdictions. Additionally, the traditional needs of clients are going to grow across multiple jurisdictions because their companies' activities on the internet, in the metaverse or Web3 are already taking place in multiple jurisdictions without regard to the intent of the company or issuer. Compliance, finance, operations and HR are all going to be re-examined in light of the nature of the metaverse for example, especially in the areas of data

privacy, choice of law for contracts, and financial transparency and reporting.

What is a misconception people in the crypto space have about the law?

Many entrepreneurs and users in the crypto space do not understand the reach of the law, particularly in terms of cryptocurrency issuance. They often believe that if they launch a crypto from a jurisdiction that does not have crypto-specific legislation or regulation that there are therefore no obligations for compliance when selling their tokens. The fact is that standing regulation and law can be applied to crypto and blockchain operations, it's just that enforcement actions are only now catching up and regulators are too.

What steps to take if we detect a crypto scam?

Reporting a scam crypto website or project is not as straightforward as it should be because it's often difficult to determine where to file the report. The most advanced and prolific scammers tend to use fake websites and fake company registrations, so it's hard to tell where they are officially located or registered. If you find out that information, you can always report it to authorities in that country or local jurisdiction.
The second problem in reporting crypto scams is that the websites, companies and projects are often located in a country that has little or no regulation of cryptocurrency or blockchain companies. While criminal laws exist to some extent in every jurisdiction, it could be difficult to get a local prosecutor interested in investigating a scam that purports to come from their local jurisdiction.
If you were exposed to a scam through a crypto exchange, you can report it to the exchange management and you might be able to make some progress through their investigative channels. The exchange will have a vested interest in finding and prosecuting scams. In the US or other developed economies, you'll be able to file a complaint with a consumer protection bureau, and a government regulator like the SEC or CFTC in the US. Finally, there are some companies that investigate crypto scams and try to recover funds for consumers. This is a relatively new development, but a welcome one.

Can we sue a crypto exchange company?

The short answer is yes. Suing an exchange will take some serious effort though, and will likely take a long time to get a result. Many exchanges are operating from non-US and non-EU jurisdictions, so you'd have to file suit in either your home jurisdiction or theirs, and depending on their terms or use or other contractual documents that you signed or acknowledged when you become a customer, your rights and ability to sue might be limited. It's also possible that there's an arbitration clause in the contract which limits your ability to file in a judicial system, but at least in arbitration there are clearly defined rules and procedures to enable a fairly quick result.

What kind of litigations arise from cryptocurrency scams and frauds?

The litigation that is arising from crypto scams and fraud is really no different than what we'd think of as typical in business today. The law on scams and fraud is old and established, only the applications are new and untested.
There have been cases of outright fraud, meaning dishonesty in statements about the nature of a cryptocurrency, fake whitepapers, fake investors, etc. There have also been cases of financial fraud, where companies and crypto issuers have acted more like a Ponzi scheme than an investment in a coin or token. Crypto mining has been loosely described to cover all sorts of activities, many of which are more akin to fraudulent currency trading and the like, simply using basic websites built and hosted by non-existent companies. The fraud remains basically the same: entrust me with your money and you'll get rich, when in fact the bad actor will just take your funds and disappear.
Just this past week, the US Department of Justice filed

charges against a Coinbase employee and two other individuals for wire fraud in connection with insider trading. This case is interesting in that it is the first high profile case involving fraud at a major exchange, but the legal theory is nothing new, it's based on insider trading and fraud.
At the same time though, the SEC filed a separate complaint against Coinbase, alleging that tokens listed on its exchange are securities. This is a major development in that practically the entire universe of coins and tokens has been built on the avoidance of classifying a token as a security under the *Howey* test under US case law. The SEC seems to be attempting to declare these digital assets as securities so it can subject them to regulation as such. This aspect is likely to be found to be an overreach by the SEC, but it will be interesting to watch how the courts deal with the issue.

Legal Technology is a rapidly growing space, what do you think lawyers can do to 'be prepared for dealing with these advancements and changes?

An interesting question. I have always believed that the true value in being educated in the law is that you're taught how to think like a lawyer. The ability to critically reason, formulate arguments and advocate is far more valuable than being given a set of answers to a specific problem. So what I'd advise in that first, have an open mind. The entrepreneurs that are building web3 and the metaverse challenging existing narratives about business structures, and key concepts like liability, enforceability, and so on. Keep up with them and apply what they are doing in legal frameworks that reduce risk. Secondly, be proactive. There are many voices in the legal community that are advocating for proactive, self-regulation in blockchain and crypto particularly, as one example. Third, be a sounding board for clients. You don't always have to force a client into an established model, you can take what you're hearing and adapt it to meet your client's needs. Finally, try and be a legal futurist.

What is some advice you would offer other people thinking about getting into the legal tech space?

Initially, read everything you can on legal tech, and stay active using technology in your practice. I would consider joining non-legal business groups and associations that are in the blockchain, crypto and AI spaces, and treat their educational materials and events like continuing legal education, even if you can't claim it as such with your licensing jurisdiction. I'd also stay abreast of how clients are communicating through online means, and particularly how the blockchain and crypto communities use mobile technology on their phones, because that's how they expect to communicate with their attorney as well. The legal tech world has been and will continue to grow rapidly and exponentially, and it's no time to be left behind, it is an opportunity

Thank you very much for talking to us today, Dr. Barrows!

Professor Dr. Paolo Balboni

Paolo Balboni (Ph.D.) is a Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law. He is a top tier European ICT, Privacy & Cybersecurity lawyer and serves as Data Protection Officer (DPO) for multinational companies as Founding Partner of ICT Legal Consulting. Chairman of the European Patent Office (EPO) Data Protection Board, Member of the EUMETSAT Data Protection Supervisory Authority and Member of the Europrivacy Board of Experts.

Hello, Professor Dr. Balboni. Thank you for accepting our interview offer.

It's my pleasure, thank you for inviting me. I am very happy to share my experience and insights into privacy, data protection, and data security with the ELSA network!

You are currently the co-Founder of "ICT Legal Consulting" an international law firm with offices in Milan, Rome, Bologna, Amsterdam, Athens, Madrid, Helsinki and Melbourne, and consulting capabilities in 49 countries and "ICT Cyber Consulting", a company specialized in cybersecurity consulting services. You are also a Professor of Privacy, Cybersecurity, and IT Contract Law at Maastricht University in addition to being the Chairman of the European Patent Office's Data Protection Board. What prompted your interest in privacy law? What are the key challenges you face?

My career in data protection started very early, nearly 20 years ago– before data protection was really a thing! I'm very fortunate to have gotten into the game at an early stage, something which allowed me to both witness and actively participate in the development of the world's most comprehensive data protection law, the General Data Protection Regulation (GDPR).

In 2002, when studying law at the University of Bologna (Italy) I participated in the Erasmus program and studied for 6 months abroad at Tilburg University (The Netherlands) where I followed a course on Privacy and Data Protection which immediately sparked my interest. It was something new, something which still needed to be explored. I later went on to complete a PhD on comparative ICT (Information and Communication Technology) law at Tilburg University and towards the end of my PhD, I returned to Italy and worked in large international law firms in Milan (Bird & Bird and Baker & McKenzie). My main areas of focus in my professional career as a business lawyer included privacy/data protection, IT sourcing & transactions, IT Advisory, media, and general IP. I didn't leave academia behind, however. In fact, during those early years I taught the course "New Technologies and Law" of the Master's in Development, Innovation and Change (MiDIC) organized by the University of Bologna, Faculty of Law, Department of Economics, and carried out research on

the right to anonymity on the Internet, and privacy & data protection more generally, working as the Assistant to the Chair of Internet Law.

Finally, in 2011, I felt that I was ready for a new challenge and founded ICT Legal Consulting with my business partner Luca Bolognini. We started with our offices in Milan and Bologna (and shortly after we opened also in Rome), advising multinational companies on legal issues related to data protection and security, IT contracts, e-commerce, e-consumer protection, cloud computing (legal risk assessment and negotiation of contracts), e-health services compliance, Web 2.0 service providers' liability, online/mobile content and service providers' liability, online gambling and online gaming regulations, electronic signatures, digital retention of documents and general IP matters, etc.

When we founded the Firm, companies and the public had not yet understood how important privacy and data protection compliance really are, but with the GDPR the relevance of the topic really took hold.

11 years later, ICTLC is a firm with over 70 professionals and a presence in 49 countries! I am very proud of how far we have come and the fact that we help organizations respect the fundamental rights of individuals through compliance. I'm also honored to be able to carry out cutting-edge research in my role as a Professor. There is really nothing more gratifying than helping students to comprehend and contribute to this evolving field of law.

What do you think, should lawyers be concerned by the rise of AI and the concept of the "robot lawyer"?

I do not think that lawyers should be concerned about the rise of AI and so-called "robot lawyers". It is true, however, that machine learning techniques are improving their capabilities as a rapid pace. That being said, there is still a long way to go before the law can be fully automated, and I doubt if it ever will be 100% automated, even in the distant future. I'd also point out that AI-based document analysis tools have already been used in the legal sector for quite some time!

As we have seen in the past with technologies (think about computers, industrial and agricultural machinery, telephones, conveyor belts, etc.) partial automation leads to increased productivity, but does not completely eliminate the need for humans. The widespread use of computers and the internet have already drastically changed the work of lawyers, allowing us to work more and to do so more efficiently. The partial automation of certain tasks that we currently carry out will allow us to focus on more strategic and delicate aspects of our profession.

In law, like in business generally, the human touch and personalization really make a difference. When I work with clients, nearly all of which are multinational companies, I assess the unique (and often very complex) needs of the company on multiple levels. As a human, I understand culturally embedded nuances and corporate needs which machines cannot accurately comprehend.

I would even go so far as to say that the use of AI in the legal sector may have a positive impact on society. For example, individuals who cannot afford a traditional lawyer may be able to make use of new technologies, like "robot lawyers" which can help them manage basic legal matters.

Do you see legal tech vendors missing any important privacy trends or changes?

Legal tech is truly booming, but it is not actually so new, even if it has become somewhat of a buzzword as of late. Legal tech encompasses multiple areas of the legal profession and there is no precise definition for the term.

As I mentioned earlier, lawyers have been using legal tech for quite some time already.
However, it cannot be denied that the relevance of legal tech in our work is increasing by the day. The last time I checked Stanford Law School's LegalTech Index, 1,939 companies active in the areas of legal research, legal education, practice management, analytics, etc. had been indexed. Moreover, according to Statista, in 2019, global revenues in the legal tech market were approximately EUR 17.3 billion, a number which is expected to reach approximately EUR 25.17 billion by 2025! With these numbers seemingly growing by the day, I don't think that startups are missing any valuable opportunities to enter the market. However, I do think that legal tech vendors should be clear about the limitations of the products they offer and ensure that customers are transparently informed about what the products can and, perhaps more importantly, cannot do.
I have also entered into the field of legal tech in my hat as co-founder of ICT Cyber Consulting, which has its own proprietary legal tech: 'ICTLC Learn'. ICT Learn helps our clients to train their employees on privacy, data protection and data security matters thanks to the customized training programs we develop in order to help our clients both comply with the requirements of the GDPR and foster a culture of data protection awareness within the client's organization.

We would love to discuss a little bit about your recent "Data Protection as a Corporate Social Responsibility (DPCSR)" research project as well. How did you come up with the idea of researching this topic?

As I mentioned earlier, I was fortunate enough to have had the opportunity to closely follow the development of the GDPR. It was already back then, as early as 2014, that I realized that regulation alone is not sufficient to adequately protect the rights and freedoms of individuals. I understood that something more was necessary - following the rules established by the EU legislator alone would not ensure ethical and socially responsible data processing for the benefit of data subjects. After ruminating on the topic for some time, I eventually consolidated my thoughts on the notion of placing data protection under the Corporate Social Responsibility (CSR) umbrella. In 2017, I published my first blog on the topic. By the time I became a full professor in 2019, I had already identified the five principles of Data Protection as a Corporate Social Responsibility (DPCSR) which I presented in my inaugural lecture.

What is Corporate Social Responsibility (CSR)? Is Data Protection a new form of Corporate Social Responsibility?

My favorite definition of Corporate Social Responsibility (CSR) is that proposed by the European Commission due to its simplicity. According to the Commission, CSR is the responsibility that companies take with respect to their societal impact. Data Protection, instead, is a legal compliance requirement. The GDPR and other applicable law such as the ePrivacy Directive, establish rules that companies are required to follow when processing personal data. However, very often data processing activities are legal in the sense that they do not violate the law, but they only create value for the organization and sometimes may even harm individuals or society (think about invasive tracking, transparency-related failures, etc.). By framing data protection as a part of CSR, we are able to really understand and tackle what the GDPR sets out to do – to encourage organizations to process personal data in a way that benefits not only the company, but also the individual and more generally, society, upholding democratic values for a more ethical, fair, transparent, and secure digital future.

What are the fundamental requirements of socially responsible data processing activities?

There are many fundamental requirements of socially responsible data processing activities. In the context of my research, together with Kate Francis, the PhD student working with me on the research, I have identified a total of 25 rules that organizations should follow. These rules or requirements can be grouped under five major categories which correspond to the principles I referred to earlier on in the interview:
Principle 1. Embed data protection, fairness, and security in the design of processes
Principle 2. Be transparent with individuals about the collection and further processing of their data
Principle 3. Balance profits with the actual benefits for citizens
Principle 4. Publish relevant findings based on statistical/anonymized data to improve society
Principle 5. Devote a portion of revenues to awareness campaigns for citizens with regards to the data-centric society.

How can companies build Data Protection into their CSR activities?

In the context of my research on DPCSR, I developed a specific framework (the UM-DPCSR Framework), which can be used by companies, but also other types of organizations such as universities, to successfully integrate data protection into new or pre-existing CSR or Environmental, Social, and Corporate Governance (ESG) programs. The Framework consists of five principles and 25 rules to be followed by the organization adhering to it. The Framework essentially translates theoretical ethical principles into tangible and practical guidelines for companies and organizations processing personal data. By adhering to the Framework, organizations can improve transparency and accountability and engage in fair and secure data processing activities. In this way, organizations can positively contribute to the greater good of a sustainable data-driven economy and a democratic digital society.

Many large organizations already have CSR and ESG programs, sometimes they are even required to report on certain CSR-related matters. Along these lines, the European Commission is taking great steps forward with respect to Corporate Sustainability Reporting and corporate sustainability due diligence, putting forth legislative proposals which will expand reporting requirements and require organizations to actively identify the environmental and human rights impacts of their business, etc.
The European Centre on Privacy and Cybersecurity ECPC, where we developed the UM-DPCSR Framework, started accepting submissions from Organizations that would like to adhere to the Framework in April 2022 after we published the initial Framework on the ECPC website in March. We will soon publish the complete Framework in the form of a book. Organizations that wish to adhere to the UM-DPCSR Framework will also be provided with an implementation Toolkit. The UM-DPCSR Framework and the related implementation Toolkit will be updated on a regular basis by the authors in collaboration with a permanent Working Group. Many organizations have already expressed their interest in adhering to the Framework.

What are the benefits for companies that embrace data protection as a CSR?

First of all, I would like to point out that it has already been demonstrated that a strategic and accurate approach to data protection can generate a significant return on investment (ROI). Therefore, data protection compliance and data security are good for the bottom line of organizations. Secondly, more and more, consumers are starting to both care about privacy and

data protection and data shows that they are more inclined to support sustainable organizations when, e.g., making purchases. While socially responsible and ethical behavior on the part of companies was once a "nice to have", I am convinced that it is becoming a "need to have", just like legal compliance. By embracing DPCSR, companies will be more trustworthy and younger generations will be more likely to support them. This means that in the long run, DPCSR will help companies reach their economic targets.

The UM-DPCSR Framework consists of five principles, and one of them is "balance profits with the actual benefits for citizens". What is the main purpose of this principle?

The third principle of the UM-DPCSR Framework, "Balance profits with the actual benefits for citizens", necessitates that organizations actively attempt to balance the profit that they make, thanks to processing the personal data of individuals, with the concrete benefits that individuals receive in exchange. The purpose of this principle is to ensure that data processing activities actually provide a benefit for individuals and that the provision of their data doesn't only benefit the organization. As with the other principles, I've developed five rules that organizations can follow to comply with this rule. For example, rule 1 calls on the organization to carry out what I have dubbed a "Profitable and Beneficial Test". In this test, the organization has to specifically look at how its data processing activities benefit society and the organization. The second rule requires organizations to engage with their stakeholders to understand what they care about and expect when it comes to data processing and the activities of the organization. Rule three instead necessitates that the organization establishes "trusted data processing activities", i.e., when using AI, enduring that bias and discrimination are actively combatted. Rule four requires the organization to take the environment and climate issues into consideration, ensuring, e.g., data minimization to reduce carbon emissions. Finally, rule 5 calls on the organization to regularly carry out Materiality Assessments so as to be sure that the data processing activities of the organization are aligned with social, economic, and environmental needs.

Last but not least, what advice would you give to anyone plotting the same career path as you?

I would tell anyone looking to follow in my career path that hard work and dedication pay off and that anything is possible if you set your mind to it. Never give up on your dreams, full steam ahead!

Yusif Bayramov

Yusif Bayramov 2015-ci ildən etibarən Azərbaycan Respublikası Ali Məhkəməsinin Elektron məhkəmə və informasiya texnologiyaları şöbəsinin müdir müavini vəzifəsində çalışır.
O, *2010-2015-ci illərdə Azərbaycan Respublikası Ali Məhkəməsində mütəxəssis, məsləhətçi və böyük məsləhətçi vəzifələrində çalışmışdır.*
Yusif Bayramov 2007-2011-ci illərdə Bakı Dövlət Universitetinin Hüquq fakültəsində ali təhsil almışdır. Bakı Dövlət Universitetinin Beynəlxalq münasibətlər və beynəlxalq hüquq fakültəsində bakalavr təhsilini tamamladıqdan sonra 2005-ci ildə Beynəlxalq münasibətlər istiqaməti üzrə magistr pilləsinə daxil olmuşdur.

Hörmətli Yusif bəy, müsahibə təklifimizi qəbul etdiyiniz və dəyərli vaxtınızı ayırdığınız üçün təşəkkür edirik.

Əvvəlcə, müsahibə üçün mən Sizə təşəkkürümü bildirir, ELSA kollektivinə gələcək fəaliyyətlərində uğurlar arzu edirəm. Ümid edirəm ki, müsahibə oxucularımız üçün faydalı olacaq.

Oxucularımızın Sizi daha yaxından tanıması üçün hazırkı fəaliyyətiniz haqqında qısa məlumat verə bilərsiniz?

Böyük məmnuniyyətlə. 2005-ci ildə Bakı Dövlət Universitetinin Beynəlxalq münasibətlər və beynəlxalq hüquq fakültəsində bakalavr təhsilimi tamamlayıb, Beynəlxalq münasibətlər istiqaməti üzrə magistr pilləsinə daxil olmuşam. Həmçinin, 2007-2011-ci illərdə Bakı Dövlət Universitetinin Hüquq fakültəsində ali təhsil almışam.
Azərbaycan Respublikası Ali Məhkəməsində 2010-cu ildə işə qəbul olmuşam, 2010-2015-ci illərdə mütəxəssis, məsləhətçi və böyük məsləhətçi vəzifələrində çalışmışam, 2015-ci ildən etibarən Elektron məhkəmə və informasiya texnologiyaları şöbəsinin müdir müavini vəzifəsində çalışıram.
"Elektron məhkəmə" informasiya sisteminin Ali Məhkəmədə tətbiq edilməsi, bu sahə üzrə təkmilləşdirilmə işlərinin aparılması, proseslərin optimallaşdırılması və onların idarə edilməsi iş fəaliyyətimin əsas tərkib hissəsi olub. Məhz buna görə də məhkəmə hüquq sistemində iş proseslərin avtomatlaşdırılması və bu sahənin inkişafı üçün süni intellekt əsaslı tətbiqlərdən istifadə edilməsi həmişə maraq dairəmdə olub. Bu məsələlərlə bağlı yerli və beynəlxalq treninq-təlimlərdə iştirak etmişəm.

"Elektron məhkəmə" informasiya sisteminin fəaliyyəti haqqında məlumat verə bilərsinizmi? Sizcə, "Elektron məhkəmə" informasiya sisteminin tətbiqi hansı üstünlükləri gətirdi?

Bu məsələ ilə bağlı qeyd etməliyəm ki, informasiya-kommunikasiya texnologiyalarının inkişaf etdirilməsi, məhkəmə fəaliyyətində rəqəmsal texnologiyaların tətbiqinin genişləndirilməsi dövlət siyasətimizin əsas prioritet istiqamətlərindən biridir.
Azərbaycan Respublikası Prezidentinin 2014-cü il 13 fevral tarixli 268 nömrəli Sərəncamı ilə müasir informasiya-kommunikasiya texnologiyalarının tətbiqini təmin edən "Elektron məhkəmə" informasiya sisteminin yaradılması ədalət mühakiməsinin həyata keçirilməsində

süründürməçilik və sui-istifadə hallarının qarşısının alınmasına, aşkarlıq və operativliyin təmin edilməsinə, məhkəməyə müraciət imkanlarının daha da asanlaşmasına, məhkəmə qərarlarının icrasına nəzarətin effektivliyinin artırılmasına, elektron kargüzarlıq və elektron sənəd dövriyyəsinin təmin olunmasına xidmət edir.

Azərbaycan Respublikası Ali Məhkəməsində 2016-ci ildən "Elektron məhkəmə" informasiya sistemi tətbiq edilməyə başlanmış və bu sistemin tətbiqi göstərilən elektron xidmətlərin keyfiyyətinin artmasına, informasiya təminatının yaxşılaşmasına, operativliyin təmin olunmasına gətirib çıxarmışdır.

Bununla yanaşı diqqətinizə çatdırıram ki, Azərbaycan Respublikası Prezidentinin 2021-ci il 16 iyul tarixli 1403 nömrəli Fərmanının 2-ci bəndində verilmiş tövsiyəsi nəzərə alınaraq, Azərbaycan Respublikası Ali Məhkəməsinin fəaliyyətinin hüquqi, təşkilati və informasiya təminatı daha səmərəli şəkildə təşkil edilərək Aparatın yeni strukturu təsdiq edilmiş, əsas fəaliyyət istiqamətlərindən biri məhz "Elektron məhkəmə" informasiya sisteminin fəaliyyətinin təkmilləşdirilməsi və inkişaf etdirilməsi olan, üç (3) struktur bölmədən ibarət Elektron məhkəmə və informasiya texnologiyaları şöbəsi yenidən təşkil olunmuşdur.

"Elektron məhkəmə" informasiya sisteminin tətbiqinin əsas üstünlüklərini diqqətinizə çatdırmaq istərdim:

1. Vahid məhkəmə portalının (www.courts.gov.az) yaradılması və heç bir qeydiyyatdan keçmədən məhkəmə işlərinə aid açıq məlumatlarla tanış olmaq imkanı;
2. Elektron kabinet vasitəsilə istifadəçilər məhkəmələrə getmədən ərizə, şikayət və digər sənədləri elektron qaydada göndərə, iştirak etdiyi iş üzrə prosesin gedişi, çıxarılan məhkəmə aktları, onlardan verilən şikayət və ya protestlər barədə məlumat əldə edə bilməsi;
3. Məhkəmə icraatının videokonfrans əlaqə sistemindən istifadə edilməklə həyata keçirilməsi;
4. Məhkəmə zallarında iclasların audio-video yazılarının aparılması;
5. Hakimlərinin "Elektron İmza" sertifikatları ilə təmin edilməsi və məhkəmə sənədlərinin elektron imza ilə təsdiqi;
6. "Elektron məhkəmə" informasiya sisteminə qoşulmuş məhkəmələrdə işlərin elektron dövriyyəsi;
7. Məhkəmə prosesində iştirak edən şəxslərə məlumatların elektron qaydada (elektron poçt, SMS məlumatlandırma və s.) çatdırılması;
8. Məhkəməyə daxil olan işlərin hakimlər arasında avtomatlaşdırılmış rejimdə, tam təsadüfi qaydada bölüşdürülməsi;
9. Məhkəmə sənədlərinin (bildiriş, məktub, qərardad) avtomatlaşdırılmış qaydada (e-şablon) hazırlanması;
10. Məhkəmə qərarlarının icra edilməsi üçün "Elektron icra" sisteminə qoşulmuş icra qurumlarına elektron qaydada göndərilməsi;
11. İş üzrə zəruri olan məlumatların digər dövlət informasiya resurslarından elektron qaydada dərhal əldə edilməsi;
12. Məhkəmə qərarlarının anonimləşdirməsini təmin edən proqram təminatı tətbiqi;
13. Yekun məhkəmə qərarlarının vahid bazasının yaradılması;
14. Bəzi statistik hesabatların elektron qaydada tərtibi;
15. Məhkəmələrin iş fəaliyyətində kağız daşıyıcıların tətbiqinin minimuma endirilməsi.

Bu üstünlüklərlə yanaşı təbii ki, çatışmazlıqlar da mövcuddur. Bu çatışmazlıqların aradan qaldırılması və sisteminin təkmilləşdirilməsi məqsədilə Ali Məhkəmənin Elektron məhkəmə və informasiya texnologiyaları şöbəsi tərəfindən ilk növbədə qanunvericilik və mövcud icra vəziyyəti təhlil edilərək məlumatlar toplanılır, tələblər müəyyən edilir və informasiya texnologiyaları üzrə mütəxəssislərin anlaya biləcəkləri formada tərtib edilərək icra edilməsi üçün aidiyyəti quruma göndərilir.

Eyni zamanda qeyd edim ki, dövlət orqanlarında qabaqcıl informasiya və kommunikasiya texnologiyalarından istifadə olunması və rəqəmsal idarəçiliyin tətbiq edilməsi

yüksək səviyyədə davam etdirilsə də, informasiya sistemləri arasında qarşılıqlı məlumat mübadiləsinin aparılması, yəni proaktivlik təmin edilmir.

“Elektron məhkəmə” informasiya sisteminə çatımlılığı olmayan mübahisə tərəfi olan vətəndaşların məhkəməyə müraciət imkanlarının genişləndirilməsi və məmnunluğunun yüksəldilməsi üçün hansı tədbirlər görülür və görülməsi planlaşdırılır?

Ədalət mühakiməsinə əlçatanlığın asanlaşdırılması, vətəndaşların müraciət imkanlarının genişləndirilməsi, məmnunluğunun yüksəldilməsi daim dövlətimizin diqqət mərkəzində olub. Bu məsələlər üzrə hazırda Azərbaycan Respublikası Ali Məhkəməsi ilə Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi arasında qarşılıqlı əməkdaşlıq çərçivəsində bir neçə layihə üzərində iş aparılır.

Eyni zamanda “Elektron məhkəmə” informasiya sistemində vətəndaşların məhkəməyə müraciət imkanlarının genişləndirilməsi və məmnunluğunun yüksəldilməsi məqsədilə Azərbaycan Respublikası Ali Məhkəməsi mütəmadi olaraq Azərbaycan Respublikası Ədliyyə Nazirliyi ilə birgə işlər görür və bu istiqamətdə həyata keçiriləcək işlərin davam etdirilməsi sistemin inkişafına təkan verəcəkdir.

Məhkəmələrə elektron şəkildə müraciət etmək imkanın sadələşdirilməsi, məhkəmə icraatının videokonfrans əlaqə sistemindən istifadə edilməklə həyata keçirilməsinin genişləndirilməsi və bu yanaşmanın sürətlə yayılması, süni intellektə əsaslanan xidmətlərin tətbiq edilməsi və bütün bunlara paralel olaraq vətəndaş cəmiyyətinin maarifləndirilməsi bu sahə üzrə fəaliyyətimizin əsas məqsədi olmaqla vətəndaş məmnunluğunu yüksəldilməsinə və məhkəməyə müraciət imkanlarının genişləndirilməsinə yönəlmişdir.

Elektron imza və ya asan imza sertifikatlarına malik olan vəkillər, sahibkarlar və məhkəmə proseslərində mütəmadi iştirak edən digər şəxslər bəzi xərclərdən azad olunmaları, əlavə əmək və vaxt sərf etməmələri, məhkəmə sənədlərini operativ əldə edə bilmələri üçün “Elektron məhkəmə” informasiya sisteminin imkanlarından geniş istifadə edirlər.

Lakin təsadüfi və zərurətdən irəli gələn hallarda məhkəməyə ilk dəfə müraciət edən şəxslərin elektron imza və ya asan imza sertifikatlarını əldə etməsi əlavə xərc tələb etdiyindən, onlar elektron kabinetdən istifadəyə maraqlı olmurlar. Hesab edirəm ki, vətəndaşlarımızın elektron xidmətlərdən səmərəli və effektiv istifadə imkanlarının artırılması və elektron kabinetdən istifadəyə təşviq edilməsi məqsədilə müvafiq güzəştlərin edilməsinə zərurət vardır. Yəni ilk dəfə elektron kabinet vasitəsilə ilə məhkəməyə müraciət edən şəxslərə müvafiq güzəştlərin tətbiq edilməsi məhkəmə icraatının elektronlaşdırılması işini sürətləndirəcəkdir. Təbii ki, bu məsələnin ilk növbədə qanunvericiliklə tənzimlənməsi məsələsi həll edilməlidir.

Sənədlərin sistemə yerləşdirildiyi zaman qanunla müəyyən olunmuş prosessual müddətlərin axımı hansı andan başlayır? “Elektron məhkəmə” sistemində müddət axımı necə tənzimlənir?

Bildiyimiz kimi qanunvericiliyə əsasən “Elektron məhkəmə” informasiya sisteminin tətbiq olunduğu məhkəmələrdə mülki və kommersiya işləri üzrə işdə iştirak edən şəxslər “Elektron məhkəmə” informasiya sistemində qeydiyyatdan keçmişlərsə, məhkəmə sənədləri bu şəxslərin həmin sistemdə yaradılmış elektron kabinetlərində yerləşdirilir və onlara bu barədə məlumat həmin sistem vasitəsilə elektron qaydada (elektron poçt, SMS və s. vasitəsilə) çatdırılır. Qanunvericilikdə məhkəmə sənədinin elektron kabinetdə yerləşdirilməsi həmin sənədin iş üzrə tərəfə rəsmi qaydada təqdim edilməsi kimi nəzərdə tutulub. Yəni müddət axımı məhkəmə sənədinin elektron kabinetdə dərc edildiyi vaxtdan başlanılır. Eyni zamanda elektron kabinet vasitəsilə məhkəməyə təqdim edilmiş ərizə və şikayətlər istifadəçi tərəfindən elektron imza ilə təsdiq edildiyi

andan məhkəmə təqdim edilmiş sayılır.
Əgər şəxs elektron kabinetdə dərc edilmiş məhkəmə aktından üzürlü səbəbdən şikayət vermə müddətini ötürərsə və bunu isbat edəcək əsaslar varsa, o zaman ümumi qaydada müddətin bərpası ilə bağlı məhkəməyə müraciət edə bilər.
Həmçinin, cinayət və inzibati xətalara, o cümlədən inzibati mübahisələrə dair işlərdə də məhkəmə aktları elektron kabinetdə yerləşdirilir və sistem vasitəsilə bu məhkəmə aktlarından elektron formada şikayət verilməsinin mümkünlüyü təmin edilir. Bu növ məhkəmə işlərində məhkəmə aktlarının elektron kabinetdə yerləşdirilməsi həmin aktların onlara rəsmi qaydada təqdim edilməsi kimi qəbul edilmir.

Vətəndaşların elektron məhkəmə informasiya sisteminin istifadəsi ilə əlaqədar narazılıq və şikayətləri adətən nə ilə bağlı olur? Bu sahədə hansı təkmilləşdirmələr aparılır?

Diqqətinizə çatdırıram ki, bütün məhkəmələrin 2/3-sində "Elektron məhkəmə" informasiya sistemi tətbiq edilməsi və qanunvericiliyə edilmiş dəyişikliyə əsasən "Elektron məhkəmə" informasiya sistemi tətbiq edilmiş məhkəmələrdə mülki işlər üzrə apellyasiya və kassasiya şikayətlərinin elektron qaydada təqdim edilməsi, eləcə də kommersiya işləri üzrə məhkəmə icraatın elektron qaydada aparılması sistemdən istifadəni genişləndirmişdir. Bu səbəbdən istifadəçilər tərəfindən daxil olan müraciətlərin də sayı artmışdır. Müraciətlər əsasən sistemdə mövcud olan funksionallıqlardan düzgün istifadə edilməməsi, elektron kabinetdən ilk dəfə istifadə edən şəxslərdə vərdişlərin tam mənimsənilməməsi, praktikada yaranan çətinliklər və texniki xətalarla bağlı olur.
Həmçinin, Vəkillər Kollegiyasının üzvləri tərəfindən də elektron kabinetin fəaliyyətinin təkmilləşdirilməsi, sistemin fəaliyyətində qarşıya çıxan suallarla bağlı müraciətlərin elektron kabinet vasitəsilə operatora ünvanlanmasının təmini və istifadəçi işinin səmərəsini artıracaq yeni funksionallıqlarının əlavə edilməsi ilə bağlı təkliflər də daxil olur.
Bununla yanaşı qeyd edim ki, 2021-ci il 5 mart tarixində Azərbaycan Respublikası Ali Məhkəməsi tərəfindən vətəndaş cəmiyyətinə məhkəmələrdə informasiya texnologiyalarının tətbiqinin genişləndirilməsi və "Elektron məhkəmə" informasiya sisteminin təkmilləşdirilməsi ilə bağlı təkliflər verməsi üçün müraciət edilmiş və həmin müraciətə uyğun olaraq 16 müxtəlif mənbədən 70-dən artıq təklif daxil olmuşdur. Daxil olmuş təkliflər Elektron məhkəmə və informasiya texnologiyaları şöbəsi tərəfindən təhlil edilərək ümumiləşdirilmiş və texniki tapşırıqlar hazırlanaraq icra edilməsi üçün aidiyyəti quruma göndərilmişdir.
Qeyd edim ki, bu sahədə daxil olan müraciətlərə diqqətlə yanaşılması və operativliyin təmin edilməsi məqsədilə Azərbaycan Respublikası Ədliyyə Nazirliyi tərəfindən 880 "qaynar xətt"i yaradılıb və vətəndaşlarımız sistemdə problemlə qarşılaşdıqları halda bu xidmətdən istifadə edə bilərlər.
"Elektron məhkəmə" informasiya sistemində tətbiq edilmiş yeniliklər barədə hakimlər, vəkillər, məhkəmə aparatı işçiləri və digər maraqlı şəxslər üçün mütəmadi olaraq təlimlər keçirilir, gələcəkdə də bu istiqamət üzrə analoji işlərin görülməsi nəzərdə tutulur.

Məhkəmə fəaliyyətində süni intellektin tətbiqini necə dəyərləndirirsiniz?

Diqqətinizə çatdırıram ki, Azərbaycan Respublikası Prezidentinin "Elektron məhkəmə" informasiya sistemi haqqında Əsasnamənin" təsdiq edilməsi barədə" 2020-ci il 1 iyun tarixli Fərmanında məhkəmə fəaliyyətində süni intellektdən istifadə edilməsi nəzərdə tutulmuşdur.
Hesab edirəm ki, bütün digər sahələrdə olduğu kimi, məhkəmə hüquq sistemində də müasir informasiya texnologiyalarının imkanlarından geniş istifadə olunması və süni intellekt əsaslı tətbiqlərin yaradılması mövcud olan problemlərin həll olunması üçün tutarlı vasitələrdən biri olmaqla həmin sahənin hərtərəfli inkişafına zəmin yaradır. Rəqəmsal transformasiyada ən çox yeni imkanlar vəd edən süni intellekt alətlərindən qanunvericilikdə

nəzərdə tutulmuş fundamental hüquqlara riayət etməklə istifadə edilməsi ədalət mühakiməsinin səmərəliliyi və keyfiyyətini artırılmasına xidmət edir. Bu kimi alətlərdən istifadə edərkən qanunun aliliyi və qərarların qəbul olunması zamanı hakimlərin müstəqilliyi prinsipləri qorunmalı, bu tətbiqlərin məhkəmə hüquq sisteminə münasibətdə törədə biləcəkləri risk və təsirlər əvvəlcədən müəyyən olunmalıdır.

Ədalət mühakiməsindən istifadə imkanlarının daha da genişləndirilməsi məqsədilə süni intellekt əsaslı tətbiqlərdən məhkəmə qərarları üzrə axtarış proqramının hazırlanmasında, proqnozlaşdırıla bilən ədalət mühakiməsində, mübahisələrin onlayn həll edilməsində, analitik təhlillərin aparılmasında, mübahisənin perspektivini öyrənmək məqsədilə müzakirə robotlarından (robot hüquqşünaslar) məlumatların əldə edilməsində istifadə edilə bilər. Qeyd edim ki, süni intellekt məlumatların (DATA) miqyası böyüdükcə, mövcud tətbiqləri bir o qədər çox təkmilləşdirir və onların proqnozlaşdırma imkanlarını yüksəldir.

Amerika Birləşmiş Ştatlarında, Avropanın bəzi dövlətlərində məhkəmə hüquq sistemində süni intellekt əsaslı tətbiqlərdən kifayət qədər geniş istifadə edilir. Onlardan, Amerika Birləşmiş Ştatlarında IBM Watson-u, "COMPAS"-ı (Alternativ cəza tədbirləri üçün müttəhimlər barəsində məlumatı profilləmənin korrektiv idarəetmə məqsədilə istifadə olunması proqramı), Böyük Britaniyada HART-ı (Zərər Riskini Qiymətləndirmə Metodu), Fransada Case Law Analytics-i (Məhkəmə təcrübəsinin təhlili), Avropada ODR-i (Mübahisələrin həlli üçün onlayn xidmət) qeyd etmək olar.

Düşünürəm ki, bu sahənin ölkəmizdə inkişafına nail olmaq üçün dövlətimiz tərəfindən görülən tədbirlərlə yanaşı, innovativ hüquqi xidmətlər təqdim edəcək hüquq texnologiya şirkətlərinin yaradılmasına və məhkəmə hüquq sistemi üzrə yeni startap layihələrin hazırlanmasına zərurət vardır.

Azərbaycan Respublikası Ali Məhkəməsinin sədri cənab Ramiz Rzayevin 2020-ci il 14 sentyabr tarixli əmri ilə Ali Məhkəmənin kollegiya sədrləri və struktur bölmə rəhbərlərindən ibarət informasiya texnologiyalarının tətbiqi üzrə işçi qrupu yaradılmışdır. İşçi qrupunun fəaliyyət istiqamətləri üzrə gördüyü və görülməsi nəzərdə tutulan işlər nələrdən ibarətdir?

Azərbaycan Respublikası Prezidentinin "Elektron məhkəmə" informasiya sistemi haqqında Əsasnamənin" təsdiq edilməsi barədə" 2020-ci il 1 iyun tarixli Fərmanının 3-cü bəndində Azərbaycan Respublikası Ali Məhkəməsinə "Elektron məhkəmə" informasiya sisteminin fəaliyyətinin təşkili və inkişaf etdirilməsi üçün zəruri tədbirlərin görülməsi tövsiyə edilmişdir.

Bu tövsiyəyə uyğun olaraq, Ali Məhkəmə sədrinin müvafiq əmri ilə Ali Məhkəmənin fəaliyyət səmərəliliyinin artırılması, informasiya texnologiyalarının daha geniş tətbiq edilməsi, bu sahədə strateji inkişafın təmin olunması, "Elektron Məhkəmə" informasiya sisteminin tətbiqinin təkmilləşdirilməsi, vətəndaşların məhkəməyə müraciət imkanlarının genişləndirilməsi və məmnunluğunun yüksəldilməsi, şəffaflıq və operativliyin təmin edilməsi məqsədilə işçi qrup yaradılmışdır.

Bu məqsədlərə nail olmaq üçün işçi qrupu tərəfindən mütəmadi olaraq görüşlər keçirilir, təhlillər aparılır və yuxarıda müəyyən edilmiş fəaliyyət istiqamətləri üzrə müvafiq işlərin görülməsi həyata keçirilir.

Görülmüş işlərlə bağlı qeyd etmək istərdim ki, Ali Məhkəmənin İnternet səhifəsində ədalət mühakiməsinin keyfiyyətinin artırılması, məhkəmələrdə hüquqi məsələlərin həllinə yanaşmanın sabitliyini təmin edilməsi və vahid məhkəmə təcrübəsinin formalaşdırılması məqsədilə müxtəlif meyarlar əsasında məhkəmə qərarlarında effektiv axtarışın aparılmasını təmin edən yeni informasiya-axtarış sistemi yaradılmışdır. (https://sc.supremecourt.gov.az/decision/).

İstifadəçilər informasiya-axtarış sistemində müvafiq funkisonallıqlardan, eyni zamanda mətn üzrə axtarış funksiyasından istifadə etməklə mübahisəli hüquqi məsələlərə dair Ali Məhkəmənin hüquqi mövqeyini asan şəkildə öyrənə bilir.

Bu sahədə görülmüş işlərin davamı olaraq Ali Məhkəməyə daxil olan məhkəmə işlərinin təsadüfi və avtomatik şəkildə müxtəlif meyarlar əsasında elektron qaydada bölgüsünü həyata keçirən yeni sistemi yaradılmışdır. Qeyd edilən sistem vasitəsilə məhkəmə işlərinin icraat növlərinə uyğun olaraq hakimlər arasında bərabər bölüşdürülməsi təmin edilir.

Yeni yaradılmış elektron bölgü sistemində məhkəmə işlərinin bölgüsünə nəzarət elektron formada təşkil edilir və sistem üzrə edilmiş bütün dəyişikliklərin (əməliyyatların) qeydiyyatı avtomatlaşdırılmış şəkildə aparılır. Yeni yaradılmış elektron bölgü sistemində məhkəmə işlərinin bölgüsünə dair müxtəlif növ hesabat formaları yaradılmışdır ki, bunun təhlili nəticəsində məhkəmə işlərin bölgüsünün əsaslı qiymətləndirilməsi və bu sahədə effektivliyin artırılması mümkün olur.

Bununla yanaşı, işçi qrupu tərəfindən "Elektron məhkəmə" informasiya sisteminin təkmilləşdirilməsi istiqamətində də müvafiq işlər həyata keçirilmişdir. Belə ki, qanunvericilikdə nəzərdə tutulmuş normaların "Elektron məhkəmə" informasiya sistemində tamlığının təmin edilməsi, eyni zamanda qanunvericiliyə edilmiş dəyişikliklərin sistemdə operativ və düzgün tətbiq olunması, məhkəmə aparatının iş fəaliyyətində effektivliyin yüksəldilməsi və digər mühüm əhəmiyyət kəsb edən məsələlərin həlli ilə bağlı təkliflər hazırlanmış və müvafiq icra hakimiyyəti orqanına göndərilərək icrası təmin edilmişdir.

Həmçinin, İqtisadiyyat Nazirliyi yanında Dövlət Vergi Xidmətinin sahibkarlara məxsus "Sahibkarların elektron kabineti"ndə tərəfin məhkəmə işindən xəbərdar olması məqsədilə məlumat xarakterli elektron bildirişin yerləşdirilməsi təmin edilmişdir.

Görüləcək işlərlə bağlı qeyd edim ki, Ali Məhkəmənin Plenumuna daxil olan müraciətlərin "Elektron məhkəmə" informasiya sistemində işlənməsinin təmin edilməsi, məhkəmə fəaliyyəti ilə bağlı analitik təhlil və statistikanın elektron qaydada aparılmasının təkmilləşdirilməsi və statistik məlumatların emalında Bİ texnologiyalarının tətbiqi, yekun məhkəmə qərarlarının bazasında mətn üzrə axtarış funkisonallığın yaradılması, elektron kabinetin istifadə imkanlarının genişləndirilməsi, sistemin avtomatlaşdırma dərəcəsinin yüksəldilməsi, iş üzrə bəzi əməliyyatların qruplaşdırılması, istifadəçi rahatçılığının daha da artırılması, məhkəmə işinin təşkili üzrə məlumat pəncərəsinin funksionallıqlarının genişləndirilməsi məsələləri hal-hazırda işçi qrupunun icraatındadır.

"Elektron məhkəmə" informasiya sisteminin əsas kompanentlərindən olan "elektron kabinet"-in istifadə qaydaları ilə bağlı vətəndaşların diqqətinə hansı məqamları çatdırmaq istəyərdiniz? Vətəndaşlar kabinetdən səmərəli istifadə üçün hansı qaydalarla tanış olmalıdırlar?

Bu məsələ ilə bağlı bildirmək istərdim ki, elektron kabinet vasitəsilə məhkəmələrə edilən elektron müraciətlərin sayı günbəgün artmaqdadır. Nəzərinizə çatdırım ki, 2022-ci ilin 2 rübünə olan məlumata əsasən sistemdə elektron kabinet istifadəçiləri sayı 80 min nəfərə yaxın təşkil edir.

Vətəndaşlarımıza məhkəmə işləri barədə məlumatları operativ almaq və məhkəmələrə elektron formada müraciət etmək üçün "Elektron məhkəmə" informasiya sistemində qeydiyyatdan keçməklə elektron kabinet yaratmağı tövsiyə edirəm. Bildirirəm ki, elektron kabinet vasitəsilə istifadəçilər əlavə əmək və vaxt sərf etmədən elektron imza ilə təsdiqlənmiş elektron iddia ərizəsi və digər sənədlər vermək, məhkəmə işinin materialları ilə ətraflı tanış olmaq, təyin olunmuş proseslər barədə SMS, elektron məktub və digər üsullarla xəbər tutmaq, məhkəmə sənədlərini hakimin elektron imzası ilə təsdiq edilmiş formada əldə etmək və məhkəmə rüsumlarını onlayn ödəmək imkanına malik olurlar.

Bir məsələni xüsusilə vurğulamaq istərdim ki, məhkəməyə iddia ərizəsi ilə müraciət etmədən də elektron kabinet açılması mümkündür və bunun əsas

əhəmiyyəti ondan ibarətdir ki, sizin elektron kabinetiniz olduğu halda istənilən məhkəmədə barənizdə olan məhkəmə işləri haqqında avtomatik məlumatlandırılacaq və elektron kabinetdə dərc edilmiş bütün məhkəmə sənədləri ilə operativ tanış ola biləcəksiniz.

Vətəndaşlarımız Ali Məhkəmənin internet səhifəsinə (supremecourt.gov.az) və Vahid məhkəmə portalına (courts.gov.az) daxil olaraq elektron kabinetdə qeydiyyatdan keçə və istifadə qaydaları haqqında təlimatla tanış ola bilərlər.

Lethal Autonomous Weapons systems threatening Human Rights

Emin Alimusayev

Bachelor of Law Graduate from Baku State University Azerbaijan

Keywords: Human Rights, International Humanitariam Law, Artificial Intelligence, Lethal Autonomous Weapons Systems, Autonomous Weapons, Killer Robots, Slaughterbots

Abstract

United Nations published a report[1] last year suggesting that a drone used in Libya's civil war selected a target without human control. This signifies a new chapter in human history: A machine that identifies and selects target based on Artificial Intelligence; A machine that makes a decision about human life. The report calls them 'lethal autonomous weapons systems', but they are also called 'killer robots' or 'slaughterbots'. These systems raise a number of legal and ethical concerns. Killer robots change the relationship between people and technology by giving life and death decision-making to machines. What we watch in movies is not science fiction anymore. We see the cloud, so we should foresee the storm coming.

Introduction

The 20th century contributed a lot to both human rights and technology. After WWII, outraged by the horrors of war and the Holocaust, the newly-formed United Nations addressed issues such as torture, warfare against civilians, the treatment of prisoners of war, and the prosecution of war criminals, setting forth new rules for warfare that protected basic rights. In 1948, the member states of the United Nations drafted the United Nations Universal Declaration of Human Rights. Since the adoption of the declaration, the UN, national governments, and independent organizations have worked to advance, promote, and enforce human rights throughout the world.[2] During the last century, technology developed even more rapidly. The invention of the triode tubes, transistors and integrated circuits revolutionized electronics and computers, which made it possible for us to think about AI. The development of technology had direct effects on our society. Nowadays, computers are being used in different fields. Although the impacts of computers on our society are mostly positive, there are some areas, in which AI and Machine learning are being used, that we should worry about. The application of AI in military, more specifically in autonomous weapons systems raise a host of concerns. Drones have been using in military since last few decades. As Second Karabakh War demonstrated to us, drones are highly effective on the battlefield. We see the same in the ongoing Ukrainian war, even songs are composed for drones. But the key point is that they have been controlled by a human operator. Lethal autonomous weapons systems are weapons systems that use artificial intelligence (AI) to identify, select, and kill human targets without human intervention.[3] After initial activation or launch by a person, an autonomous weapon system self-initiates or triggers a strike in response to information from the environment

[1] United Nations Security Council, 'Letter Dated 8 March 2021 From The Panel Of Experts On Libya Established Pursuant To Resolution 1973 (2011) Addressed To The President Of The Security Council' (United Nations Security Council 2021) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/037/72/PDF/N2103772.pdf?OpenElement> accessed 9 April 2022

[2] 'Introduction To Development Of Human Rights | Encyclopedia.Com' (Encyclopedia.com, 2022) <https://www.encyclopedia.com/history/legal-and-political-magazines/introduction-development-human-rights#:~:text=The%20modern%20concept%20of%20human,that%20humans%20possess%20from%20birth.> accessed 2 April 2022

[3] 'LETHAL AUTONOMOUS WEAPONS SYSTEMS' (2021) <https://futureoflife.org/lethal-autonomous-weapons-systems/> accessed 11 July 2022

received through sensors and on the basis of a generalized "target profile". This means that the user does not choose, or even know, the specific target(s) and the precise timing and/or location of the resulting application(s) of force.[4] Developing technologies like facial or vocal recognition often fail in recognizing people of colour or persons with disabilities. There are many examples on internet, which show failures of chatbots, self-driving cars, image recognition systems and many other AI systems. However, the mistake that a lethal autonomous weapons system might make, would not be forgivable as the mistakes of other AI systems. A machine with the ability to kill is a massive threat to human rights. It would be difficult for them to comply with international law, and their ability to act autonomously would interfere with legal accountability. The weapons would also cross a moral threshold, and their humanitarian and security risks would outweigh possible military benefits.[5]

Problems lethal autonomous weapons systems can cause.

A United Nations report suggested that a drone, used against militia fighters in Libya's civil war, might have selected a target autonomously. [6] The STM Kargu-2 drone, which the report described as "a lethal autonomous weapons systems", attacked soldiers during a battle in Libya's civil war in 2020, may have done so without human control, according to Final report of the Panel of Experts on Libya submitted in accordance with resolution 2509 (2020), published by UN Security Council on March 8, 2021. The Kargu-2 signifies something perhaps even more globally significant: a new chapter in autonomous weapons, one in which they are used to fight and kill human beings based on Artificial Intelligence.[7] Due to lack of human control, these systems raise a host of legal and ethical concerns. Main legal concerns:

1. **Would autonomous weapons systems be able to comply with international humanitarian law's fundamental rules of distinction and proportionality?**
International humanitarian law stipulates the military operations, tactics and weapons that are permissible. The two generally accepted principles of Distinction and Proportionality are the basis for a number of specific rules such as the prohibition of direct attacks on the civilian population or on Civilian objects, the prohibition of indiscriminate attacks and the obligation to adopt precautionary measures (Precaution) so as to avoid or limit casualties among Civilians and damage to civilian objects to the greatest possible extent.[8] Without meaningful human control, lethal autonomous weapons systems cannot comply with the principles mentioned above.

2. **Would these weapons be able to show compassion and respect human dignity in order to not to undermine the principle of humanity?**
Immanuel Kant said, 'Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means, but always at the same time as an end.' The concepts of sympathy, compassion and understanding belong to humanity,

[4] International Committee of the Red Cross, 'ICRC POSITION ON AUTONOMOUS WEAPON SYSTEMS' (2021) <https://www.icrc.org/en/download/file/166330/icrc_position_on_aws_and_background_paper.pdf> accessed 6 April 2022

[5] Human Rights Watch, 'The Dangers Of Killer Robots And The Need For A Preemptive Ban' (2016) <https://www.hrw.org/sites/default/files/report_pdf/arms1216_web.pdf> accessed 5 April 2022

[6] Cramer M, 'A.I. Drone May Have Acted On Its Own In Attacking Fighters, U.N. Says' (nytimes.com, 2021) <https://www.nytimes.com/2021/06/03/world/africa/libya-drone.html> accessed 5 April 2022

[7] Kallenborn Z, 'Was A Flying Killer Robot Used In Libya? Quite Possibly' (https://thebulletin.org/, 2021) <https://thebulletin.org/2021/05/was-a-flying-killer-robot-used-in-libya-quite-possibly/> accessed 5 April 2022

[8] 'Practice Relating To Rule 1. The Principle Of Distinction Between Civilians And Combatants' (icrc.org, 2005) <https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v2_cou_ch_rule1#:~:text=The%20two%20generally%20accepted%20principles,adopt%20precautionary%20measures%20(Precaution)%20so>

and they cannot be mimicked by machines. So they need to be controlled by humans in order to respect human dignity and the principle of humanity.

3. Who would be held responsible for crimes committed by lethal autonomous weapons systems?

Both, internal law systems and international criminal law only recognize the criminal responsibility of persons. For example, according to Rome Statute, Article 25, only natural persons can be criminally responsible. In order to avoid accountability gap, people must make decisions.

4. How can we be sure that, the use of these systems would not undermine the right to live, remedy and dignity?

These rights are meant to be understood by people, not by machines. Machines only do what they are programmed to do. It's absurd to think that, they can substitute human understanding and human decision-making.

5. How can we be sure that these systems will not be used to target certain people groups?

It will only be a matter of time until they appear on the black market and in the hands of terrorists, dictators wishing to control their populace better, warlords wishing to perpetrate ethnic cleansing, etc. Autonomous weapons are ideal for tasks such as assassinations, destabilizing nations, subduing populations and selectively killing a particular ethnic group.[9]

From an ethical perspective, this functioning process risks effectively substituting human decisions about life and death with sensor, software and machine processes. This raises ethical concerns that are especially acute when autonomous weapon systems are used to target persons directly. They risk harming those affected by armed conflict, both civilians and combatants hors de combat, and they increase the risk of conflict escalation. Another issue is the deployment of Autonomous weapons systems in military operations may start global arms race. After gunpowder and nuclear arms, autonomous weapons have been described as the third revolution in warfare.[10]

Warnings and possible solutions.

In order to warn states and humanity, and recommend solutions to the problems mentioned above, international organizations set their positions on this topic.

In 2012, Human Rights Watch published a report called Losing Humanity: The Case against Killer Robots. The report specifies, 'Human Rights Watch and Harvard Law School's International Human Rights Clinic (IHRC) believe that such revolutionary weapons would not be consistent with international humanitarian law and would increase the risk of death or injury to civilians during armed conflict.' In order to solve this issue, the report makes the following recommendations to states: 'Prohibition of the development, production, and use of fully autonomous weapons through an international legally binding instrument; Adaptation of national laws and policies to prohibit the development, production, and use of fully autonomous weapons.' That report also suggests that the roboticists and others, involved in the development of robotic weapons should establish a professional code of conduct governing the research and development of autonomous robotic weapons, especially those capable of becoming fully autonomous, in order to ensure that legal and ethical concerns about their use in armed conflict are adequately considered at all stages of technological development.

[9] 'AUTONOMOUS WEAPONS: AN OPEN LETTER FROM AI & ROBOTICS RESEARCHERS' (2015) <https://futureoflife.org/2016/02/09/open-letter-autonomous-weapons-ai-robotics/> accessed 5 April 2022

[10] The Atlantic. 2021. The Third Revolution in Warfare. [online] Available at: <https://www.theatlantic.com/technology/archive/2021/09/i-weapons-are-third-revolution-warfare/620013/> [Accessed 13 July 2022].

International Committee of Red Cross (ICRC) also addressed the concern autonomous weapons raise. ICRC's position on autonomous weapon systems argues that, 'the process by which autonomous weapon systems function: Brings risks of harm for those affected by armed conflict, both civilians and combatants, as well as dangers of conflict escalation; Raises challenges for compliance with international law, including international humanitarian law, notably, the rules on the conduct of hostilities for the protection of civilians; Raises fundamental ethical concerns for humanity, in effect substituting human decisions about life and death with sensor, software and machine processes.' Since 2015, The International Committee of the Red Cross has urged States to establish internationally agreed limits on autonomous weapon systems to ensure civilian protection, compliance with international humanitarian law, and ethical acceptability.

Amnesty International also started a petition and called people to sign it. They called on government leaders around the world to launch negotiations for new international law on autonomy in weapons systems – to ensure human control in the use of force and to prohibit machines that target people, reducing us to objects, stereotypes and data points. [11] 'We are stumbling into a nightmare scenario, a world where drones and other advanced weapons can choose and attack targets without human control', said Verity Coyle, Amnesty International's Senior Advisor on Military, Security and Policing.

In 2013, nongovernmental organizations launched the Campaign to Stop Killer Robots, and since then, concerns about lethal autonomous weapons have steadily climbed the international agenda. A growing number of policymakers, legislators, private companies, international and domestic organizations, and ordinary individuals have endorsed the call to ban fully autonomous weapons. The United Nations Secretary-General António Guterres said, 'Imagine the consequences of an autonomous system that could, by itself, target and attack human beings. I call upon States to ban these weapons, which are politically unacceptable and morally repugnant.' Referring to the development of weapons that could select targets and kill people without any human intervention as "unconscionable", 20 individuals and organizations who have won the Nobel Peace Prize issued a joint statement endorsing the call for a preemptive ban on these fully autonomous weapons: 'We, the undersigned Nobel Peace Prize Laureates, applaud this new global effort and whole-heartedly embrace its goal of a preemptive ban on fully autonomous weapons that would be able to select and attack targets on their own.' Almost 100 states have acknowledged the importance of meaningful human control over the use of force. Many tech companies have pledged not to participate in the development and the use of lethal autonomous weapons systems.

In 2015, the Future of Life Institute announced an open letter (Autonomous Weapons: An open letter from AI & Robotics researchers), which foresaw some of the problems which that might be posed by Autonomous weapons in future. The letter indicates: 'If any major military power pushes ahead with AI weapon development, a global arms race is virtually inevitable, and the endpoint of this technological trajectory is obvious: autonomous weapons will become the Kalashnikovs of tomorrow.' The letter suggests a ban on offensive autonomous weapons beyond meaningful human control as a solution. It has been signed by famous names, such as Elon Musk, Stephen Hawking, Steve Wozniak and many others.

A chapter ('The Need for and Elements of a New Treaty on Fully Autonomous Weapons') from publication by Fundação Alexandre de Gusmão, based on a presentation at the Rio Seminar on Autonomous Weapons Systems, February 20, 2020, argues, 'fully autonomous weapons

[11] 'Stop Killer Robots' (https://www.amnesty.org/, 2021) <https://www.amnesty.org/en/petition/stop-killer-robots/>

cross the threshold of acceptability and should be banned by a new international treaty'. The chapter proposes key elements of a new treaty to maintain meaningful human control over the use of force and prohibit weapons systems that operate without it. As the author suggests, the main element of the 'new treaty' should be meaningful human control.

As mentioned above, many international organizations and scientists warned humanity about the problems that lethal autonomous weapons systems can cause, offering few possible solutions. First of all, it should be understood that autonomy in weapons systems is not entirely useless. Using advanced military technology helps to diminish casualties on one's own side. However, there is a saying, 'guns don't kill people, people do'. Giving the decision-making to machines is what causes the problem.

It is obvious that military operations carried out by humans are not perfect and they often cause civilian casualties (it is called 'collateral damage'). But according to international criminal law, it is acceptable as long as it was not intentional and only constitutes war crimes when committed intentionally. Nevertheless, the same logic cannot be applied to lethal autonomous weapons systems, as they are unpredictable by their nature. The mistake of a machine and the mistake of a human cannot be considered the same.

Prohibition of the development of lethal autonomous weapons systems seems like the first solution to the problem. Such prohibition can be included in a new treaty or new protocol. However, considering the fact that these weapons do not require hard-to-get materials and their systems are built on computers, such prohibition would be difficult to monitor. Also, it is not certain whether states will reach a consensus on such prohibition or not.

Another possible solution of the problem is regulating the use of lethal autonomous weapons systems. Defining the main principles, standards and criteria for the development and the use of such systems would increase their reliability. Such regulations can also be included in a new treaty or protocol. Instead of prohibiting such weapons systems, regulating them seems like a better option. Standards should be defined about lethal autonomous weapon systems. Such as, what level of autonomy is acceptable, on what missions these systems can be used and etc.

Conclusion.

The first possible solution to the above mentioned problems is the prohibition of lethal autonomous weapons systems. The second one is the regulation of the development and the use of lethal autonomous weapons systems. Either way, it's obvious that something must be done. As mentioned above, a complete ban of such systems doesn't seem to be possible in the modern World. Instead, setting rules for developing and using such systems appears to be a more reasonable option. Key factor in such regulations should be limiting the level of autonomy in weapons systems and providing meaningful human control or supervision over decision-making. Such prohibition or regulations could come in the form of a new treaty or protocol to the Convention on Conventional Weapons.

It is encouraging, there is an increasing union of opinions among states that something must be done about lethal autonomous weapon systems. A new international law that bans or regulates the development and the use of such systems is the perfect way to solve these problems before technological developments have gone too far.

John Lindsey

John Lindsey is the founder of "InCite LegalTech", a technology optimization firm that leverages proprietary assessment software to provide a custom roadmap for law firms looking to Digitally Transform and get the most out of their Legal Technology investments.
You can find John on LinkedIn singing the praises of Technology through song parodies or email him at JohnL@InCiteLegalTech.com

Hello, Mr. Lindsey. Thank you for accepting our interview offer. How did you find yourself becoming involved with Legal Tech?

Funny story, we did an interview with a Legal Tech expert named Cat Casey. Cat is a Legal Tech influencer and a tech genius who works in the eDiscovery space and she shared with us a major flaw in how Law Firms and Legal Dept were attempting to take advantage of the various legal technologies available to them but with no regard to their current infrastructure readiness or systems optimization. (and they were suffering a high rate of project failures.) And since we had built a tool years ago to assist with this process and have utilized it across various domains such as Oil & Gas, Energy, Supply Chain & Logistics, BioTech, Healthcare, etc. It struck us after we did that show that there is an absolute opportunity to leverage the solution in the Legal domain as well.

You are currently working as a president of the "InCite LegalTech". How did the "InCite LegalTech" come about?

We are a very diverse firm made up of several different divisions with unique areas of focus, however, our AIRR - AI Readiness Roadmap tool has been a successful guide for firms in many different domains, so when we see an area that is "ripe" for digitally transforming, we make a push into the space. Following our discussion with Cat and our analysis of the Legal domain and need for tech, we felt it would be a perfect area to leverage our solutions. Since migrating into the Legal Tech domain, we added Anna Lozyinski to our team, and she added the Legal Tech assessment portion to our already existing tool, and we are referring to it as the Tech Optimization Tool.

Have you worked as a lawyer in any law firm? If yes, how does your previous life as a lawyer and current life as a President of "InCite LegalTech" compare?

No, I am not a lawyer, I rely on my General Council within our firm as well as affiliate Lawyers for any areas requiring detailed knowledge of the law. I am and have been a technologist and businessman for my entire career.

What effect has the COVID-19 crisis had on the progression and take up of legal tech amongst law firms and in-house legal teams?

In my opinion, Covid has been a huge catalyst for the Legal domain as it pertains to tech adoption.

It forced firms and organizations to work differently or perish, so everyone, for the most part, had to find a way to leverage technology to reach people that could not be together in person any longer. It was by far (in my opinion) the single most factor in digital adoption in the past 2 decades.

Should lawyers be concerned by the rise of AI and the concept of the "robot lawyer"?

No, I don't believe skilled Lawyers will ever be displaced by robots. AI is really about helping free Lawyers up from the mundane and allowing them to focus on the Higher Quality work that they are trained to do. I don't see where there is any rational fear for Lawyers... They should be looking at this technology as another way to serve their clients better and in a more efficient and cost-effective manner.

Do you think women are well represented in legal tech? If not, how do you think it could be improved?

I think that women are a huge part of the Legal Ops and Legal Tech profession, but can we do better by expanding their roles into leadership, ownership, partnership, and board positions?? Absolutely, we can and need to. I think the movement is happening as there is such an enormous talent pool of powerful women, and we support it 100%.

How do you think the next generation of lawyers should approach using tech in their careers?

I think tech should be taught in school as a critical part of becoming a Lawyer.

I think they are missing a huge opportunity to leverage tools and solutions that will help them run a better business and be a better lawyer and the sooner they are schooled on this the better.

What challenges did you face at the beginning of your journey related to LegalTech?

For us, it's been being viewed as outsiders since we didn't start in the Legal domain. The way we have successfully gotten around any of those objections was by sharing how the technology we build and deploy has been effective in other services-driven professional industries, so we know it will work in Legal as well. And secondly, we have partnered with prominent Lawyers that have been deploying tech in global firms for years, such as Anna Lozyinski and allowing them to build out the Legal tech portion of our optimization solution.

Do you have any advice for lawyers seeking to get to grips with legal tech?

Reach out to the massive LinkedIn community and find some mentors (and there are a ton) that are willing to help guide them through the learning process. Chad Aboud is a perfect example of this. He posts all the time about wanting people to DM him if they are thinking about Digitally Transforming and he will share his journey of success and help guide them to the necessary resources to move forward. This type of help is readily available, you just have.

Thank you very much for talking to us today, Mr. Lindsey!

Is privacy still possible on social media?

Chinara Gasimova

The highest education title she possesses now is a bachelor's degree in law earned from Baku State University. She is a first-year student of master's degree studies at Lund University. Gasimova is planning to graduate by 2023 with a degree of LL.M in European Business Law. She is one of the Swedish Institute Scholarship for Global Professionals holders.

Abstract

Because the 21st century has become an age of technology, social media, digital devices, and cloud connectivity have become an integral part of our lives. Especially, in this pandemic era where everything is almost digitized and technology is so deeply surrounded in daily lives which makes to think about privacy. Today, a large amount of information some of which is personal is shared by Internet users on social media platforms such as Facebook, Instagram, Twitter, Telegram, LinkedIn, TikTok, Snapchat, and others. The more the Internet and social networks expand, the more information is being shared online by social media users, and consequently, it seems hard to control social media privacy.

The meaning and value of privacy have become the subject of considerable controversy. The power of new technology, the Internet, and social media raises problems concerning the law, policy, and ethics on privacy. This essay will investigate the value of privacy and explore the relationship between social media and privacy. We will also analyze the possibility of protection of a person's data collected and stored on social media and identify ways to protect privacy on social media.

The right to privacy increased worldwide with the advent of information technology in the 1960s and 1970s[1]. As the value of privacy depends on society, culture, and context, it is a complex and broad term to define. The concept of privacy is articulated as the individual's "right to be left alone" and it has been defined as "the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others" [2]. As an interest and a valuable aspect of the human personality, privacy protects individual's self-determination, independence, dignity, and integrity. Privacy is an important element for a democratic society[3] as a social, public, and collective value.

All persons have a common interest in a right to privacy, so privacy is something we all ought to value. If we do not value our privacy, it may cause us to lose our privacy. Consequently, individuals and society must recognize the value of privacy and take measures to protect it. However, the massive stores of personal data collected and retained by social media make it almost impossible to control privacy. In addition, in some cases, it is difficult to strike a balance between freedom of expression and the right to information, which are among the instrumental values of a democratic political system, and the right to privacy.

Social media is a technology where personal information can be easily collected, processed, and disseminated.

[1] Piller C. "Privacy in peril". Macworld 10.7. (Jul.1993): 124-130.

[2] Thomas McIntyre Cooley. Treatise of the Law of Torts. 2nd ed. Callaghan, (1888): 29.

[3] Kirsty Hughes, The social value of privacy, the value of privacy to society and human rights discourse, Published online by Cambridge University Press: (05 July 2015), p 225.

The Internet has become a new meeting place for individuals as well as a business hub for corporates and merchandisers for selling and promoting their products and services. The rapid growth and development of social media platforms cause us to disregard the importance of privacy. With technological advancements, it is now possible to invade an individual's privacy without physically accessing his/her place or property. Researchers can obtain vast amounts of high-quality observational data about human interactions and behaviors via social media[4], which shows that such a platform has allowed eavesdroppers to intrude into our privacy. Data at risk can include our location, health information, sexual orientation, religious identification, facial recognition imaging, private messages, personal photos, and more, depending on the social media platforms. Such kind of personal data collected and stored by social media platforms is vulnerable to scraping, hacking, and data breaches, especially if platforms fail to institute crucial security measures and access limitations. Therefore, today, social media is not really the safest place to be and share personal information.

The question may arise that how does social media affect privacy? Data mining, Phishing Attempts, Malware Sharing, and Botnet Attacks are typically social media threats in which criminals are adept at tricking social media users into handing over sensitive information, stealing personal data, and gaining access to accounts that users consider private. Such threats to privacy on social media lead individuals to suffer harassment and lose their peace of mind. Privacy concern on social media has grown in recent years.

Data breaches, in particular, have worried many social media users, make them reconsider their relationships with the social media platforms and the security of their data on social media. The tragic story of Cambridge Analytica, a consulting firm, is a case in point. This is exactly how Cambridge Analytica used Facebook data in an effort to influence voter behavior in the 2016 presidential election in the United States.[5] The scandal involved exploited Facebook data of 87 million people being used for advertising to influence during elections. [6] One of the recent incidents belongs to LinkedIn which more than 780,000 personal information such as full names, email addresses, phone numbers, and workplace information associated with the leak this year. [7] However, LinkedIn has denied reports of this data breach: “We want to be clear that this is not a data breach and no private LinkedIn member data was exposed”.[8] While LinkedIn denies this leak, leastways, this situation makes individuals aware of dealing with their personal information and wake up data sharing in relation to social media privacy. This and other examples have steadily eroded public trust, leaving many people questioning if they have lost control over their personal data. According to a Pew Trust survey, 80 percent of social media users are concerned about corporations and advertising accessing and utilizing their posts on social media.[9] By understanding the value of privacy, the impact of social media on privacy, individuals need to do a lot to protect their data.

Although each individual is in charge of their social media privacy, in reality, it is hardly possible to control social media privacy in your own way. This is because

[4] Moreno Mancosu and Federico Vegetti, What You Can Scrape and What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data, SAGE journals, First Published July 31, 2020, p 2.

[5] Granville, K. The New York Times. Facebook and Cambridge Analytica: What you need to know as fallout widens (2018, March 19). Available at https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[6] Cristina Criddle, BBC News Facebook sued over Cambridge Analytica data scandal (28 October 2020). Available at https://www.bbc.com/news/technology-54722362.

[7] CyberNews Team, Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof (06 April 2021, Updated on 07/04). Available at https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/.

[8] LinkedIn Pressroom, An update on report of scraped data (Jun 29, 2021). Available at https://news.linkedin.com/2021/june/an-update-from-linkedin.

[9] Lee Rainie, Pew Research Center, Americans’ complicated feelings about social media in an era of privacy concerns (March 27, 2018). Available at https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

your friends and relatives will still disclose your personal information, such as your pictures, locations, and more on social media even if you take measures to safeguard your privacy on social media, including deleting your social media accounts. In another word, "Tell me who your friends are, and I will tell you who you are." works on social media, too. In 2008 testimony, EPIC's Executive Director Marc Rotenberg stated that "on Facebook ... third-party applications do not only access the information about a given user that has added the application. Applications by default get access to much of the information about that user's friends."[10] This makes it clear that we are not alone in controlling our privacy on social media.

To have a balance of privacy for all of us and organizations in this digital age is only possible through the toughest laws on privacy such as the General Data Protection Regulation (GDPR)[11], as well as increased inspections of companies responsible for protecting personal information under greater scrutiny. For example, the EU recognized the necessity for updated security as technology advanced, the Internet was developed and the European Data Protection Directive was adopted. Then in 2006 Facebook opened to the public and in 2011 the company was sued by a Google user for scanning her emails, Europe's data protection authority declared the EU needed "a comprehensive approach on personal data protection". Following the GDPR was adopted by the EU as the successor of the EU 1995 Directives as the result of the conceptual debates and issues regarding personal data. If privacy issues on social media are taken lightly, then digital privacy issues will invite more and more cyber attacks thereby leading companies to lose their reputation, theft of sensitive records of users, and no trust of social media users. When it comes to digital data nothing can be completely private such as photos, conversations, health information, or financial information. If there is currently not a way to 100 percent obscure your online profile, then that could open the door to future strict regulatory action. "When it comes to making these decisions about privacy and vulnerabilities, without any clear law or anything, it all becomes a matter of opinion," said Jeremiah Grossman, Chief of Security Strategy and Founder of WhiteHat Security.

Even today, many countries do not recognize the right to privacy as a specific constitutional right. Some countries have enacted general comprehensive data protection laws, and sectoral legislation dealing with privacy rights, yet privacy law has primarily evolved through judicial interventions in which the courts have read a right to privacy into existing rules. Considering that Internet, social media do not have a border, privacy needs international action. Although in many countries, international agreements such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights recognize privacy rights have been adopted into law, however, the law on privacy and its regulation mechanism needs to keep pace with technological development.

In conclusion, data privacy must not be ignored even if you think that you have nothing to hide. What we should be doing now is actively participating in the fight against the challenges that are causing the unintended death of data privacy in this era of digitization.

[10] Testimony and Statement for the Record of Marc Rotenberg Executive Director, EPIC, Hearing on "Impact and Policy Implications of Spyware on Consumers and Businesses" Before the United States Senate Committee on Commerce, Science and Transportation (June 11, 2008). Available at https://epic.org/wp-content/uploads/privacy/dv/Spyware_Test061108.pdf.

[11] What is GDPR, the EU's new data protection law? Available at https://gdpr.eu/what-is-gdpr/.

References

1. Piller C. “Privacy in peril”. Macworld 10.7, Jul.1993.
2. Thomas McIntyre Cooley. Treatise of the Law of Torts. 2nd ed. Callaghan, 1888.
3. Kirsty Hughes, The social value of privacy, the value of privacy to society and human rights discourse, Published online by Cambridge University Press: 05 July 2015.
4. Moreno Mancosu and Federico Vegetti, What You Can Scrape and What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data, SAGE journals, First Published July 31, 2020.
5. Granville, K. The New York Times. Facebook and Cambridge Analytica: What you need to know as fallout widens, 2018, March 19. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.
6. Cristina Criddle, BBC News Facebook sued over Cambridge Analytica data scandal, 28 October 2020. https://www.bbc.com/news/technology-54722362.
7. CyberNews Team, Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof, 06 April 2021, Updated on 07/04. https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/.
8. LinkedIn Pressroom, An update on report of scraped data, Jun 29, 2021. https://news.linkedin.com/2021/june/an-update-from-linkedin.
9. Lee Rainie, Pew Research Center, Americans’ complicated feelings about social media in an era of privacy concerns, March 27, 2018. https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.
10. Testimony and Statement for the Record of Marc Rotenberg Executive Director, EPIC, Hearing on “Impact and Policy Implications of Spyware on Consumers and Businesses” Before the United States Senate Committee on Commerce, Science and Transportation, June 11, 2008. https://epic.org/wp-content/uploads/privacy/dv/Spyware_Test061108.pdf.
11. What is GDPR, the EU’s new data protection law? https://gdpr.eu/what-is-gdpr/.

The European Law Students' Association

AZERBAIJAN