

FOURTH-GENERATION HUMAN RIGHTS AND THE VIOLATION OF THE CONCEPT OF PRIVACY

Abdülmecit Nuredin, page 9-23

ABSTRACT

Internet drove the world in the path of advancement. In the present situation, the regular lives of individuals are intermingled with the uses of the internet. Therefore, the lack of accessibility can put the individual in the backward stage of life. Therefore, the accessibility of the internet can be considered a significant human right in the fourth generation. however, the use of the internet has even some negative sides.

Since the use of the internet is easy and rapid, it has become an easy podium to intrude into the private lives of others. maintaining privacy is also a human right. therefore, in a time where both the accessibility of the internet and the maintenance of privacy are important, the question lies in the relationship. Therefore, the aim of the paper is eventually is to discuss the fourth-generation human rights and the violation of the concept of privacy.

Keywords: Human Rights, Violation, Privacy.

Prof. Dr. Abdülmecit Nuredin

*Faculty of Law,
International Vision
University, Gostivar,
N.Macedonia*

e-mail:

nuredin@vision.edu.mk

UDK: 342.737/.739:004

Date of received:

02.01.2023

Date of acceptance:

26.01.2023

Declaration of interest:

The authors reported no conflict of interest related to this article.

INTRODUCTION

In the present generation, the utilization of the internet and its uses in the present day to day lives cannot be ignored. The use of the internet and the latest form of technology has helped in making life highly easier and simple. It can be considered that the individuals who do not have accessibility to the internet are at the backward stage because now the entire system of living has intermingled with the uses of the internet. Therefore, the accessibility to the internet can be considered as the basic right of humans as per the fourth generation. however, though the use of the internet and the latest form of technology has helped in bringing positive changes in our lives, it has even helped in bringing negative changes in our lives as well. with the wider utilization of the internet, it has become highly easier to get the accessibility of the other's information which leads to the breaching of the privacy of others. researches show that the breaching of one's private data has become very common in the time of the internet. The aim of the paper is therefore to comprehend the importance of fourth-generation human rights which is the accessibility of the internet and how it is connected to the concept of privacy. The paper will be offering a literature review conducted by the other scholars, a reanalysis of the subject matter through research, findings, discussion along a conclusion of the topic.

LITERATURE REVIEW

The literature review is highly significant as it helps in offering the researches which have already been conducted about the subject matter in the past. This is highly vital as it helps in offering a wider aspect to the topic.

CONCEPTUAL FRAMEWORK

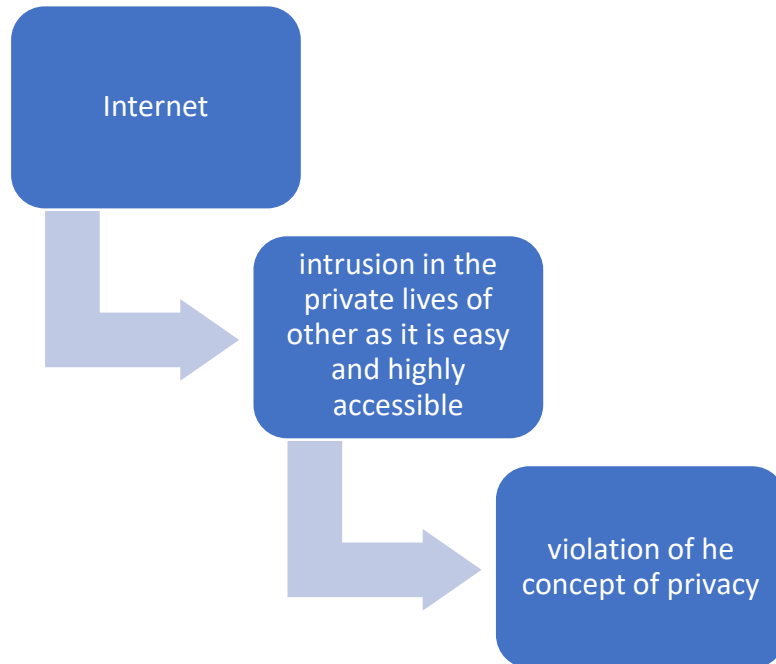


Figure 1: Conceptual map

WHAT ARE FOURTH-GENERATION HUMAN RIGHTS

Human rights can be considered as simply the rights which are being enjoyed by human beings. However, it is being observed that with time, technology has become a significant part of human beings. Technology has helped in bringing a higher rate of advancement. With the use of technology, human beings can communicate from one part of the world to the other, access a wider range of information, and even do things much faster. Therefore, not getting the accessibility to the latest technology and the internet can be considered as the source of deprivation (Soh et al 2018). This can eventually put the individuals at the backward stage. In this context, Valdés (2015), claims that in the context of the fourth generation, the accessibility to the internet and the latest form of technology can be considered to be human rights. (Filipovski, Z, Nuredin A, Sotiroska K, Galetin M, 2018) Dinçer et al (2020), claims that in the 21st century, daily regular life depends on technology and the accessibility to the internet, and therefore, it was important for the third generation of human rights (Nuredin, 2022) to catch up with the technology and consider its accessibility as the right.

Risse (2021), states that presently, the jobs and the entire system of education are dependent on education and therefore the inaccessibility of it can drive the individual towards deprivation. There is a various number of families who are struggling to keep up with the added expenses. Therefore, free access to the internet and the right to it can help individuals in coping up with the world and progressing with it.

CONCEPT OF PRIVACY

Protection of one's private information is one of the basic rights of every individual (Naresh 2020). However, in the time of the 21st century where the world is dependent on technology and the internet, it has become very much difficult to safeguard privacy. The information of one's data tends to get easily breached. According to Mulligan et al (2016), privacy can be described as the condition of the individual which is described by segregation from publicity. It can be considered as the "right of an individual to be left alone". In terms of the business, the economic situation is dependent on the information (Weber 2015). Therefore, it is the right of every business organization to safeguard their information and maintain their rate of privacy.

RELATIONSHIP BETWEEN TECHNOLOGY AND INTERNET WITH THE BREACHING OF DATA

In the time of technology, the utilization of the internet has led to the higher visibility of information. This is also one of the causes of the breaching of data. organizations are investing huge amounts to secure their data so that it does not get stolen by other rival companies (Kshetri & Voas 2018). In the year 2020, Microsoft claimed that the internal customer support database on which the company stored anonymity user analytics had been accidentally exposed. Researches show that there have been 1767 visibly reported privacy breaches in the only first six months of 2021. This tends to be 18.8 billion records. Sen and Borle (2015), in his research claims that statistics presented that 4 out of 5 breaches can be classified as the "hack" which was conducted by the "hackers" easily because of the feebler passwords. Cheng et al (2017), states that with the advancement of technology, the issues of visibility have increased. He further states that with the help of the internet, it has not just become easier

to hack the private information of others through illegitimate ways which further enables the hackers to blackmail it. Cookies have become an important concern. Additionally, the installation of software with viruses even leads to the theft of the data. Solove and Citron (2017), claims that the privacy of the individual is also intruded through the mobile applications which one utilizes. The smartphone user utilizes about 9 applications per day and 30 per month. These applications request location details, usernames, and email addresses. In this context, it is to be noted that there are some information's which can be considered risky information's which would lead an individual to trouble if the information's gets into the wrong hands. Identify theft can be considered to be a significant crime that is mostly done through the application of the internet.

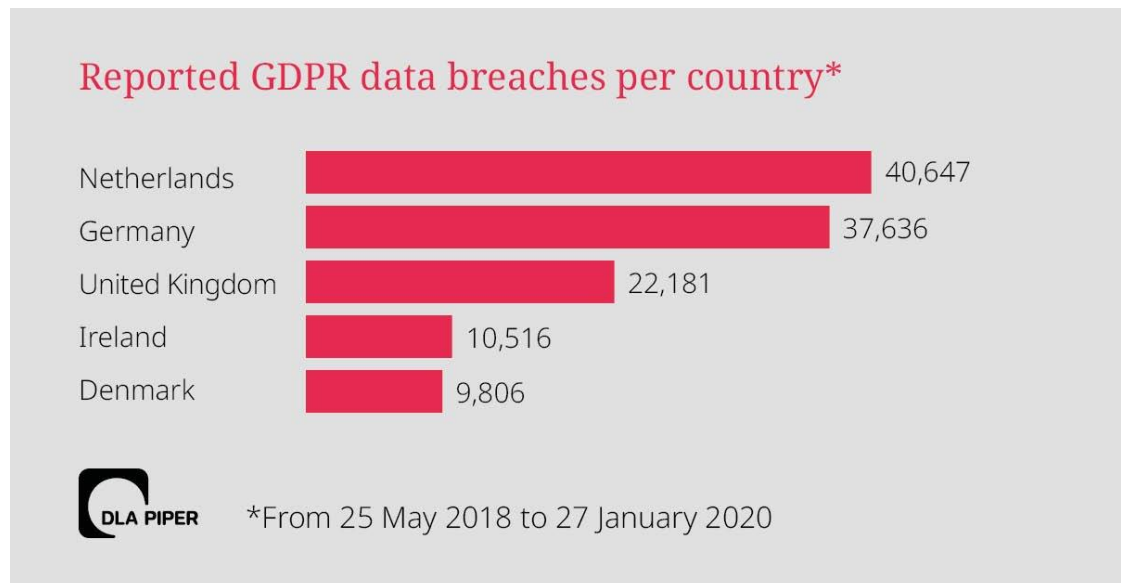


Figure 2: GDPR per country

IMPORTANCE OF PRIVACY IN THE TIME OF 21ST CENTURY

Maintaining privacy is also one of the significant rights of every individual (Hess et al., 2015). However, Nooteboom et al., (2020), claims that modern technology has progressed to the stage in which every individual is becoming highly dependent on the utilization of various sources like the worldwide internet and the new age electronic digital devices to operate our regular businesses.

Holmes et al., (2018), in contrast claims that the new age technology does not only helps in ensuring that improvements in our lives but it even acts as an intruder in our lives and invades away information's and it is being further shared outside the sources, blackmailed, or even bullied. (Nuredin, 2022) In this context, online privacy can be considered to be highly significant for various reasons. researches show that one might not be comfortable with the targeted ads which remember the internet search history. Kaley et al (2020), claims that there have been incidents in which people have fought to have their names and their images removed from the “revenge porn”. Additionally, some even requested the past private stories to get eradicated from the internet as well. according to Oliveira et al (2017), there is a various organization like Amazon, Google, and Facebook that have earned in the data economy through the congregation of the user data which leads to the maximization of the ad sales (Selim & Ali, 2022). Additionally, it can be said that people are not comfortable in sharing their private information with others as it even leads to the theft of money from their bank, destruction of their image, lead them in some sort of conspiracy which are among the others (Selim, 2021).

METHODS

To examine the importance of privacy in the time of the fourth generation, both the primary and the secondary methods of data collection have been conducted. In the process of the primary research, a survey was being conducted among 20 individuals whose data were being breached through the utilization of the internet. In the context of the secondary research, all the information which are already prevalent is taken into the consideration.

- **Primary research**

The questions which were being asked are as follows and their responses:

1. What is your gender segregation and is your privacy violated?

Options	Response of participants	Total no of participants	percentage
Female	17	20	85%
Male	3	20	15%

Table 1: gender segregation among the candidates

the above table demonstrates that out of the 20 participants whose privacy was being breached, 17 were females while 3 were males which are 85 percent and 15 percent respectively.

2. Do you remain active in social media applications?

Options	Response of participants	Total no of participants	percentage
Yes	19	20	95%
No	1	20	5%

Table 2: response of the candidates regarding their active activities in social media applications

The above table shows that out of 20 participants who were randomly surveyed, 19 participants claimed that they remain highly active in social media which is 95 percent whereas only 1 participant claimed that they don't remain online in social media which is 5 percent of the participants.

3. Do you have a strong password?

Options	Response of participants	Total no of participants	percentage
Yes	9	20	45%
No	11	20	55%

Table 3: Response of the candidates of whether they have a strong password the above table demonstrates the 9 out of 20 participants claimed that they have a strong password which is 45 percent of the candidates whereas 11 candidates which are 55 percent claims that they did not have a strong password.

4. Do you think the hackers have tried to take revenge or had any purpose for you?

Options	Response of participants	Total no of participants	percentage
Yes	16	20	80%
No	4	20	20%

Table 4: Response of candidates regarding their viewpoint that whether they perceived that their information was breached for the purpose of revenge

The above table demonstrates the fact that 14 candidates which are 80 percent of the candidates claimed that they perceived that their privacy is breached because people wanted to take revenge from them while 4 candidates which are 20 percent of the candidates claimed that they do not take the hackers had any intention of revenge.

5. Do you think that the hackers wanted money from u?

Options	Response of participants	Total no of participants	percentage
Yes	17	20	85%
No	3	20	15%

Table 5: Response of candidates whether the intruders of privacy invaded for the purpose of money 17 candidates claimed which is 85 percent that they perceive that the hackers wanted money from them while only 3 candidates which are 15 percent of the candidates claimed that it is not so.

6. Do you think that the hacker wanted to disrupt the steady flow of operations?

Options	Response of participants	Total no of participants	percentage
Yes	14	20	70%
No	6	20	30%

Table 6: Response of the candidates whether the hacker wanted to disrupt the steady flow of operation 14 candidates (70 percent) claimed that their privacy was breached because the hackers wanted to disrupt their steady operations while 6 candidates (30 percent) had contrasting views regarding it.

7. Do you think that you get attracted by the advertisements which u see while u surf the internet?

Options	Response of participants	Total no of participants	Percentage
Yes	11	20	55%
No	9	20	45%

Table 7: Response of the candidates that whether they get attracted towards the advertisements while surfing the internet

11 candidates (55 percent) claim that they get attracted to the items which they see in the pop-up ads while 9 candidates (45 percent) have contrasting viewpoints.

- **Secondary research**

Cyberstalking and cyberbullying- cyberstalking can be considered as the application of the internet or other electrical means to stalk or even annoy an individual or an association. It leads to false cases of accusations and even defamations (Short et al 2015). Researches show that it can even incorporate the continuous examining of other information, identify theft, threats, solidi cation of sex, vandalism, and even blackmails. Kaur et al (2020), in his case study claims that one out of 12 women and one out of every 45 men is being stalked at some moment in their lives. In a survey conducted among 4446 girls randomly selected, it was being found that 696 women have been stalked through email, breaching data, communication, watched, and are being constantly phoned. However, the majority of them claimed that they are active users of online platforms and they suspect that their information is being gathered through the online platform. Cyberbullying is the process in which internet is used as the medium to bully the victims. (Filipovski, 2017)

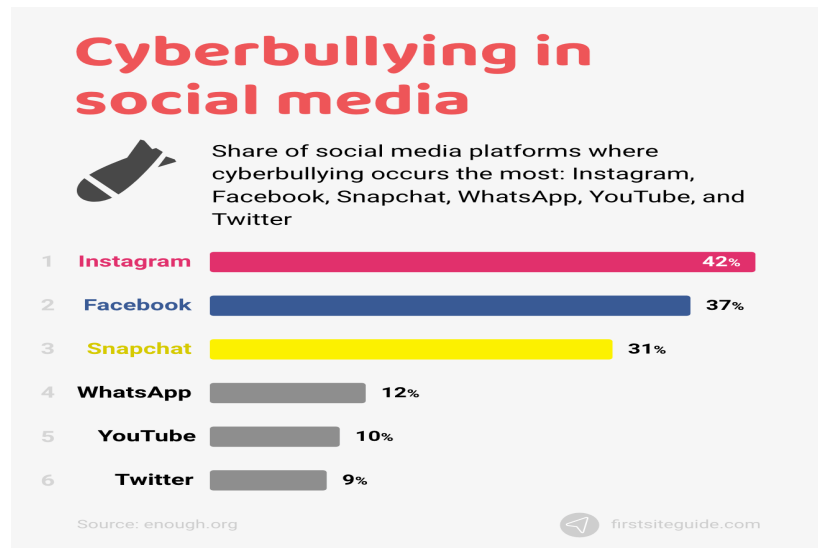


Figure 3: Cyberbullying in Social Media

Identify theft- identify theft occurs when one utilizes the other's personal information and pretends it to be theirs to commit some form of fraud or to gather some form of the economic advantages (Berghel 2017). The internet and the social media platforms are being utilized by the users as it enables the individuals to hide their real face, mask themselves and conduct blackmails. In the year 2019, 14.4 million customers reported that they have been the victim of identity fraud. This equals around 1 among 15 people (Hille et al 2015).

Doxing- This can be considered as the procedure of recovering, hacking, and even publishing other's information like the name, addresses, phone number, and other debit card details. This can be done to target a particular individual or even an organization. this has hugely given rise to the frauds in online transactions. Chen et al.,(2019), claims that a total of 615.39 crores has been lost in more than 1.17 lakh cases in online banking cases (Douglas 2016).

Information hacking through cookies by companies- cookies permit the websites to store data or the user's machine and later acquire it. Syomin (2020), claims that cookies can track when a visitor lands on a website and even examines what one does there.

This can eventually intrude on the privacy of the customers. According to Lohani (2019), almost every individual sees advertisements of their last searched item. The cookies permit the companies to understand the likings and the choices of the customers through which they tend to attract the customers.

Top Results Of Pop-Up Shops For Global Retail Professionals

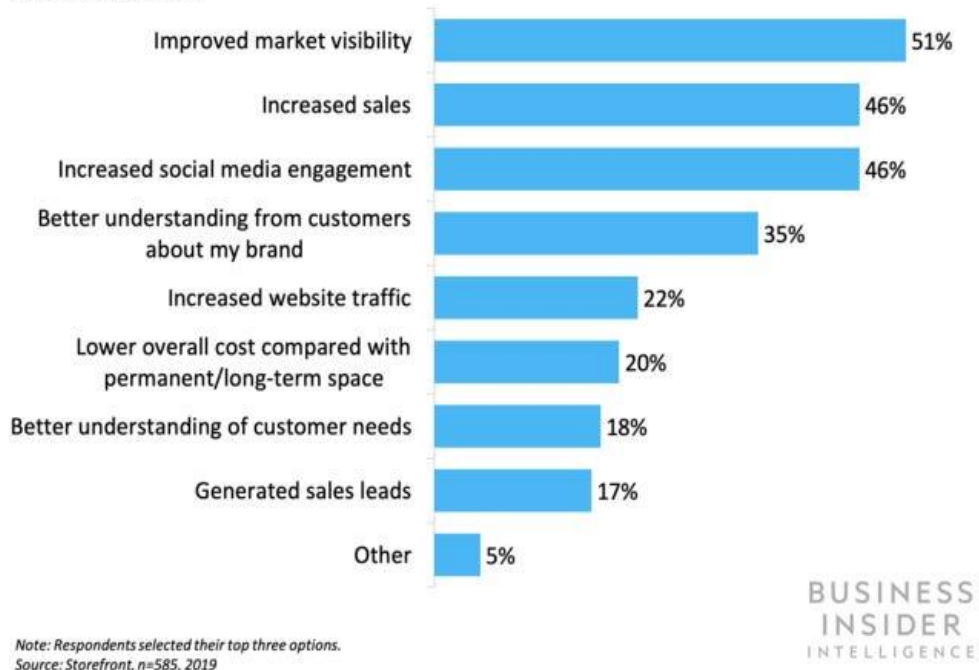


Figure 4: Top Result of Pop-Up Shops for Global Retail Professionals

DISCUSSION

From both the primary and the secondary researches, the reanalysis of the subject matter has been effectively been conducted. The following points can be considered through the reanalysis.

Revenge- the prime cause which can be considered to be the reason for breaching privacy is that of revenge. The accessibility of the internet and social media applications has enabled hackers to mask themselves and easily blackmail their victims.

Information stealing- in the time of advancement, everyone seems to be in some form of competition. Therefore, the internet has been utilized as the medium to disrupt the steady flow of operations of others. this is applicable for business purposes as well. acquiring the information of the rival company enables the organization to be competitively advanced in the market scenario.

Attracting customers- this is one of the most common reasons for which the privacy of the customers is being intruded on. The cookies enable the companies to comprehend the search items of the customers and further remind them about the item through the popup ads to attract them. this has eventually lead to a higher rate of sales.

Gender discrimination- it can be perceived that the women are more stalked, intruded in comparison to the males. Here the concept of gender can be taken into the consideration.

CONCLUSION AND RECOMMENDATIONS

In conclusion, it can be said that just like a coin has two sides, similarly the uses of the internet has both the positive and the negative sides. It depends upon the individual o the way they utilize it. The use of the internet has driven the world towards advancement however, it has even become a very easy medium to invade the privacy of others. maintaining privacy is the right of every individual. Therefore, it is highly important to utilize the internet in the correct way instead of considering it as the platform for intrusion in the lives of others.

Recommendations

- It is highly important to have a very strong password
- It is important to use the internet from the right sources and strong internet security services
- The cookies must be cleared
- Only the official sites must be utilized
- Cybersecurity forums must be immediately informed if their privacy is being breached.

REFERENCES

- Berghel, H. (2017). Equifax and the latest round of identity theft roulette. *Computer*, 50(12), 72-76.
- Chen, M., Cheung, A. S. Y., & Chan, K. L. (2019). Doxing: What adolescents look for and their intentions. *International journal of environmental research and public health*, 16(2), 218.
- Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), e1211.
- Dinçer, F. I., Bayram, G. E., & Altunoz, O. (2020). Fourth generation of rights and their reflections on human resources practices in tourism businesses. In *Organizational behavior challenges in the tourism industry* (pp. 60-81). IGI Global.
- Douglas, D. M. (2016). Doxing: a conceptual analysis. *Ethics and information technology*, 18(3), 199-210.
- Filipovski Z. (2017) Transition Process in Southeast Europe and the Protection of the Corpus of Basic Rights and Freedoms, *International Scientific Journal Vision*, 2(1), 23-30.
- Filipovski, Z, A Nuredin A, Sotiroska K, Galetin M, (2018) A Role and Impact of International Organizations in International Relations in the Direction of the Protection of Human Rights and the Rights to the Environment, *International Scientific Journal Vision* 3 (2), 23-35
- Hess, A. N., LaPorte-Fiori, R., & Engwall, K. (2015). Preserving patron privacy in the 21st century academic library. *The Journal of Academic Librarianship*, 41(1), 105-114.
- Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, 30, 1-19.
- Holmes, J. H., Soualmia, L. F., & Séroussi, B. (2018). A 21st century embarrassment of riches: the balance between health data access,

- usage, and sharing. *Yearbook of medical informatics*, 27(01), 005-006.
- Kaley, H., Eagle, M. N., & Wolitzky, D. L. (Eds.). (2020). *Psychoanalytic therapy as health care: effectiveness and economics in the 21st Century*. Routledge.
- Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2020). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, 120426.
- Kshetri, N., & Voas, J. (2018). Cyberthreats under the Bed. *Computer*, 51(5), 92-95.
- Lohani, S. (2019). Social engineering: Hacking into humans. *International Journal of Advanced Studies of Scientific Research*, 4(1).
- Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083), 20160118.
- Naresh, R. (2020). The concept of Privacy and Standardization of Microservice Architectures in cloud computing. *European Journal of Molecular & Clinical Medicine*, 7(2), 5349-5370.
- Nureidin, A (2022). Uluslararası İnsan Hakları Hukuku. *International Vision University Publications*, 110-113
- Nooteboom, L. A., Kuiper, C. H., Mulder, E. A., Roetman, P. J., Eilander, J., & Vermeiren, R. R. (2020). What do parents expect in the 21st century? A qualitative analysis of integrated youth care. *International journal of integrated care*, 20(3).
- Oliveira, L. B., Pereira, F. M. Q., Misoczki, R., Aranha, D. F., Borges, F., & Liu, J. (2017, July). The computer for the 21st century: Security & privacy challenges after 25 years. In *2017 26th*

International Conference on Computer Communication and Networks (ICCCN) (pp. 1-10). IEEE.

Risse, M. (2021). The Fourth Generation of Human Rights: Epistemic Rights in Digital Lifeworlds. *Moral Philosophy and Politics*.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314-341.

Selim A. (2021). Systematic Review of Big Data, Digital Transformation Areas and Industry 4.0 Trends in 2021, *International Scientific Journal Vision*, 6(2), 27-41

Selim A. & Ali İ. (2022). Dijital Okuryazarlık Becerilerinin Kuzey Makedonya'da Yükseköğretim Üzerindeki Etkisi. 6. International Congress of Economics & Business, 81-91

Short, E., Guppy, A., Hart, J. A., & Barnes, J. (2015). The impact of cyberstalking. *Studies in Media and Communication*, 3(2), 23-37.

Soh, C., Connolly, D., & Nam, S. (2018). Time for a fourth generation of human rights. *UN Research Institute for Social Development*, available at <http://www.unrisd.org/TechAndHumanRights-Soh-et-al> (last visited 28 April 2019).

Solove, D. J., & Citron, D. K. (2017). Risk and anxiety: A theory of data-breach harms. *Tex. L. Rev.*, 96, 737.

Syomin, K. A. (2020). Open-source intelligence. *ББК 56я73+ 32.973*, 165.

Valdés, E. (2015). Biolaw, genetic harm and fourth generation human rights. *Boletín mexicano de derecho comparado*, 48(144), 1197-1228.

Weber, R. H. (2015). The digital future—A challenge for privacy?. *Computer Law & Security Review*, 31(2), 234-242.