DATA SECURITY AWARENESS WITHIN THE SCOPE OF DIGITAL PUBLIC RELATIONS PRACTICES AND PRIVACY

Mehmet KARANFİLOĞLU[*]

INTRODUCTION

Public relations (PR) practices vary in parallel with the developments in communication technologies and the progress of web 2.0 and 3.0 technologies and are increasingly acquiring a digital form. Such circumstances bring PR practices to digital platforms, which are currently digital public relations. The concept of digital public relations; effectuates the strategic relationship management goals based on favorable between the organization and its target audiences via digital platforms. Hence, conveying the PR career to the extended reality (XR) -most probably the metaverse- has evolved additionally. On the contrary, the digitalization of everything-things drives all business processes computer-based and refines them in data/info security.

Besides, it requires assessing the consequential data sources consisting of data pools on the axis of privacy. The information collected for PR applications, by all the information produced before, during, and after the application, must be stored and processed within cyber security measures. In this chapter, the subject is studied in-depth and contextualized, considering the information obtained from the literature and recent debates.

[*] Assist. Prof., Ibn Haldun University, Communication Faculty New Media and Communication Department, mehmet.karanfiloglu@ihu.edu.tr

The digitalization process started with the computer-based transformation of numerous known methods, defined as the digitization of information (Ersöz & Özmen, 2020, p. 172). In contrast, digitization is said to be converting analog processes into a digitized format by storing them in a computer environment (Karakaş, Rukancı, & Anameric, 2009). This form enabled the familiar analog processes of the past to be done utilizing computer software. It has resulted in computers and software being seen in many parts of life. The cumbersome structure of analog processes and digital forms has been affected by speed, variety, volume, and accuracy.

For this reason, organizations and sectors have started to use it. In particular, the global economy has become more centralized and widespread due to political and social events. The fact that far eastern countries such as China, India, and Japan gained strength against the developed economies of the past (Ersoy, 2017) in global trade and that human-based processes are increasingly seen as a powerful trump card against the declining population of developed countries has resulted in the importance of digitalization in the eyes of these triple economies. The concept of industry 4.0, named and designed at a fair held in Hannover, Germany, in 2011, has deepened digitalization (DeutscheMesse, 2014). For its part, with the COVID-19 pandemic that appeared in 2019 and impacted the entire world, the need for digitalization of sectors increased due to remote working and curfews.

Digitalization dramatically affects the characteristics of life, and due to the rapid development of technology, the world has had to cope with digitalization. Industries have likewise been a part of this transformation; by digitalization, the sectors have acquired the imperative software applications, transferred all the processes, from internal correspondence to the end-user, into the digital environment, and made the hardware materials compatible with the digital world. Senior management and subordinates had to make heroic efforts in the digital transformation process, which is imperative to promptly provide the necessary equip-

ment and tools and provide the required information effectively. Nevertheless, it would be beneficial to focus on the issue of security by foreseeing the foreseeable problems that may arise from using these systems.

Albeit digital systems are practical implements in many ways, they are susceptible structures in terms of security because much critical information for the sectors is transferred through these systems and stored in them. According to data, by January 2022, 62.5 percent (4.95 billion people) of the eight billion human population are seen as individual internet users (Wearesocial, 2022). Even this data alone can inspire ideas about security issues, and most users of digital systems may not be aware of the risks and threats. Problems created by digital systems can result in economic loss for individuals, allow them to access the information they hold without permission, and cause irreparable damage by deleting or altering that information (Özenç, 2007).

Individual and non-individual factors threaten digital data security. Power, camera system, and switchboard failures due to natural disasters, email, internet banking, online shopping, hardware problems, computer viruses, and abuse of authorized access are just a few. As Wagner and Brooke (2007) stated, human-made threats are fundamental security problems, the weakest link in the chain that creates information security. These threats can appear because users use technology unknowingly or without proper training and deliberately damage the system (Tekerek, 2008). For instance, according to the Internet Security Threat Reports' data published by Symantec (2013) and Sophos (2021), cyber-attacks, spam attacks, phishing attacks, and virus attacks are increasing.

Amidst such threats, the PR profession and its practices are affected by becoming increasingly data-driven. In the PR sector of the world, big data is increasingly being adopted and trying to be the basis for best practices. Accessing, sharing, and using data requires planning. This study discusses data security considerations, which have been studied for years but are now receiving more

attention in PR applications. At a time when the value of information is increasing, it becomes imperative for PR agencies to leverage secure online opportunities in professional practice without becoming a threat to providing specific data security.

Data Security in Cyber-Systems

The issue of data security can be addressed in the context of cyber security. Cybersecurity is a broad topic that includes the constant protection of the confidentiality and integrity of the information and data generated by individuals using the digitization process. The accessibility of data on the internet has made it necessary to take precautions with regard to the given security; therefore, this accessibility has led to crimes such as accessing, stealing, using, or destroying critical essential information from institutions. Data security focuses on the unauthorized performance of these behaviors, which can be considered a criminal offense (EntegreYazılım, 2018).

According to some news in *Hürriyet*, "F- Secure, one of the internet security providers Mikko, Chief Research Officer of Oyj Hypponen, claimed that the Fortune 500 companies with the largest revenues were hacked" ("500ŞirketHacklendi", 2015). As per the news, institutions become more vulnerable to cyber attacks as they transition into cyber environments. The topic of cyber security and data security will be able to present issues about vulnerabilities and threats. As individuals in the digitization process come online through their avatars on the system, their digital twins allow those who are available to survive virtual environments. However, staying in digital environments leads to the daily threat of hacking, data loss, phishing, or cyberbullying. As already existing problems have been observed, data security becomes even more vulnerable.

Conversely, cybersecurity agreements and legal sanctions have been prepared, and numerous cybersecurity system software are designed to protect data for individuals and companies. Smart factories will create cybersecurity software and systems by adopting cybersecurity measures for all their plans. There is

firewall software that existing organizations are currently using. Although this situation offers partial protection, malicious software can be produced for up-to-date security software. For broader aspects, it raises issues such as cyber war, cyber threat, cybercrime, cyber extortion, cyber informatics, cyber sabotage, cyber espionage, and cyber-terrorism.

A review of studies undertaken looking at countries' attitudes on cyber security, software-related security vulnerabilities, leaked information, and cyber threats come to the fore. For example, they are finding a 10-year-old girl with a flaw in the Apple iPhone (Yeni Şafak, 2017), leaking the secret correspondence of countries with Wikileaks (Aydınlık, 2016), and announcing that the USA will consider cyber-attacks a cause of war (Milliyet, 2011), the emergence of the first cyber weapon named Stuxnet (Paksoy, 2012), the Anonymous organization's attack on the Telecommunications Communication Presidency -TIB (NTV, 2011).

Cyber attacks are carried out using two simple methods: DDoS (Distributed Denial of Service) and hacking. With the DDoS attacks, the country's internet system was rendered inoperable in the 2007 attack in Estonia. Sometimes it is carried out as a reactive protest movement: in 2010, DDoS attacks were organized against various ministry websites in Turkey to protest the ban on YouTube (Tufan, 2017). Several security systems have been developed in response: Router, Firewall, Intrusion Detection and Prevention Systems (IDS/IPS), Web Application Firewall (WAF), DDoS Prevention System, and Data Loss Prevention (DLP) (BGASecurity, 2013).

Another problem is that states are known to form hacking teams to fight cybersecurity threats and respond when necessary. Some cyber armies of volunteers and professionals, like the US and North Korea. Meanwhile, countries likewise have cyber security strategies: Canada, Estonia, Germany, the United Kingdom, and Australia. Cyber security will be one of the main areas of discussion. Smart factories, smart cities, innovative education, and other smart technologies that have entered or will enter

personal life with digitization seem to facilitate most of the life process and concisely surround individuals. However, as with any innovative technology, these developments make the issue of security a bit trickier. For example, when surveillance cameras first came out, it was thought that they could effectively solve specific problems such as theft, homicide, and traffic accidents (Silva & Larsen, 2011). Now all crimes are solved by surveillance cameras. However, there are very few areas that do not have surveillance cameras at the level we have today. It brought discussion issues such as the privacy of private life and a panoptic social structure.

Being everywhere has also brought with it the ability to be observed anytime, anywhere. Every step has become traceable, whether in real life or the virtual environment. We discussed these benefits in the previous sections, Big Data Analytics, the Internet of Things, and New Ways to Communicate. However, all the technologies mentioned here still entail security problems.

Digitalization and The End of Privacy

Digitalization has become one of the most important developments of the last century and affects many areas. Experienced digital transformations affect companies, brands, and institutions as well as societies. There is a digitalization effect in many fields such as economy, politics, and education, and the only common point of the changes in these fields, which differ according to job status and industry, are digital transformations. All public institutions, private or official organizations that realize these transformations have become a branch of the digital world (Şahinaslan & Şahinaslan, 2018, p. 423). Digitalization directs companies to change and manage this change to the conditions of the age.

The concept of digitalization is affecting all sectors with its increasingly popular effect. In this respect, unique digitization methods can be found in every industry. In general, digitization refers to becoming computer-based. Because of this, many processes performed with computer hardware and software can be

overlooked by digitization. Other concepts are proposed from this point of view: Industry 4.0. In Industry 4.0, many hardware and software transformations for the dehumanization of factories and artificial intelligence and autonomous robots to work with the dark factory model within the factory are expressed.

In this private space, which lies outside the social sphere, the individual freely decide where, when, and how to communicate with other people. Their criteria and value judgments govern the dominance of individuals in this area. This situation, i.e., the differentiation of the understanding of privacy from one individual to the next, further blurs the boundaries of privacy (Uğurlu, 2018, p. 258). *Privacy* is a concept brought to the fore by the reality of the individual, sociocultural, economic, and political developments, along with 19th-century enlightenment philosophy and modern understanding of science (Yılmaz, 2012, p. 249). In addition to philosophy and law, the concept of privacy has changed over time, society and culture. The idea of privacy has been, and continues to be, widely debated with individuals' widespread use of the internet and, primarily, social media. However, privacy debates are raging across generations because of their varying degrees of use of social media. Today, as the distinction between private and non-private has become increasingly uncertain, it has become more difficult for people to define their privacy boundaries. People who use social media intensively are not afraid to share topics, information, and images that many people consider private in these media.

Privacy is a fundamental human right. It forms the basis for rights such as freedom of association and freedom of expression that support human dignity. The concept of privacy is an essentially modern human right. Then again, privacy is one of the most challenging concepts to define of all human rights. Although definitions of privacy differ in many contexts, widespread reports of privacy in law focus on physical, regional, information and communications privacy. As a concept, privacy refers to a realm in which people can be alone, think, act, and decide what boundaries they set for relationships and communication with

others (Yüksel, 2003, p. 182). In this context, the right to privacy can be understood as the right of individuals to determine the extent to which they share their living space with others.

The techniques and analysis that have emerged with big data applications show that traditional methods of protecting the privacy of individuals will no longer be effective. In this direction, many countries are developing laws and regulations regarding data protection and confidentiality. These privacy laws focus on individual consent and the collection of personal information. However, that is no longer enough these days. Because individual assistance in collecting personal information is provided during data collection, much of the information used in online procedures may contain important notices for individuals while not linked to personal information. At this point, personal data may be obtained, consistent with the interpretation of the data collected, through methods such as recording online behavior and keeping log records (Tan & Pivot, 2015, p. 860). This situation raises concerns about the protection of privacy. A closer examination of the literature reveals the privacy concerns of individuals. Several studies have examined the lack of knowledge about the subject, and the thought that individuals do not have control increase privacy concerns (Dinev & Hart, 2005; Dwyer, Hiltz, & Passerini, 2007; Goettke & Christiana, 2007; Miltgen, 2009; Ridley-Siegert, 2015; Tan & Pivot, 2015). The students are further analyzed in studies on the topic. In related research, while students' awareness of privacy concerns and Facebook usage is high, and they are aware of the potential consequences of sharing personal information, they feel comfortable enough to use personal information on these platforms (Govani & Pashley, 2014).

It is pretty surprising that online social networking studies challenge the common assumption that young people do not protect their confidential information. Research shows that young people employ various self-developed protective strategies in these environments. These strategies include using pseudonyms and providing false information, accessing personal profiles, setting privacy controls, limiting friend requests, and

deleting tags and photos (Boyd & Hargittai, 2010; Miltgen & Peyrat-Guillard, 2014; Young & Quan-Haase, 2013).

The fact that data become personal data or represents a specific person can only be unavoidable during data processing. Processing of personal data includes processes such as collecting, recording, editing, adapting, transforming, using, explaining, combining, and deleting data (Kaya, 2011). According to the Organization for Economic Co-operation and Development (OECD), the principles to be considered in the protection and processing of personal data, published in 1980 and updated in 2013, are (2013):

- Irritability
- Quality
- Purpose Specificity
- Usage Limitation
- Security
- Openness
- Consent of the Individual
- Accountability

Although the protection of personal data is a topic that has been studied for a long time, with the rapid development of technology, the topic has started to be interpreted from different perspectives by changing its dimension. Personal data protection has gained international importance due to global data movements and traffic between countries (Akıncı, 2017, p. 2). In addition, efforts by countries to bring their legal infrastructures into line with technological developments have increased in recent years.

In the processes experienced, the existence of individual and societal defense mechanisms against threats to personal data gains in value. The protection of personal data is fundamental to the right to respect for private and family life. Personal data protection is interpreted in international documents with data protection regulations. Confidentiality, the confidentiality of private life, and international laws regarding personal data are monitored as follows:

First, we see that *Article 12* of the *United Nations Universal Declaration of Human Rights* was issued in 1949. *Article 17* of the *United Nations Covenant on Personal and Political Rights* was also regulated in 1966 as a right to privacy. The *OECD* published the text titled "*Guiding Principles on the Protection of Privacy and Transboundary Data Flow*" in 1980. The other is defined in *Article 8* of the *Council of Europe's European Convention on Human Rights* as the right to respect for private and family life. *The European Union Directive No. 95/46* on the protection of natural persons with regard to the processing of personal data and on the free movement of such data guarantees the same protection of personal data in every member country. Finally, the European Parliament passed the General Data Protection Regulation (GDPR) on April 14, 2016, (Eroğlu, 2018, p. 135).

In addition, there are some other regulations in Turkey, which can be summarized as follows: *Articles 20, 21* and *22* of the *Turkish Constitution* regulate the title of "*Privacy and Protection of Private Life.*" *Article 24* of the "*Turkish Civil Code*" contains regulations regarding the right to privacy. The 21st Article of the "Acquisition of Information Law" regulates privacy-related matters. *Articles 10, 125, 134, 135, 136, 137* and *280* of the "*Turkish Penal Code*" contain privacy regulations. In 2016, the law study on the subject was completed. "*Personal Data Protection Law No. 6698*" was published in the Official Gazette dated 7 April 2016, numbered 29677 and entered into force (Eroğlu, 2018, p. 135).

Digital Public Relations Practices and Privacy

The view of PR as a profession aligns with the 1900s. Although the activities of Phineas Taylor Barnum previously formed the basis of public relations, it flourished in 1906, owing to Ivy Ledbetter Lee, a journalist, and advisor of John Davison Rockefeller (Tortop, 1993, p. 13-14). In 1916, he founded his first PR office, and in this agency, he used truthful communication as a public relations method. In this direction, the agency used "Accuracy, Authenticity and Interest" as its slogan (Turney, 2015).

Another critical name was Edwards Bernays in 1913. Bernays' most significant job was to increase public support for the United States Administration's entry into World War I (Şen, 2012, p. 67). Over time it has developed and changed professionally in PR. According to Grunig and Hunt (1984), public relations practices can be examined in four different models: Press agentry/publicity (1850-1900), public information (1900-1920), two-way asymmetrical communication (1920 and later), two-way symmetrical communication (the late 1960s and after 1970).

As in other areas, pacing with the latest technology world is also an essential topic in PR. The internet has enormous potential for PR and other communication disciplines and has become a strategic tool for PR departments. PR professionals can leverage the wired global village for instant, engaging, and persuasive communications. Generally speaking, while traditional public relations practices persist today, the internet brings new tools and conveniences to the public relations field. PR practices in the digital environment represent a communication opportunity (Petrovici, 2014, p. 80). In other words, *digital public relations* is the management of communication between an organization and its stakeholder, target group, target audience, and the public through internet applications. In addition, digital public relations is the state of the art of PR in digital media (Sönmez, 2020, p. 188).

The historical development of PR has significantly influenced the design of today's modern and digital approaches. Today, the Public Relations Association of America (PRSA) defines the term as a strategic communication process that builds mutually beneficial relationships between organizations and their public (PRSSA, 2022). Due to the digital transformation, technological developments have led to an increase and spread of production; Changing the balance between supply and demand in the opposite direction has played a role in the emergence of the latest information economy and the path leading to PR digital outreach. Digital transformation affects all sectors, including public relations. The increase in the value of information, the replacement

of personal computers with smartphones, the shift to phone applications instead of programs, and the rise of new media platforms have all led to the emergence of digital data. Companies with intellectual and property rights to the new generation of digital products, where production has left technology and information to their own devices, have experienced a profound change in the entire business world (Ljungqvist & Wilhelm-Jr, 2003) that has led to the accumulation of data in heaps and the developments called Big Data.

The process of converting big data, confidential and raw data groups into helpful information and then analyzing it is done automatically with programs and techniques and offers benefits in many areas based on the authority the technology confers (Taşçı & Şamlı, 2020, p. 89). This data is growing, and much vital information for companies is embedded in the resulting mountains of data. The economic value of significant data increases when it is made meaningful with current processing techniques such as statistics, data mining, artificial intelligence, machine learning, and deep learning. Acting on this data has become a necessity for PR.

Thanks to this data, organizations; can identify the wants, needs and expectations of their target groups through research and produce different products, services and experiences of their competitors. While PR professionals listen to the wants and needs of audiences and individuals, their digital expectations must also be considered. Ultimately, it is crucial for organizations to meet these PR expectations on the road to reputation (Barnett, Jermier, & Lafferty, 2006). By reinforcing the perception that institutions provide value, corporate reputation has attracted various academic disciplines' attention and has increasingly become focused (Chun, 2005; Gotsi & Wilson, 2001).

The work and tasks of PR agencies and experts are increasing and diversifying with the new generation, digital applications, and business understandings. Nowadays, in PR there are activities aimed at informing the public about a company's products, services and activities, changing attitudes and behavior, raising

awareness and creating selective perception, in addition to some basic company actions like the uphold the company's existence, corporate culture and philosophy. Implementation of printed, visual and digital activities to characterize and fulfill all types of activities, creating a trusted brand, proceeding with the marketing public relations activities and social media management in line with the expectations of target groups and stakeholders, in accordance with the company's goals, vision and mission are some of the recent PR assignments (Newsom, Turk & Kruckeberg, 2012).

Defining and maintaining processes based on the information and digital applications for *digital public relations* studies has become essential to PR processes. Individuals, who are the target audience of PR agencies and the companies they serve, are no longer passive in the communication established with them by the institutions; they are not only the crowd who receive the messages sent and act accordingly. They have become sources that follow all kinds of data and produce their data. With web 2.0 technology, individuals have become able to interact with institutions through smartphone applications, and institutions' reputations are built on sensitive ground, on much more diverse issues and individuals who may take immediate action.

At the same time, these people use digital communication channels to obtain more information about products and services than is provided. Additionally, the businesses that individuals may reach not only know what type of product or service they are responding to what needs; Based on the technical information, comparative comments, likes and complaints about the products, how well they satisfy other consumers and whether they engage in legal or unethical activities.

In the new digital universe, the fact that individuals can switch digital services and products very quickly means that they can easily switch from one product and service to another, adding new dimensions to the selection criteria for comparable products and services (Whitten & Leidner, 2006). This situation requires that institutions need more digital public relations

practices. Due to the nature of PR, as the crowds change, there is a need for the use of new tools. Therefore, the earlier and faster institutions implement new communication technologies, the greater their competitive advantage (Özpınar, 2021).

Though, the digital transformation brings the amount of data produced to step values that cannot be expressed with numbers known at the standard level. Instead of numbers, the quantities are difficult to understand because of the zeros in them. According to the calculations, an average of 2.5 quintillion data is produced daily. Google processes more than twenty petabytes of data daily, and about 3.5 billion searches are performed. Currently, as of 2020, there are forty-four zettabytes of data (Vuleta, 2021).

Cyber-physical systems, autonomous robots, three dimensions (3D) printers, artificial intelligence, big data, the internet of things (IoT), wearable technologies, augmented virtual reality technologies, metaverse and other online platforms open the doors for new PR applications, and this leads to more data production and consumption. This large amount of data created and consumed has become too large to be managed with traditional internal data storage and processing systems, and requires specialized hardware, software, and processes to store and manage it. According to data from 2020, data production was more than 118.8 zettabytes, and it showed that users store this data at a rate of two percent. However, by 2025, the amount of data produced is expected to reach 180 zettabytes, and the data storage business is expected to grow by 19.2 percent (Petrov, 2022). These modern technologies listed above are fundamental for organizations, individuals, businesses, communities, and governments as they have started to be at the center of any digital transformation (Manyika, et al., 2011).

Both the regulations on the protection of personal data and the preferences of individuals, cyber security approaches, producing information from data, using big data in PR processes, "generating knowledge from big data is a demanding, complex process" (Wiencierz & Röttger, 2019) optimizing all these changes and requirements, and ensuring that it is ergonomic and

usable for all stakeholders in the ecosystem is a challenging and complex process. Data from PR and corporate communication agencies, internal communication data and feedback from the company's communication channels, publicly shared data, and PR data derived from events and sponsorships.

This data can also be incorporated into many digital public relations applications. Additionally, user information, referred to as a digital footprint in digital public relations, may consist of content such as social media statistics that may directly concern PR specialists (Wright & Hinson, 2008). In addition to this data, there is data from the company's communication channels (first-party), competitors' marketing and advertising activities (second-party), and social media (third-party) (Weiner & Kochhar, 2016, p. 8). This data can be used to analyze audience behavior and preferences. Studies can be conducted to change user knowledge, attitudes, and behavior in digital public relations and to raise awareness of corporate social responsibility activities, crisis management, image management, reputation management, and social media management. This data can be used to develop digital PR strategies in the field. In general, the tools used in digital outreach are listed as follows (Tanyıldızı, 2021, p. 52-75):

- Wikis
- Blogs and corporate blogs
- Microblogs
- Forums
- Social bookmarks
- Podcasting
- Social networks:
  - Facebook
  - Twitter
  - Instagram
  - LinkedIn
  - YouTube
- Corporate websites

A strategic digital public relations application may be realized by disclosing the statistical data, correlations, or trends created from the traces left by the users in digital public relations studies (Stacks, 2016).

As can be seen, when PR is considered from the perspective of digital transformation, data emerges as the number one element. While performing digital transformation in an environment where such data is produced, data privacy and security have likewise become essential concepts. Regardless of the subject, users have become more conscious and sensitive about protecting their data in the digital environment. As with the actions conducted on social media, digital public relations applications try to collect data in the background. This data and its use; policy changes in the organization's strategy determination and activities are effective on significant financial results such as market share for organizations.

In 2021, the WhatsApp instant communication application operating under Meta (Formerly Facebook) announced that it would adjust the data processing policies, and its users reacted to this (Wijoyo, Limakrisna & Suryanti, 2021). Meanwhile, security-related problems and information leaks may leave institutions in a challenging situation. An example is a hacking attack that Apple experienced in the iCloud service in 2014 and the subsequent leaking of privileged information (Kovach, 2014). Data usage comparisons later with alternative applications revealed the importance of long-lasting differences in perspective and personal data security (Sindermann, Lachmann, Elhai & Montag, 2021).

With these processes, the concept of data governance is also evolving, which includes storing, protecting, viewing, using, modifying and processing data obtained only from the owner and authorized parties, and many studies have been conducted on the subject (Khatri & Brown, 2010). Based on these studies, the privacy issue is a critical topic of discussion.

The issue of data protection can be one of the topics of discussion in relation to digital public relations. Apart from unlimited storage of information using Internet technologies, the features

of some applications violate users' privacy. The software developed is offered for use with backdoors so that future problems can be solved more easily. These backdoors not only interfere with the application but also allow users' movements within the application to be viewed (Öztekin & Öztekin, 2010, p. 536). While applications developed for free make everyday life easier for users, they create themselves a database with the information entered during registration and access to the content on the phone. Surveillance and privacy are two related phenomena. When privacy is violated, there must be an act of surveillance. Although data breaches have been critical in surveillance from ancient times to the present day, the structure of surveillance has changed in tandem with developments in business, information, and, most importantly, technology. This change has brought a different meaning and perspective to the violation of restricted areas. Today, the sense of surveillance and control has increased, and modern people have started to have less privacy (Langenderfer & Miyazaki, 2009, p. 381).

Sharing based on user claims in digital environments can allow data to spread unchecked. While making this data public makes it copyable or usable, it can simply pose serious legal problems. Individuals may knowingly or unknowingly collect personal information through digital platforms. A study conducted at the University of North Carolina found that 96.2% of teens disclosed their birthday, 83.2% their relationship status, 74.7% their political views, and 16.4% their cell phone number (Tüfekçi, 2008, p. 23). Although the data shared with other users may seem harmless, websites ask for information such as date of birth or mobile phone to change passwords; There are severe problems with virtual cheating. Individuals may face negative consequences related to cyberbullying as a result of this information.

CONCLUSION

The topic of data protection is becoming increasingly important alongside the topic of data security. Data protection is an issue that is particularly important for both individuals and insti-

tutions and must be taken seriously. Technological developments that are the result of Big Data and other digitization are leading to enormous increases in data production worldwide. It is about the security and protection of the storage, processing and evaluation of this data for various purposes related to data security.

As in other professions, PR has acquired a digital form in which the internet and its applications are used to get its share of digitization. The presence of the masses in the new media increases data production and enables the realization of digital applications in public relations. PR specialists will hardly have competent people to manage these applications via digital platforms. It is undeniable that in the future there will be a need for PR specialists who are experts in digital predisposition and data security. Because in a world where cyber wars are gaining momentum, caution against situations that could throw institutions into trouble in both legal and practical areas is a crucial issue for both organizations and PR professionals.

This study discusses the topic of data security in the context of cybersecurity from a PR perspective and in relation to data protection. There is a need for qualitative and quantitative studies on this topic. Many studies are conducted based on this information. The future of practical and strategic communication studies is made possible by addressing digital security issues. In this respect, unfamiliar problems await the PR specialists of the future, which need to be solved with significantly more complex and step-by-step applications. This is something that should be borne in mind in future studies.

REFERENCES

"500ŞirketHacklendi". (2015, Ekim 27). *Hürriyet Ekonomi*. Retrieved from Hürriyet Gazetesi: http://www.hurriyet.com.tr/ekonomi/500-sirket-hacklendi-30383340

Akıncı, A. N. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün getirdiği yenilikler ve türk hukuku bakımından değerlendirilmesi.* İkdisadi Sektörler ve Koordinasyon Genel Müdürlüğü. T.C. Kalkınma Bakanlığı. Retrieved from http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf

Aydınlık. (2016, Ekim 4). *Aydınlık Gazetesi*. Retrieved from "Wikileaks tarafından açıklanan 10 büyük sır": https://www.aydinlik.com.tr/wikileaks-tarafindan-aciklanan-10-buyuk-sir

Barnett, M. L., Jermier, J. M., & Lafferty, B. A. (2006). Corporate reputation: The definitional landscape. *Corporate Reputation Review, 9*(1), 26–38.

BGASecurity. (2013). *Gerçek dünyadan siber saldırı örnekleri*. Retrieved from https://www.bgasecurity.com/makale/gercek-dunyadan-siber-saldiri-ornekleri/

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares?. *First Monday, 15*(8). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/3086

Chun, R. (2005). Corporate reputation: Meaning and measurement. *International Journal of Management Reviews, 7*(2), 91–109.

DeutscheMesse. (2014, April 2). *Hannover Fuarı'nda endüstri 4.0*. Retrieved from deutschland.de: https://www.deutschland.de/tr/topic/ekonomi/kuresellesme-ulusiararasi-ticaret/hannover-fuarinda-endustri-40

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29. doi:10.2753/JEC1086-4415100201

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of facebook and myspace. *13. AMCIS 2007 Proceedings*, (p. 71-110). Keystone: Colorado.

EntegreYazılım. (2018, Mart 25). *Veri Güvenliği*. Retrieved from Entegre Yazılım: https://www.entegreyazilim.com.tr/veri-guvenligi

Eroğlu, Ş. (2018). Dijital yaşamda mahremiyet (Gizlilik) kavramı ve kişisel veriler: Hacettepe Üniversitesi bilgi ve belge yönetimi bölümü öğrencilerinin mahremiyet ve kişisel veri algılarının analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi, 35*(2), 130-153. doi:10.32600/huefd.439007

Ersoy, A. R. (Director). (2017). *Endüstri 4.0 (D)evrimi yolunda* [Motion Picture].

Ersöz, B., & Özmen, M. (2020). Dijitalleşme ve bilişim teknolojilerinin çalışanlar üzerindeki etkileri. *AJIT-e: Bilişim Teknolojileri Online Dergisi, 11*(42), 170-179. doi:10.5824/ajite.2020.03.007.x

Goettke, R., & Christiana, J. (2007). Privacy and online social networking websites. in M. D. Smith, J. Waldo, A. Rosen, & A. Friedman, *Computer Science 199r: Special Topics in Computer Science Computation and Society* (pp. 1-13). doi:10.1.1.92.1380

Gotsi, M., & Wilson, A. M. (2001). Corporate reputation: Seeking a definition. *Corporate Communications: An International Journal, 6*(1), 24-30. doi:10.1108/13563280110381189

Govani, T., & Pashley, H. (2014). Student awareness of the privacy implications when using Facebook. *Cyberpsychology, 8*(2), 1-17. Retrieved from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

Grunig, J. E., & Hunt, T. (1984). *Managing public relations*. New York: Holt, Rinehart & Winston.

Karakaş, S., Rukancı, F., & Anameriç, H. (2009). *Belge yönetimi ve arşiv terimleri sözlüğü*. Ankara: Devlet Arşivleri Genel Müdürlüğü.

Kaya, C. (2011). Avrupa Birliği veri koruma direktifi ekseninde hassas veriler ve işlenmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 69*(1), 317-334.

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM, 53*(1), 148–152.

Kovach, S. (2014, September 3). *We still don't have assurance from apple that icloud is safe.* Retrieved from businessinsider.com: https://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *The Journal of Consumer Affairs*, 380-388.

Ljungqvist, A., & Wilhelm-Jr, W. J. (2003). IPO pricing in the dot-com bubble. *The Journal of Finance, 58*(2), 723–752. Retrieved from http://www.jstor.org/stable/3094556.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung-Byers, A. (2011). *Big data: The next frontier for innovation, competition, and productivity.* McKinsey Global Institute.

Milliyet. (2011, Haziran 1). *"ABD siber saldırıları 'savaş sebebi' sayacak".* Retrieved from Milliyet Gazetesi: http://www.milliyet.com.tr/abd-siber-saldirilari-savas-sebebi-sayacak/dunya/dunya-detay/01.06.2011/1397381/default.htm

Miltgen, C. L. (2009). Online consumer privacy concern and willingness to provide personal data on the internet. *International Journal of Networking and Virtual Organizations, Indersciences, 6*(6), 574-603.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103-125. doi:10.1057/ejis.2013.17

Newsom, D., Turk, J., & Kruckeberg, D. (2012). *This is PR: The realities of public relations.* Boston MA: Wadsworth Cengage Learning.

NTV. (2011, Haziran 8). Anonymous TİB'e saldırdı! Retrieved from https://www.ntv.com.tr/turkiye/anonymous-tibe-saldirdi,OsGUZfEn50SCXCLVyGOIfg

OECD. (2013). *New data for understanding the human condition: International perspectives.* OECD. Retrieved from https://www.oecd.org/sti/inno/new-data-for-understanding-the-human-condition.pdf

Özenç, K. (2007). Bilgi ve iletişim teknolojilerinde kişisel ve kurumsal bilgi güvenliğinin sağlanması. *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı.* Ankara.

Özpınar, Ş. B. (2021). Yeni teknolojiler ve kurumsal iletişimin yeni araçları. *Etkileşim, 7*, 150–168.

Öztekin, H., & Öztekin, A. (2010). Modernleşme-mahremiyet ilişikisi ve siber mekanda mahremiyetin aleniyete dönüşmesi. *NWSA: e-Journal of New World Sciences Academy, 5*(4), 526-540.

Paksoy, M. (2012, Ocak 24). *Teknoloji oku.* Retrieved from İlk Siber Silah : Stuxnet !: https://www.teknolojioku.com/guvenlik/ilk-siber-silah-stuxnet-5a28f28f18e540630d1ce10a

Petrov, C. (2022, June 22). *25+ Impressive big data statistics for 2022*. Retrieved from techjury.net: https://techjury.net/blog/big-data-statistics/#gref

Petrovici, M. A. (2014). E-Public relations: Impact and efficiency. *A case study. Procedia-Social and Behavioral Sciences, 141*, 79-84.

PRSSA. (2022, June 20). *Learn about public relations*. Retrieved from prsa.org: https://www.prsa.org/prssa/about-prssa/learn-about-pr

Ridley-Siegert, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice, 17*, 30-35. doi:10.1057/dddmp.2015.40

Silva, B. v., & Larsen, T. (2011). *Setting the watch: Privacy and the ethics of CCTV surveillance*. Hart Publishing.

Sindermann, C., Lachmann, B., Elhai, J. D., & Montag, C. (2021). Personality associations with whatsapp usage and usage of alternative messaging applications to protect one's own data. *Journal of Individual Differences, 42*(4), 167-174. doi:10.1027/1614-0001/a000343

Sophos. (2021). *Sophos 2022 Threai Report: Interrelated threats target an interdependent world*. Sophos ltd. Retrieved from https://assets.sophos.com/X24WTUEQ/at/b739xqx5jg5w9w7p2bpzxg/sophos-2022-threat-report.pdf

Sönmez, H. Ş. (2020). Dijital ortamda yapılan halkla ilişkilerin bir aracı olarak kurumsal bloglar: 2019 yılı türkiye'nin en değerli 25 markası üzerine bir inceleme. *Kocaeli Üniversitesi İletişim Fakültesi Araştırma Dergisi, 16*, 185-207.

Stacks, D. W. (2016). *Primer of public relations research* (Third Edition ed.). New York: Guilford Press.

Symantec. (2013). *Internet security threat report*. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

Şahinaslan, E., & Şahinaslan, Ö. (2018). E-dönüşüm uygulamalarında güvenlik. *Proceedings of the International Congress on Business and Marketing*, (pp. 420-435).

Şen, F. (2012). Kamu yönetiminde halkla ilişkileri yeniden düşünmek. *Akdeniz İletişim Dergisi, 16*, 63-79.

Tan, Q., & Pivot, F. (2015). Big data privacy: Changing perception of privacy. *2015 IEEE International Conference on Smart City/SocialCom/SustainCom together with DataCom 2015 and SC2 2015*, (pp. 860-865). Retrieved from 10.1109/SmartCity.2015.176

Tanyıldızı, N. İ. (2021). *Dijital dünyada halkla ilişkiler*. Ankara: İksad Yayınevi.

Taşçı, M. E., & Şamlı, R. (2020). Veri madenciliği ile kalp hastalığı teşhisi. *Avrupa Bilim ve Teknoloji Dergisi*(Özel Sayı), 88-95.

Tekerek, M. (2008). Bilgi güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi, 11*(1), 132.

Tortop, N. (1993). *Halkla ilişkiler*. Ankara: Yargı Yayınları.

Tufan, O. (2017, Ekim 21). *Ddos nedir?*. Retrieved from Shift Delete: https://shiftdelete.net/ddos-nedir

Turney, M. (2015). *Foreshadowing the explanatory and the mutual satisfaction phases of public relations, Ivy Lee was decades ahead of his contemporaries*. Retrieved

from Online Readings in Public Relations by Michael Turney: https://www.nku.edu/~turney/prclass/readings/3eras2x.html

Tüfekçi, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science Technology & Society, 28*(1), 20-36. doi:10.1177/0270467607311484

Uğurlu, S. (2018). Dijital PR ve itibar yönetimi açısından sosyal medyada kriz yönetiminde bir vaka incelemesi: "Üsküdar belediyesi - Kedi Evi" projesi. *İnsan & İnsan, 5*(17), 233-248. doi:10.29224/insanveinsan.417128

Vuleta, B. (2021, October 28). *How much data is created every day? [27 Staggering Stats].* Retrieved from SeedScientific.com: https://seedscientific.com/ how-much-data-is-created-every-day/#:~:text=Every%20day%2C%20we%-20create%20roughly%202.5%20quintillion%20bytes%20of%20data.

Wagner, A. E., & Brooke, C. (2007). Wasting time: The mission impossible with respect to technology-oriented security approaches. *Journal of Business Research Methods, 5*(2), 117-124.

Wearesocial. (2022). *Digital 2022 global overview report.* England: We Are Social Ltd.

Weiner, M., & Kochhar, S. (2016). *Irreversible: The public relations big data revolution.* IPR: Institute for Public Relations. Retrieved from https://instituteforpr.org/irreversible-public-relations-big-data-revolution/

Whitten, D., & Leidner, D. (2006). Bringing IT back: An analysis of the decision to backsource or switch vendors. *Decision Sciences, 37*(4), 605–621.

Wiencierz, C., & Röttger, U. (2019). Big data in public relations: A conceptual framework. *Public Relations Journal, 12*(3), 1–15.

Wijoyo, H., Limakrisna, N., & Suryanti, S. (2021). The effect of renewal privacy policy whatsapp to customer behavior. *Insight Management Journal, 1*(2), 26–31.

Wright, D. K., & Hinson, M. D. (2008). How blogs and social media are changing public relations and the way it is practiced. *Public Relations Journal, 2*(2), 1–21.

YeniŞafak. (2017, Kasım 16). *"Apple'ın en güvendiği teknolojinin açığını 10 yaşındaki çocuk buldu".* Retrieved from Yeni Şafak Gazetesi: https://www.yenisafak.com/teknoloji/applein-en-guvendigi-teknolojinin-acigini-10-yasindaki-cocuk-buldu-2810460

Yılmaz, A. (2012). Sosyal medya kullanımında güncel tartışmalar: üniversite öğrencileri örneğinde mahremiyet- kamusal alan ilişkisi. *Global Media Journal, 3*(5), 246-264.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society, 16*(4), 479-500. doi:10.1080/1369118X.2013.777757

Yüksel, M. (2003). Mahremiyet hakkı ve sosyo - tarihsel gelişimi. *Ankara Üniversitesi SBF Dergisi. 58*(1), 181-213. doi:10.1501/SBFder_0000001619