DIGITAL LITERACY IN INCREASING DATA SECURITY: AN EVALUATION FROM THE COMMUNICATOR'S PERSPECTIVE

Mehmet KARANFİLOĞLU[*]

INTRODUCTION

Many communication means persistence in changing both individual and corporate lives. From the communication perspective, utilizing these tools is vital regarding the tools' diversity and users. However, this diversification in information communication technologies likewise creates tremendous data production. These data, produced in massive quantities, are circulated in the internet universe uncontrollably, driving info and data security-sensitive. When considered from a communicative point of view, digital literacy emerges from applying basic security steps for the privacy and protection of this data digital literacy guides in using these media tools and shows how to use these tools more safely. Therefore, accurate reading and proper use of digital media tools emerge as essential elements in data security, communication process continuity, and cybercrime prevention. This chapter aims to reveal these concepts, relations, and concerns about how communicative activities shall be overseen by assembling securer data usage from the digital literacy perspective.

Although the digitalization process has become noticeable in the last few years, a process in the 1960s shall be mentioned; in

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

this process, many philosophers and theorists have focused on this issue and discussed some consequences. The world has become globally interconnected; Dijk claims developing countries have converted to a network society with the rapid spread of satellite television, mobile phones, and the internet and defines the 21st century as the "age of networks" (Dijk, 2016, p. 13).

The time when increasing data production with technology is widespread is named the post-industrial information society (Daniel Bell), information society (Alvin Toffler), global village (Marshall McLuhan), and some technologies produce and rapidly disseminate information as advanced technology. Castells points to this structure in conceptualizing the post-industrial information and network society. As the most effective means of transmission, the internet is the system that establishes a link between the network society and the information society. Transitioning from the industrial society to the information age, Castells states that new communication technologies accelerate globalization with fast and simultaneous communication by eliminating space. According to Castells, power relations are the basis of society in which power is used through networks. Accordingly, he discusses four different forms of power under social and technological conditions (Castells, 2011, p. 773):

1. Networking Power
2. Network Power
3. Networked Power
4. Network-making Power

For its part, the ability to understand, interpret and reproduce incoming information is related to literacy. While the process of understanding information brings the concept of literacy to the agenda, it is evident that many types of literacy gain paramountcy today; however, digital literacy is at the forefront of digital transformation and its benefits. The concept of *digital literacy* explains the competence of using tools so that the individual may search for and find accurate, reliable, scientific information sources.

Furthermore, individuals may analyze and synthesize the acquired information and their ability to think critically through network devices such as smartphones, tablets, laptops, and desktop computers. It includes finding, understanding, analyzing, producing, and sharing information. Technology and the new communication tools very popular in today's society are the actors of a parallel world living with humanity (Artut, 2014, p. 12).

It is not possible to discuss a single type of literacy today; the concept of literacy is increasingly referred to as digital literacy, media literacy, technology literacy, health literacy, internet literacy, risk literacy, computer literacy, environmental literacy, economic literacy, legal literacy, cultural literacy, intercultural literacy, political literacy. In addition, many other types of literacy have been popularized recently, such as consumer literacy, critical literacy, moral literacy, civic literacy, and web literacy (Kurbanoğlu, 2010, p. 739).

This study discusses digital literacy and other related literacy types as well as privacy and data security from a communication perspective.

The Future of Communication and Digital Literacy

As technology develops, the subject of communication becomes increasingly central; by digitalization, the consequence of communication has become more comprehensible than ever afore. Notwithstanding, some skills have lustered as humanity recenter; due to the rapid change and technological transformation, the skills that individuals need to acquire have undergone a significant difference compared to the last century (Ala-Mutka, 2011; Dede, 2010). These skills are believed to contain much information about what may happen in the future in communication; along with the changing skills, there has been a shift in the perception of traditional literacy defined in the middle of the 20th century, and alternative and contemporary literacy concepts have been replaced (Condy, Chigona, Gachago, & Ivala, 2012).

Literacy status indicates how many individuals have these skills, and having sufficient knowledge in terms of literacy brings along the ability to use communication technologies effectively and strategically. Previously, the definition of the traditional literacy concept and the primary purpose of non-formal education systems was to equip students with reading and writing skills in their mother tongue; this purpose began to be questioned in the middle of the 20th century (Kurt, Orhan, Yaman, Solak, & Türkan, 2014). When it comes to literacy, much more complex processes are on the list, conversely, many types of it are noted to define literacy more accurately.

With the emergence of digitalization since the 1960s, many concepts have emerged, such as computer literacy, *digital literacy*, information literacy, technology literacy, and information and communication technologies literacy, which are based on various cognitive, affective, and psychomotor competencies, especially technology and literacy skills (Leaning, 2019). In the 2010s, we encounter the concept of digital literacy with the increasing level of technological maturity and the effect of digital transformation along with other global factors. Eshet-Alkalai (2004) provides a conceptual framework that defines digital literacy as a compilation of five diverse types of literacy: photo-visual, reproductive, information, branched, and socio-emotional literacy. Nonetheless, when digital literacy is mentioned, some other concepts should be known; computer literacy, technology literacy, and media literacy. These three definitions of literacy are related to each other by reason of the fact that is knowing all three shall be considered as completing a part of a triple trivet. According to Oliver and Towers (2000), computer literacy has long been expressed as people's predisposition to their ability to use computers and information technologies by the definition of media literacy made by Aufderheide (1993). Accordingly, *media literacy* is defined as an individual's ability to decipher printed and electronic media tools, evaluate the data there, analyze these data, and produce data suitable for these media organs. Technology

literacy, in other respects, has been a catalyst that includes human cognitive and psychomotor skills for the last ten years (Crowe, 2006). According to another definition, it is a way of thinking about how technology may become a tool to solve any problem (Herman, Maknun, Barliana, & Mardiana, 2019). Technology literacy is used, managed, evaluated, and understood by technology (ITEEA, 2000).

With the use of digital language in all communication technologies, there are three essential features of new media technologies that enroll personal lives: interaction, demassification, and asynchrony (Rogers, 2003). From this point of view, it is possible to make some predictions about digital literacy; however, there are many uncertainties in the definition of digital literacy (Eshet-Alkalai, 2004; Bawden, 2008). Forasmuch as the question of what digital components are may differentiate the meanings. Experts (Eshet-Alkalai & Amichai-Hamburger, 2004; Bawden, 2008) recommend many digital literacy components (Perdana, Yani, Jumadi, & Rosana, 2019). In this context, it is possible to consider digital literacy from various aspects.

Alkalai and Hamburger (2004) define digital literacy as photo-visual, reproduction, branching, information, and socio-emotional skills. Honan (2008) states that these skills; that breaking the code of texts is defined as participating in the meaning of the texts using the texts functionally, critically analyzing, and transforming the texts. Hague and Payton (2010, p. 19) define digital literacy more comprehensively with eight skill areas: functional skills, creativity, critical thinking and evaluation, cultural and social understanding, collaboration, finding and selecting information, effective communication, and e-safety. Hobbs, on the other side, approaches the subject from another angle. Hobbs (2010, p. 7) mentions that digital and media literacy must be combined, and education must be given in schools. Based on this, individuals who have media and digital literacy skills; are people who may access and share information through research, evaluate and analyze the quality and safety of digital content, as

well as could create content, and apply ethical principles by acting socially (Hobbs, 2010, p. 7). According to Hobbs (2010, p. 7), digital literates are people who may take social action. Finally, Belshaw (2011, p. 206) tried determining the dimensions of digital literacy skills in his thesis study. Evaluating this skill in eight assorted sizes. Belshaw's classification deals with the elements of the craft rather than the characteristics of the digital literate individual:

1. Cultural
2. Cognitive
3. Constructive
4. Communicative
5. Confident
6. Creative
7. Critical
8. Civic

JISC (Joint Information Systems Committee), which likewise works on cyber-security, defines *digital literacy* as individuals who have the skills to live with digital technology, learn and work in this environment. Accordingly, digital literacy encompasses all the previously mentioned technology-based literacy. Therefore, the framework for digital literacy is explained through this definition (JISC, 2014):

- Media Literacy
- Communications and Collaboration
- Career and Identity Management
- ICT (Information Communication Technologies) Literacy
- Learning Skills
- Digital Scholarship
- Information Literacy

Data/ Information Privacy

Developments in communication and technologies dismay the world about security. The fact that individuals are more

present on the internet and digital platforms has led to an enormous increase in digital data. Using this data brings many conveniences for both users and companies; however, it triggers many sensitive situations regarding data security. Data security requires careful use within the framework of some ethical principles during the collection, storage, and processing of the obtained data. Nevertheless, it is possible to deal with the issue within the framework of more than one dimension regarding data security. In this sense, there are dimensions of security, such as database security, communication network security, communication systems security, and access security, within the scope of ensuring personal data security (Şimşek, 2008, p. 85).

Databases are data sets that consist of the traces that individuals leave behind while browsing the Internet. Thanks to these sets, it becomes feasible to produce meaningful information. Without databases, companies cannot perform tasks such as estimation and measurement; however, this information may be sensitive information that may be considered personal and protected by law. Therefore, the security of databases is regarded as the first dimension. In the second and third stages, there are communication networks and systems where this data is obtained and used. Their safety is considered at least as important as primary care.

Consequently, deciding which data is sensitive at this stage is necessary. In this context, it is possible to divide the data into sensitive and non-sensitive data (Küzeci, 2010). Different persons may obtain sensitive data, and due to the nature of such data, it may cause the related persons to be victimized, offended, and discriminated against in different situations (Gündüz, 2022, p. 32). It is possible to call the remaining data as non-sensitive data.

Data security requires the protection of both types of information. Various platforms and institutions have set specific standards and principles to ensure data security. There are personal data security regulations at the international level, such as the United Nations, the European Court of Human Rights, the

Council of Europe, the Organization for Economic Co-operation and Development (OECD), the Universal Declaration of Human Rights (UDHR), and the European Union. Apart from international regulations, there are some accepted principles in data security. According to Gündüz, those may be listed as follows (2022, p. 30):

1. Critical and sensitive data should be prevented from being obtained unintentionally by unauthorized persons, and a guarantee of accessibility should be ensured only by those authorized to access it (Confidentiality).
2. Modification and deletion of data by persons other than the owner or authorized person should be prevented (Integrity).
3. The data or the systems in which the data is processed must be ready to be used continuously and work uninterruptedly (Availability).
4. The data owner's or authorized person's identity requires authentication (Authentication).

As can be seen, the issue of data security is susceptible and is given importance by many international institutions and organizations. In Turkey, the security of personal data is fundamental at the national level, and limits have been determined within the scope of the Personal Data Protection Law (known as KVKK *in Turkish*). However, although data security is considered essential by by-laws, conventions, and international institutions, the perception of privacy in data security is getting more sensitive daily.

The penetration of technology into all areas of life with intelligent devices, and the new media opportunities such as social media affecting increased users, raise the issues of surveillance and privacy. Sharing has become more widespread, bringing social media to the fore. Risks related to data and privacy security on social media platforms are always possible.

Although it may seem harmless and leisurely for users, social media has a high history of privacy and data security issues. Despite these benefits, the concerns and discussions about security

and privacy issues in the social media environment never fall from the agenda (Patel, 2017, p. 836). For instance, on Facebook, in June 2013, due to an error, the e-mail addresses and phone numbers of approximately six million members were accessed without being requested (Newcomb, 2018). Another example, most notably, is the "Cambridge Analytica (data) scandal." It is the event that the personally identifiable information of millions of Facebook users (approximately fifty million) is collected by Cambridge Analytica, and the data obtained is used to influence the opinion of the voters on behalf of some politicians. Brittnay, former director of Cambridge Analytica after Wiley Kaiser, used expressions that people may change their minds with their method. After the data of the people called "persuasive" while targeting, this data allows them to vote by bombarding them with blogs, articles, and videos to change their behavior (Noujaim & Amer, 2019).

When it comes to social media, individuals need to be more careful when using these platforms. Because of new media opportunities, especially in social media, individuals may encounter difficulties such as inappropriate content, internet addiction, adverse effects, virtual fraud, identity theft, harassment, and cyberbullying (Altun, et al., 2018, p. 41-43). Hence, during the profile creation process on social networking sites, name, home address, e-mail address, and other confidential information are requested. Because of this information, there is no need to doubt that unknown and unwanted malicious persons may present various dangers (Chewae, Hayikader, Hasan, & Ibrahim, 2015, p. 1). If personal information is not used judiciously and reliably on social media, the user's privacy may be attacked in numerous ways. Because the social media environment is closely monitored, information, documents, and images should be shared as little as possible. All of this is constantly being archived and accumulated in the centers of social networks in the USA. The possibility that large images are created to be used for different purposes should never be underestimated (Ceylan, Demiryürek, &

Kandemir, 2015, p. 8). So even a single photo or video may result in an enemy accessing this information (Ghazinour & Ponchak, 2017, p. 267-268).

Regarding data security, social media results are not only encountered. In addition to this, especially in big data and data mining, the issue of data security is discussed, and the methods of ensuring privacy are mentioned. Data mining applications and mathematical analyzes should be made by considering personal privacy (Eyüpoğlu, Aydın, Sertbaş, Zaim, & Öneş, 2017). Regarding confidentiality, taking security measures between the computer layers may be necessary, as violations cause legal responsibilities and ethical problems. For instance, virtual barriers such as firewalls, secure socket layers, and transport layer security are designed to limit access to data (Eyüpoğlu, Aydın, Sertbaş, Zaim, & Öneş, 2017). To the contrary, it is tried to take measures for privacy by employing some additional elements. Organizations use a variety of de-identification methods (Eyüpoğlu, Aydın, Sertbaş, Zaim, & Öneş, 2017, p. 177) to ensure security and privacy.

Although such measures are sometimes aimed at ensuring privacy to a certain extent, they may likewise complicate the use of data. This situation may pose problems that hinder the development of some technologies. Therefore, the development of some technologies may be slower before security problems are overcome. Alternatively, a developing technology may be subjected to tests and procedures to overcome security barriers for a while. Passwords supervised access and two-factor authentication; are technical solutions nonetheless low-level that are extensively used to ensure security and privacy when data is shared and aggregated in dynamic and distributed data systems. The more advanced technical solution is cryptography. AES and RSA are well-known Encryption algorithms. Recent disclosures show that the NSA (National Security Administration) has found ways to crack existing internet Encryption algorithms (Matturdi, Zhou, Li, & Lin, 2015; Perlroth, Larson, & Shane, 2013). Cryptog-

raphy is the art/science of secret writing (Karaarslan, Ergin, Turğut, & Kılıç, 2015). The most basic service that cryptography provides is encryption. Encryption converts data into a format (ciphertext) that only the intended recipients may read. The aim is to ensure confidentiality (Kaufman, Perlman, & Speciner, 2002).

In light of all this information, we conclude that data security must be ensured to ensure privacy. Problems arising from using data without privacy may leave individuals and companies in distress. Therefore, with several applications and changes to be made at both the technical and awareness level, it will be possible to protect privacy by providing data security awareness.

Relation of Data Security Issue with Digital Literacy and Communication Processes

The future of communication brings us to a point where there will be much more complex conditions, and communication will inevitably be at the center of life. Therefore, in such a case, it would be helpful to combine the data security and privacy discussed in the previous sections with the digital literacy issue in this section to explain the problem.

The more critical the privacy phenomenon is for people and companies, the more digital literacy becomes necessary to understand and realize this serious situation sustainably. Considering the 21st century, which is living under information bombardment, the uncontrolled circulation of information directly threatens privacy. Whereas all kinds of mass media, including new communication tools, especially the internet, have an essential role in transferring knowledge, they are the first source that individuals apply when they need information.

While information is power, conversely, it may become a tremendous threat when it is not used correctly. For this reason, the regular and controlled flow of information depends on the level of digital competencies and digital literacy in using technologies that transmit information. Media is where much information

may circulate due to its nature and is partially devoid of control and supervision; these areas are where contradictory, incorrect, or distorted information is found. At the point reached today, it is possible to circulate misinformation and fake news on all media platforms. It makes the confirmation of the information necessary. In this context, we are faced with the importance of media literacy.

The prodigiousness and diversity of the information in the media and the fact that it may be inaccurate/fake make it arduous for the public to understand and analyze the data and simultaneously cause discombobulation. Thus, individuals may be manipulated in the information flow they are exposed to, become irate, and ineluctably experience situations that aliment the lynching culture.

In the period where digital transformation is proceeding; therefore, in such a period, literacy such as digital, media, and technology has become necessary for individuals, and information and communication are essential in terms of improving the daily needs of individuals and accessing the information they need in order to use their full potential (Horton, 2008). Nonetheless, the reliability of the information is possible with the correct use of information access tools. Otherwise, this situation may lead to some undesirable or criminal cases.

According to the Cost of Cybercrime Study (Ponemon-Institute, 2016), the cost of cybercrime for US organizations is 17.36 million dollars on average, 8.39 million dollars for organizations in Japan, and 7.84 million dollars for those in Germany. Security breaches may further affect end users. In some cases, FBI data becomes remarkable when this situation is reflected as a complaint. In 2015, the FBI received 288,012 complaints regarding cybercrime, with more than 40% of these complaints resulting in monetary losses (Cain, Morgan, & Still, 2018). As is known, cyber-security threats are a problem that affects not only institutions nonetheless individuals, and measures should be taken to prevent losses (Aslan, Aktaş, & Akbıyık, 2020).

Taking precautions depends on making some prognostications beforehand; categorical risks must be identified to make estimations, and actions must be taken accordingly. Risk communication, which includes disseminating information about all types of risks and hazards, is essential to developing a rational understanding of risks (Reynolds & Seeger, 2005, p. 47). In contrast, cyber-hygiene also draws attention as an effective solution besides identifying risks and managing the situation with an initiative-taking approach besides identifying risks and managing the situation with an initiative-taking approach, cyber-hygiene also draws attention as an effective solution. In the field of cyber security, that is, data security, the understanding of cyber-hygiene has come to the fore recently. Although cyber-hygiene is critical in protecting cyber-security, it should not be seen as synonymous with cyber-security. Cyber-hygiene involves establishing and maintaining healthy cyber behaviors (Vishwanath, et al., 2020), in other words, to protect individuals' financial and social information against cyber-attacks, individuals need to follow the rules and make these behaviors a habit. As the level of awareness and implementation of these rules and behaviors, called cyber-hygiene, increases, people's protection level against possible cyber-security violations will increase. No doubt, this will directly affect digital and media literacy competencies. Growing cyber threats make end-user computer security behavior even more critical because individuals consciously or unconsciously take action that uses cyber breaches (Bulgurcu, Cavusoglu, & Benbasat, 2009). Today, with the increasing number of cyber-crimes, governments, security experts, and decision-makers want individuals to give more importance to the issue of cyber-hygiene (Vishwanath, et al., 2020).

As indicated, the issue of data security is essential in terms of ensuring privacy, which is related to the level of *digital literacy* that will enable cyber-security measures to be taken. Therefore, increasing information contamination with the centralization of communication, media reading habits gaining importance, being

unaffected by *fake news*, and overcoming the difficulties experienced in the virtual world, such as cyberbullying, can be possible by increasing digital literacy. Many platforms and systems often have security options that may be set and changed; nonetheless, end users often do not understand these options and know how to find and use them (Furnell, 2005).

CONCLUSION

The increasing number of communication technologies affects both individuals and businesses. Technological developments such as smartphones, tablets, laptop computers, wearable technologies, cyber-physical systems, autonomous robots, augmented reality technologies, and artificial intelligence, which are new every day, deepen digital transformation and accomplish more efficacious than the previous day. With the COVID-19 pandemic, which was experienced very soon and whose effect is still persistent, large masses have rapidly adopted digital transformation with its much more profound impact.

These possibilities, tremendous developments for the field of communication, on the one hand, have a say in the transition of humanity to the next stage; on the other hand, they have some systemic and human openings capable of shaking people to the deepest. With the increasing technological possibilities, more data production may pave the way for cybercrimes that expose and disclose the most private ones rather than their benefits and harm to individuals. Increasing numbers of misinformation activities confuse individuals and make it difficult to distinguish truth from delusiveness.

Information circulating uncontrolled similarly enhances the possibility of personal data falling into the hands of malware and individuals. While data security is under threat, we observe that what may be done about cyber-security is diversified. At the point of protection, storage, and processing of sensitive and non-sensitive data, it is necessary to act together with some legal regulations and software, systematic and practical applications.

However, the increase in digital literacy comes to the fore regarding providing cyber-security and data security. Digital literacy teaches us how to use these media tools. In parallel with this, it shows how we may use these tools more safely. Therefore, from the perspective of communication, one of the vital future discussion topics is the necessity of reading and using digital media tools correctly. Continuity of data security and communication processes is an essential element that will prevent cybercrimes.

REFERENCES

Ala-Mutka, K. (2011). *Mapping digital competence: Towards a conceptual understanding*. Seville, Spain: European Commission, Joint Research Centre, Institute for Prospective Technological Studies. doi:10.13140/RG.2.2.18046.00322

Altun, A., Pembecioğlu, N., Orhon, E., Aydın, H., Erkmen, N., Şahin, G., Üstün, E. (2018). *Medya okuryazarlığı*. Ankara: Milli Eğitim Bakanlığı Publications.

Artut, S. (2014). *Teknoloji- insan birlikteliği*. Istanbul: Ayrıntı Publications.

Aslan, T., Aktaş, B., & Akbıyık, A. (2020). Kullanıcıların bilgisayar güvenliği davranışını inceleme: Siber Hijyen. *7. Uluslararası Yönetim Bilişim Sistemleri Konferansı"Sağlık Bilişimi ve Analitiği"*. İzmir. Retrieved from https://www.researchgate.net/profile/Tugce-Aslan-3/publication/348182462_kullanicilarin_bilgisayar_guvenligi_davranisini_inceleme_siber_hijyen/links/5ff2c5a6299bf140886c7412/kullanicilarin-bilgisayar-guevenligi-davranisini-inceleme-siber-hijyen.pdf

Aufderheide, P. (1993). Media literacy. A report of the national leadership conference on media literacy. *Communications and Society Program* (pp. 3-44). Washington, DC: Aspen Institute.

Bawden, D. (2008). Origins and Concepts of digital literacy. In C. Lankshear, & M. Knobel, *Digital literacies: Concepts, policies and practices* (pp. 17- 32). New York: Peter Lang.

Belshaw, D. A. (2011). What is digital literacy? A pragmatic investigation. *Ed.D Dissertation*. Department of Education, Durham University. Retrieved from http://etheses.dur.ac.uk/3446/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. *European and Mediterranean Conference on Information Systems 2009*, (pp. 1-11). Izmir.

Cain, A. A., Morgan, E. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36-45. doi:10.1016/j.jisa.2018.08.002

Castells, M. (2011). A network theory of power. *International Journal of Communication, 5*, 773-787.

Ceylan, F. B., Demiryürek, E., & Kandemir, B. (2015). Sosyal ağlarda güncel güvenlik riskleri ve korunma yöntemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 1*(1), 8-10.

Chewae, M., Hayikader, S., & M. H. Hasan, J. İ. (2015). How much privacy we still have on social network?. *International Journal of Scientific and Research Publications, 5*(1), 1-3.

Condy, J., Chigona, A., Gachago, D., & Ivala, E. (2012). Pre-Service students' perceptions and experiences of digital storytelling in diverse classrooms. *Turkish Online Journal of Educational Technology, 11*(3), 278-285.

Crowe, A. R. (2006). Technology, citizenship, and the social studies classroom: education for democracy in a technological age. *International Journal of Social Education, 21*(1), 111-121.

Dede, C. (2010). Comparing frameworks for 21st century skills. In J. Bellanca, & R. Brandt, *21st century skills: Rethinking how students learn* (pp. 51-76). Bloomington, IN: Solution Tree Press.

Dijk, J. V. (2016). *Ağ toplumu*. Istanbul: Kafka Publications.

Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia, 13*(1), 93-106.

Eshet-Alkalai, Y., & Amichai-Hamburger, Y. (2004). Experiments in digital literacy. *cyberpsychology & behavior, 7*(4), 421-429.

Eyüpoğlu, C., Aydın, M. A., Sertbaş, A., Zaim, A., & Öneş, O. (2017). Büyük veride kişi mahremiyetinin korunması. *Bilişim Teknolojileri Dergisi, 10*(2), 177-184. doi:10.17671/gazibtd.309301

Furnell, S. (2005). Why users cannot use security. *Computers & Security, 24*(4), 274-279.

Ghazinour, K., & Ponchak, J. (2017). Hidden privacy risks in sharing pictures on social media. *Procedia Computer Science, 113*, 267-272. doi:10.1016/j.procs 2017.08.367

Gündüz, M. Ş. (2022). Uluslararası hukuk açısından kişisel veri güvenliği. Batman: Batman Üniversitesi, Lisansüstü Eğitim Enstitüsü. (Published Master's Thesis).

Hague, C., & Payton, S. (2010). *Digital literacy across the curriculum*. Futurelab. Retrieved from https://www.nfer.ac.uk/publications/futl06/futl06.pdf

Herman, N. D., Maknun, J., Barliana, S., & Mardiana, R. (2019). Technology literacy level of vocational high school students. *Proceedings of the 5th UPI International Conference on Technical and Vocational Education and Training (ICTVET 2018)*, (pp. 519-522). doi:10.2991/ictvet-18.2019.118

Hobbs, R. (2010). *Digital and media literacy: A plan of action*. Washington, DC: The Aspen Institute. Retrieved from https://www.aspeninstitute.org/wp-content/uploads/2010/11/Digital_and_Media_Literacy.pdf

Honan, E. (2008). Barriers to teachers using digital texts in literacy classrooms. *Literacy, 42*(1), 36-43.

Horton, J. F. (2008). *Understanding information literacy: A primer.* Paris: United Nations Educational, Scientific and Cultural Organization-UNESCO. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000157020

ITEEA. (2000). *Standards for technological literacy: Content for the study of technology.* Reston, VA: Iteea-International Technology and Engineering Educators Association.

JISC. (2014). *Developing digital literacies.* JISC: Joint Information Systems Committee. Retrieved from https://www.jisc.ac.uk/guides/developing-digital-literacies

Karaarslan, E., Ergin, A. M., Turğut, N., & Kılıç, Ö. (2015). Elektronik sağlık kayıtlarının gizlilik ve mahremiyeti. *Conference: INET-TR* . Istanbul. Retrieved from http://acikerisim.mu.edu.tr/xmlui/bitstream/handle/20.500.12809/9990/Karaarslan.pdf?sequence=3&isAllowed=y

Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network security: Private communication in a public world.* Upper Saddle River, NJ: Prentice Hall.

Kurbanoğlu, S. (2010). Bilgi okuryazarlığı: Kavramsal bir analiz. *Türk Kütüphaneciliği, 24*(4), 723-747.

Kurt, A. A., Orhan, D., Yaman, F., Solak, M. Ş., & Türkan, F. (2014). Bilgi ve iletişim teknolojileri ışığında Türkiye'de yapılan okuryazarlık çalışmalarındaki eğilim. *Eğitim Teknolojileri Araştırma Dergisi, 5*(2), 1-21.

Küzeci, E. (2010). *Kişisel verilerin korunması.* Ankara: Turhan Kitapevi.

Leaning, M. (2019). An Approach to digital literacy through the integration of media and information literacy. *Media and Communication, 7*(2), 4-13.

Matturdi, B., Zhou, X., Li, S., & Lin, F. (2015). Big data security and privacy: A review. *China Communications, 11*(4), 135-145.

Newcomb, A. (2018, Mart 24). *A timeline of Facebook's privacy issues u* Retrieved from nbcnews.com: https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651

Noujaim, J., & Amer, K. (Directors). (2019). *The Great Hack* [Motion Picture]. Retrieved from https://www.netflix.com/title/80117542

Oliver, R., & Towers, S. (2000). Benchmarking ICT Literacy In Tertiary Learning Settings. *Proceedings of the 17th Annual ASCILITE Conference,* (pp. 381-390).

Patel, M. (2017). Cyber security for social networking sites: Issues, challenges and solutions. *International Journal for Research in Applied Science & Engineering Technology (IJRASET), 5*(4), 833-838.

Perdana, R., Yani, R., Jumadi, J., & Rosana, D. (2019). Assessing students' digital literacy skill in senior high school Yogyakarta. *JPI-Jurnal Pendidikan Indonesia, 8*(2), 169-177. doi:10.23887/jpi-undiksha.v8i2.17168

Perlroth, N., Larson, J., & Shane, S. (2013, September 5). *NSA able to foil basic safeguards of privacy on web.* Retrieved from nytimes.com: https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

Ponemon-Institute. (2016). *2016 cost of cyber crime study & the risk of business innovation.* Ponemon Institute.

Reynolds, B., & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication, 10,* 43-55.