

DİJİTAL TOPLUMDA MAHREMİYETİN İMKÂNI ÜZERİNE BİR İNCELEME

A Review OnThe Possibility Of Privacy In Digital Society

Hasan TUTAR*

Ceren Güler ÇAĞILTAY**

Özet

Dijital teknolojiler alanında yaşanan gelişmeler bir taraftan bireysel ve toplumsal yaşamını dönüştürürken, diğer taraftan bireylerin ve toplumların mahremiyet anlayışlarını dönüştürmektedir. Dijital teknolojiler marifetiyle görüntü ve seslerin kaydedilmesi, saklanması ve iletilmesi yeteneği mahremiyetin ihlal edilmesi sorununu ortaya çıkarmakta ve kişinin özel alanını daraltmaktadır. Bu çalışmanın temel amacı, gözetim, akıllı teknolojiler ve mahremiyet olguları arasındaki ilişkiyi olgusal veriler üzerinden analiz etmektir. Araştırma betimsel istatistiksel yöntemle dayalı olarak yürütülmüştür. Araştırmanın problemi ve temel sorusu doğrultusunda evren parametrelerine doğrudan ulaşma imkânı olduğu için betimsel istatistiksel yöntem tercih edilmiştir. Araştırmanın analizleri çeşitli veri tabanları yoluyla ve açık kaynaklardan elde edilen ikincil verilere dayandırılmıştır. Veriler hem eğilimleri açısından incelenmiş hem de toplumlara gözetim toplumu yapan akıllı teknolojilerin yıllar itibarıyla gelişimi grafik olarak verilmiştir. Bu çalışmada mahremiyet ve gözetim toplumunun birlikte düşünülmesinin imkânı eleştirel bakış açısıyla incelenmiştir. Araştırma bulguları gelişmiş ülkelerin gözetim imkânı açısından da gelişmiş olduğunu ve bu toplumlarda mahremiyetin korunmasının neredeyse imkânsız olduğunu göstermektedir.

Anahtar Kelimeler: Gözetim toplumu, mahremiyet, akıllı cihazlar, betimsel istatistik, dijital teknoloji.

Abstract

Developments in the field of digital technologies, on the one hand, transform individual and social life, and on the other hand, transform the privacy understanding of individuals and societies. The ability to record, store and transmit images and sounds through digital technologies raises the violation of privacy and narrows one's private space. The main purpose of this study is to analyze the relationship between surveillance, smart technologies, and privacy phenomena through factual data. The research was conducted based on the descriptive statistical method. In line with the research problem and basic question, the descriptive statistical method was preferred because it can access the universe parameters directly. The research analysis was based on secondary data from various databases and open sources. The data has been examined in terms of trends, and the development of smart technologies that make societies surveillance societies over the years is given graphically. In this study, the possibility of considering privacy and surveillance society together has been critically examined. Research findings show that developed countries are also developed in terms of surveillance, and it is almost impossible to protect privacy in these societies.

Keywords: Digitalsociety, privacy, smart devices, descriptive statistics, digital technology.

*Prof. Dr. , Bolu Abant İzzet Baysal üniversitesi, İletişim Fakültesi, hasantutar@ibu.edu.tr, <https://orcid.org/0000-0001-8383-1464>

** Yüksek Lisans Öğrencisi, Bolu Abant İzzet Baysal Üniversitesi, İletişim Fakültesi, cerencagiltay16@gmail.com, <https://orcid.org/0000-0003-4953-2019>

1. Introduction

The main factor that narrows people's private space is the irresponsible use of digital technologies, and the possibility of these irresponsible behaviors is increasing daily. As of 2021, 66.6% of the 7.83 billion population in the world are mobile phone users, 59.5% are internet users, and 53.6% are social media users. As of 2021, 90.8% of the 84.6 million population in Turkey are mobile phone users, 77.7% are internet users, and 70.8% are social media users (We Are Social, 2021). While digitization rates are increasing worldwide, this change is above the world average in Turkey. It is understood that the idea that digital technology can be used for the benefit and welfare of society, together with the concept of Society 5.0, is an illusion in terms of privacy (Fukuyama, 2018: 47; Granrath, 2017; Martin, 2008: 151). On the other hand, ignoring the opportunities provided by technology means resisting digital transformation and staying behind the change. However, it is undeniable that every opportunity brings risks and problems.

The digital revolution, which emerged with the development of information and communication technologies, changes every aspect of life, transforming it according to its place and changing the understanding of traditional privacy. Understanding privacy, associated with bodily privacy in traditional societies, causes problems such as "privacy of personal data" and "right to be forgotten" with the widespread use of digital technologies. Digital technologies, which direct not only the private life of many people but also their business and social life, can be used for different purposes. These technologies function as a communication channel, social environment, information source and transaction environment in the lives of individuals. While this situation facilitates human life, on the other hand, it raises the problem of making more private information public and sharing it over the Internet. While people are using digital media tools, they may consciously or unconsciously share much information about their private lives, causing a violation of privacy (Boyd & Ellison, 2007:15; Tuunainen, Pitkänen, & Hovi, 2009: 25). violation of privacy raises the problem of various violations in general human rights, constitutional rights and personal data protection rights. The increased possibility of digital surveillance may cause a new problem called "violation of privacy" in digital societies.

Sustaining life in a rapidly changing and digitalizing world is possible by not staying out of the digitalization process, that is, by bringing together pieces of information in digital environments and transforming them into concrete outputs. With the contribution of digital technologies, a new social structure called "surveillance societies" emerges, and the possibility of surveillance can cause privacy violations. When the desire for surveillance is combined with the ability of smart devices, the narrowing of the private space of individuals and the violation of privacy is inevitable. This situation raises the problem of the uncertainty of the boundaries of concepts such as surveillance, private space and privacy in digital societies. With the help of smart devices, what is public and what is

private becomes an important topic of discussion (Dolgun, 2005: 55-58; Bauman and Lyon, 2018: 31; Çaycı and Çaycı. 2017: 36). Opportunities provided by digital technologies can easily cause the violation of the privacy rights of individuals.

Thanks to mobile phones, security cameras, computers, biometric controllers and other smart devices, the privacy limits of individuals are eliminated, and the data that should not be in the public domain is recorded in cyberspace (Erdem and Kaya, 2019: 148; Cormack, 2019: 23). With the help of smart devices, surveillance activities based on display and peeping are changing in pre-modern times, and new types of surveillance such as “synopticon” and “super panopticon” appear. Synopticon means the transfer of surveillance to cyberspaces thanks to digital technologies (Çakır, 2015: 344; De Laat, 2008: 57). In cyberspace, the boundaries of private-public space disappear, and the problem of privacy arises. Invisibility, a requirement of privacy, is taken away from the individual with the spread of smart devices. The main problem here is that individuals do not care about privacy and see it as a price to be paid against the opportunities provided by smart technologies (Bauman and Lyon, 2018: 41; Amitay and Rahav, 2020: 20). Another issue is that surveillance has become an object of desire for individuals due to cultural changes. The irresponsible use of digital technologies transforms both the watcher and the observed individuals into power apparatus without the powers’ pressure.

2. Conceptual Framework

2.1. The Problem of Privacy in Digital Societies

Developments in digital technologies have recently led to the emergence of a new problem specific to the digital society: the problem of protecting personal data privacy and privacy violations. Privacy is one’s own private space, a zone of autonomy. It refers to an area where people can be alone, think, act, and decide on what boundaries to communicate and communicate with others (Bauman and Lyon, 2018: 41). confidentiality or privacy encompasses protecting personal data. The use of digital technology often disrupts the balance between the private and public domains, bringing along the problem of privacy violation (Dinev and Hart, 2005: 7-8; Aimeur, Gams and Ho, 2010: 172-179; Pitkänen and Tuunainen, 2012: 25; Buchenscheit et al., 2014: 20-29). Privacy is a fundamental human right and underpins rights that support human dignity, such as freedom of association and expression.

The right to privacy is the right of individuals to determine to what extent they will share their living spaces with others (Bennett, 2009: 229; Yüksel, 2003: 181; Kokolakis, 2017:122). Although the concept of privacy differs from culture to culture and even from time to time, it has a common and universal aspect. Privacy means not sharing information, images, sounds and photographs belonging to the person unless he/she wishes. Although there are different forms of privacy, privacy consists of territorial privacy,

which means the privacy of the physical space surrounding a person, personal privacy that prevents unnecessary interference with the physical existence of the individual, and information privacy regarding the collection and processing of personal data (Kokolakis, 2017:125; Buchenscheit et al., 2014: 20-29). Types of privacy require the protection of physical space, the protection of individuals against unfair interventions and the protection of information security of individuals. Privacy violations also occur with the violation of the elements that make up the types of privacy.

With the changes in the field of information and communication technologies, the violation of the privacy rights of individuals becomes easier. The use of the Internet by individuals while working, maintaining their daily lives or enjoying their free time causes them to leave a footprint in the digital world, which raises the issue of various privacy violations. The storage and use of data regarding the private lives of individuals in digital environments cause health and financial data security concerns. Techniques and analyses emerging with big data applications bring along the problem of protecting the privacy of individuals (Tan and Pivot, 2015: 862; Miltgen, 2009: 103-125). For this reason, many countries make legal arrangements for privacy. It aims to protect personal data collected by recording online behavior and keeping log records. Individuals have no idea what kind of data is collected and where it is kept, how long it will be kept and what it will be used for can cause various concerns (Ridley-Siegert, 2015: 30-35; Tan and Pivot, 2015: 860). An important aspect of privacy and privacy risks is the problem of who has access to personal data shared on the Internet and social networking sites. When malicious persons access personal data, privacy and confidentiality are risks (Hughes-Roberts and Kani-Zabihi, 2014: 220; Kaya, 2011: 317). Loss of Confidentiality and control of personal information can cause personal and social irreparable harm.

Today, digitalization has started to create the virtual online projection of the physical offline world, revealing the "digital twin" concept. In addition to digital twins, individuals begin to express themselves with the digital identities they create in online environments, causing the emergence of digital online ecosystems (Guettl & Chang, 2008 50-60; El Saddik, 2018: 87). In digital online environments, participation in online society emerges as the phenomenon of digital citizenship (Mossberger, Tolbert, & McNeal, 2008). Although digital citizenship includes being respectful to oneself and others, protecting oneself and others, carrying digital rights and responsibilities, and digital security in digital environments, the irresponsibility shown in these media causes digital privacy violations.

Surveillance is a special information collection, storage, processing, evaluation and use. Surveillance, which can be taken back to the known history of humanity, has gained its real prevalence in social life in the modern time when digital technologies have become widespread. Surveillance practices strengthened with modernity have diversified over

time and become one of the important weapons of the governments (Fuchs, 2016: 218; Gandy, 1989: 61). The main source of power in surveillance societies can be expressed as holding information and using it when necessary. In the western world, the concept of surveillance is identified with the “Big Brother” in Orwell’s novel 1984. In the surveillance provided by punishment and violence, the eyes of the governments are always on the individual, and in this way, they can keep them under constant control. This also means that private space for the individual cannot be easy. In his book, Orwell described a world where individuals are watched 24 hours a day, with a bureaucratic system he called Big Brother. Huxley’s Brave New World novel describes this desire for control in a world where individuals consent to surveillance by persuasion (Erdem and Kaya, 2019: 1457; Lyon, 2013: 161). In both novels, surveillance is one of the important tools to ensure the control of the powers and control individuals’ lives.

The concept of surveillance was first used in the literature with Bentham’s conceptualization of the “Panopticon.” Bentham defined surveillance as “a new method that has no precedent and gains mental power over the mind” (Güven, 2011: 8; Lyon, 2013: 184). According to Marx, the phenomenon of surveillance emerged in parallel with the development of capitalism in modern times. It is an element of the struggle between labor and capital. Surveillance is tool capitalist managers use to achieve the highest level of efficiency. As a result of keeping the factory workers under constant surveillance and control, the system reaches its most efficient state (Bozkurt, 2014: 104). Giddens described the surveillance as a tool that nation-states should have to maintain their power. Societies are disciplined by surveillance (Giddens, 2005: 69; Güçlüyener, 2011: 6; Allen, 2008: 323).

Foucault (1992), in his book “The Birth of Prison,” defined surveillance as a “functional means of discipline.” The discipline of the government can only be possible with the existence of the means of suppression. Governments are trying to establish order by employing surveillance. According to Foucault, surveillance is not only a means of maintaining order but also an important means of establishing biopower. Structures suitable for surveillance are built. Foucault explains this situation with the military school model. The building of the military school is modeled on surveillance. Bedrooms are scattered along the corridor like a series of small cells. Officer lodgings frame it at regular intervals. There is an officer on the left and right of every ten students. Students are closed and kept under surveillance in these rooms during the night (Foucault, 1992: 216). Today, the ability of smart devices has been added to this mechanical surveillance, and the power of surveillance has been consolidated. This situation, which Foucault defines as “immanent power,” has been achieved by violating the individual’s privacy. The governments, who are aware of all the private information of the people, who are constantly watched and whose preferences are stored, benefit from this data while taking their steps and thus expand their sovereignty.

The main reason for oversight to hold power is security and discipline. The “Panopticon” designed by Jeremy Bentham in 1785 is a prison model and a prototype of surveillance activities. Inspired by the prison model architecture and the basic design of invisible surveillance, Foucault developed the panopticon as a type of surveillance. Foucault uses the panopticon to mean “the power of the mind over another mind.” The main purpose of the panopticon as a type of surveillance is that it is not known by whom the surveillance was carried out. The panopticon aims to act under control by thinking as if the individual is being watched at all times, without knowing when he is being watched (Foucault, 1992: 251; Erdem and Kaya, 2019: 1458). The basic tool of invisible surveillance was the panopticon yesterday, and today it is thanks to the MOBESE cameras spread all over the place. Thanks to this system, governments are expanding their sovereignty by violating privacy for the sake of the security of the society, by monitoring everything from parks to streets, from prisons to streets and boulevards, and from public buildings to common living spaces.

The advancement of technology and the widespread use of smart devices increase the surveillance possibilities of governments. Bauman expresses this situation with the concept of “fluid surveillance,” a continuation of liquid modernity. Fluid surveillance is a form of orientation, not a way of explaining surveillance. In this orientation, the spread of surveillance for security reasons is mentioned instead of the surveillance for disciplinary purposes in the panopticon. Unmanned Aerial Vehicle systems exemplify the fluidization of surveillance in Bauman and Lyon’s book “Fluid Surveillance.” These digital technological tools allow individuals to collect personal data without their awareness. Today, surveillance individuals are no longer worried about spying on but rather desire to be spied on. Bauman describes this situation as “surrender” (Bauman and Lyon, 2018: 31). With the technological developments in the information age, individuals in surveillance societies are not citizens but registration numbers consisting of letters and numbers. This does not mean anything other than the reduction of the subject to the object (Lyon, 1997: 311; Çaycı and Çaycı, 2017: 43). Digital citizenship, in a way, means renouncing being a natural citizen.

Surveillance in pre-modern societies; was used for display, disclosure and even architectural structures. In post-modern societies, surveillance is done through smart devices and internet technology. Surveillance practices always include a violation of privacy, regardless of their purpose. The concept of privacy has faded and lost its importance in surveillance societies (Dolgun, 2004: 15; Schoenherr, 2021). Privacy is where the veil worn against the outside world can be removed, leaving aside the armor needed in the public sphere (Lyon, 1997: 29). privacy is not taking away the individual’s will to hide what is unique (Yüksel, 2003: 182; Bennett, 2018: 239). However, developing technologies and the spread of smart devices simplifies access to all kinds of information at a level that violates the privacy of individuals. The effect of smart device technologies on privacy in surveillance societies causes a kind of “death of privacy” problem.

2.2. The Opportunity of Privacy in Digital Societies

The concept of privacy is “the right to be alone,” “protecting personal information from others, protecting what should be kept confidential. Privacy means protecting personal space where people can be alone and deciding the conditions under which they will interact with others. The private area constitutes a special place in the individual’s life, and this area is closed to the public. This area is ambiguous because it has a special meaning for each individual and its boundaries are not clear; it contains its ethical codes. Every aspect that the person does not need to share with others and does not want others to know is his privacy (Robison, 2017: 1-9; Berkup, 2015: 28; Çaycı and Karagülle, 2014: 195). While the lives of individuals in digital societies show a transition from real life to digital life, a new form of privacy called digital privacy emerges. While privacy in real life is “the areas determined by the person unilaterally,” digital privacy emerges in many ways due to reasons arising from both technology and those who consume it. Individuals’ perceptions of private and public spaces in the digital environment and their perceptions of privacy are also changing. Surveillance areas are diversifying simultaneously with the development of digital communication and surveillance practices.

The relationship between the observed subject and the observer in digital surveillance is different from that in surveillance in the classical period. In digital surveillance, there is often no interaction between two subjects. Simultaneity in surveillance practices in the pre-modern period has spread to all times of the day (Lyon, 2013: 52-53). The fact that traces left in cyberspace do not disappear spreads surveillance to all areas of human life. The boundaries of the private-public sphere, which determine the boundaries of privacy in cyberspace, are getting blurred. This situation can often be realized with peeping and surveillance practices and the spread of the culture of display and sharing in social relations. Although exposing the privacy of personal life is individual freedom, in the last instance, it means the elimination of privacy (Giddens, 2010: 169). Surveillance, one of the most important power tools in the historic process, reveals its real social weight with modernization. With the development of nation-states and bureaucratic organizations, surveillance has become widespread. In digital societies, the spy disseminates information to the public sphere without being seen and surveilled voluntarily.

Privacy is according to society, and societies create privacy according to their beliefs, traditions, customs and, in short, their cultures. Therefore, privacy has been part of society’s culture since ancient times. Intelligent technologies, which affect the daily life practice of individuals and social life in many ways, transform privacy by eroding it. With the possibility of digital technologies and smart devices, while the world is globalizing economically, culturally, politically and politically, on the one hand, it also brings with it ethical and privacy problems (Flanagan, 2014: 128; Javor, 2016: 248). People develop

ethical codes according to the education they receive from their family and intimate environment and the cultural codes of the environment. As culture belongs to local, national and a certain society, it can be mentioned that ethical codes and privacy perceptions shaped according to culture are local. However, with digitalization, cultural norms and ethical values are damaged universally.

It is difficult to protect privacy in an environment where the private becomes public. The public sphere is a social life zone outside the family and friendship environment and is very different from them (Sennett, 2002: 52). It is not easy to define the boundaries of privacy in a society where the distinctions between the private and the non-private, the public and the private, are increasingly blurred (Berman and Bruening, 2007: 306). The phenomenon of privacy constitutes an important part of human life, the boundaries and shape of privacy are shaped within the cultural understanding and according to the ethical codes of the society. Developments in digital technologies cause the concept of privacy to change its meaning and form, and sharing over social networks can threaten the perception of personal privacy and ethical values.

Being open to everyone's access and sharing anytime, anywhere eliminates the possibility of being out of sight and transforms the person into a common consumption object. The convenience provided by digital technologies to participate in daily life is turning people into a more public product day by day. Intelligent technologies that provide access to desired information anytime, anywhere push the limits of privacy, creating a strange situation such as being visible from anywhere (Bennett, 2018: 239; Grossberg, 1990: 41). Web 2.0 and Web 3.0 technologies, which enable social interaction and content creation, turn into an important privacy violation tool in the hands of careless users. While these developments provide many opportunities for people to be visible, they violate visibility's privacy and ethical dimensions.

Today, digital technologies are transforming cultures through social networks and eroding traditional judgments. Social networks, web 2.0 and web 3.0 technologies push the limits of control due to the opportunity to offer platforms where users can create content and cause the problem of protecting privacy and observing ethical attitudes and behaviors. Ethical problems caused by users becoming active content producers and consumers, together with social media, which constitutes the infrastructure of digital technologies, cause the erosion of cultural values. The rich content offered by digital technologies, on the one hand, allows the visualization of every moment of life; on the other hand, it causes the emergence of a new sharing culture that violates privacy and ethical boundaries. The fact that approximately 73% of the developing countries are Facebook users today while pushing the limits of privacy offers great opportunities for the surveillance of one's private life (Ono, 2018; Swinton, 2020; Hall, Kearney, & Xing, 2019: 1396). The desire of people to share their experiences with others and the curiosi-

ty of being watched and followed by them eliminates the distinction between private and public life and causes a violation of privacy.

Thanks to smart technologies, images, messages, and personal signs flow through internet systems. In this case, people cannot escape from surveillance. With the help of smart technologies, traditional privacy disappears, and the phenomenon of “online privacy” emerges; online privacy poses the risk that the information that individuals transfer to the Internet can be copied and passed into the hands of other people or institutions (Castells, 1996: 376; Saeri et al., 2014: 352). The legal infrastructure and legal regulations that exist at the stage of integrating technological developments into social life are insufficient to protect privacy. Information privacy is one of the most difficult areas to protect in the digital environment. Difficulties in solving the problem arise from the thought that the legal regulations to ensure confidentiality conflict with personal rights and freedoms.

Virtual surveillance, facilitated by digital technologies and, in a way, makes everyone willing to be visible in the global network, brings various risks. One’s health, bank accounts, religious belief, political opinion, ethnicity, sexual life, etc. Information on the subject can be used for purposes that are not in good faith (Yüksel, 2003: 211; Çalık and Toker, 2016: 9). This wide surveillance possibility expands the possibility of violation of privacy (Rigel, 2005: 275). While smart devices allow people to participate in social processes as active players, they also turn them into “objects of surveillance.” This reveals the strange situation of being visible all the time and everywhere and turning into the “general person.”

According to the results of the “Digital in 2020” research conducted by We Are Social and Hootsuite, the most dynamic social platform globally is Facebook with 2 billion 449 thousand users, while Youtube ranks second with 2 billion users. According to the research conducted by the application tracker AppAnnie in 2019, the four most downloaded applications of the decade belong to Facebook. The most downloaded app between 2010 and 2019 is Facebook’s main app, followed by the company’s Facebook Messenger app, with WhatsApp third and Instagram fourth (Shead, 2019; Snowden, 2018). Reaching a total of 2.4 billion users as of 2020, Facebook –ok has become the most populous country globally and has made its owners, together with its stakeholders, the richest and most powerful people globally. Individuals create the identities they design here. Allowing a self-design through filtered photos, selected relationships, and selected words, Facebook satisfies individuals’ feelings of being seen and appreciated in the modern world. Facebook founder Zuckerberg’s words that privacy is outdated reveal the company’s view of privacy.

3. METHOD

3.1. Research Design

This research is a descriptive statistical study, and data obtained from open sources were used to explain a certain situation. The descriptive statistical method compiles, collects, summarizes, and analyzes numerical data. As a difference from inductive statistics, descriptive statistics are to be carried out based on quantitative number values or counting or ranking values (Spiegel, Stephen, & Laryy, 2013:112). In this method, numerical values are presented in the form of graphics in order to help the reader's mind map. The descriptive statistics method was preferred in this research because a situation is explained with factual data and quantitative indicators and is suitable for generating hypotheses for future research.

3.2. Analysis of Data

Data analysis is an ongoing process of classifying and analyzing the collected data with appropriate techniques. Generally, two different techniques are used in data analysis, the first is the descriptive statistical method, where the population parameters can be directly accessed, and the parameters can be calculated directly. The other is the predictive statistical method, which analyzes the data obtained from the sample drawn impartially from the population in cases where the population parameters are not reached. (Tutar and Edem, 2020: 386; Salzmann and Erikson, 2018; Bazhair, 2014: 14; Lui, 2019). In this study, the descriptive statistical method was preferred because of the research problem situation and its compatibility with the main question of the research. In order to support formal analysis, as it is based on the analysis of quantitative data in the descriptive statistical method; Tables such as frequency count table, frequency distribution table, classification table and graphical descriptive statistical tools such as bar graph, box graph and histogram were used (Montalco et al., 2020; Büyüköztürk et al., 2016; Dimic et al., 2019; Reddy and Nallabolu, 2020).

4. Findings

4.1. Social Media Platforms Usage Analysis

This research presents data on social media platforms and internet usage rates. The data examined in the research were taken from the "Global Digital Overview" report published by We Are Social and Hootsuite in 2015. The data were turned into tables and graphs in the Excel program. It aims to determine the effective role of social media platforms and the Internet in the surveillance of the individual in the surveillance societies of the analyzed data. Social media platforms play an important role in surveillance today, where surveillance has become an object of desire. As indicated in Table 1, some social media platforms' number of active users between 2015 and 2020 is given. Active users

are individuals who regularly use these applications every month. Facebook has been the most used social media platform since its inception. The number of active users of Facebook, the first application to reach one billion users among social media platforms, is 2 billion 449 million as of 2020. Regarding the number of active users, Facebook is respectively; Youtube, WhatsApp, Instagram, Snapchat and Twitter followers. In the Instagram application, where mutual surveillance is experienced at the highest level, the number of active users has increased compared to years, and according to the data for 2022, the number of individuals using this application has exceeded one billion.

Table 1: The World's Most-Used Social Platforms by Years (In Millions)

Country/Year	2015	2016	2017	2018	2019	2020	2021
Argentina	4.3	3.2	3.32	3.09	3.18	3.11	3.22
Australia	2.1	1.2	1.39	1.39	1.31	1.44	1.46
Brazil	3.8	3.3	3.43	3.39	3.34	3.31	3.42
Canada	2.1	1.4	1.47	1.48	1.47	1.49	1.46
China	1.7	1.5	1.50	2.00	1.57	2.12	2.04
France	2	1.3	1.23	1.22	1.17	1.42	1.41
Germany	2.1	1.1	1.09	1.13	1.04	1.19	1.24
Hong Kong	1.8	1.5	1.41	2.01	1.47	1.57	1.57
India	2.5	2.3	2.36	2.26	2.32	2.24	2.25
Indonesia	2.9	2.9	3.16	3.23	3.26	3.36	3.14
Italy	2.5	2.0	2.00	1.53	1.51	1.57	1.52
Japan	0.7	0.3	0.40	0.48	0.36	0.45	0.51
Malaysia	3.5	3.0	3.19	3.00	2.58	2.45	3.01
Mexico	3.9	3.2	3.32	3.7	3.12	3.25	3.27
Netherlands	1.9	n.d.	n.d.	1.20	1.16	1.19	1.24
Philippines	4.3	3.7	4.17	3.57	4.12	3.53	4.15
Poland	2.1	1.3	1.45	1.42	1.45	2.00	1.59
Russia	2.6	1.9	2.19	2.19	2.16	2.26	2.28
Saudi Arabia	3.0	2.9	2.55	2.34	2.50	3.02	3.06
Singapore	2.5	1.6	2.07	2.06	2.08	2.08	2.17
South Africa	3.2	2.7	2.54	2.48	2.48	3.10	3.32
South Korea	1.3	1.1	1.11	1.12	1.09	1.13	1.08
Spain	1.9	1.6	1.41	1.38	1.39	1.51	1.54
Thailand	3.8	2.9	2.48	3.10	3.11	2.55	2.28
Turkey	2.9	2.5	3.01	2.48	2.46	2.51	2.57
UAE	3.6	3.0	3.24	2.56	2.59	2.57	2.55
UK	2.2	1.5	1.48	1.54	1.50	1.42	1.49
USA	2.7	1.7	2.06	2.01	2.04	2.03	2.07
Vietnam	3.1	2.3	2.39	2.37	2.32	2.22	2.21

Source: Hootsuite and We Are Social

Table 1 compares the daily usage times of social media platforms by country. When the table is examined, it is seen that the Philippines' use of social media has increased over the years. After the Philippines, the daily social media usage times are respectively; Mexico, Indonesia, Argentina and South Africa. One of the striking findings in Table 1, where daily social media times are compared to years, is that developed countries' social media usage times are less than in underdeveloped countries. The average daily social media time of Japan, which is at the peak of the world in producing smart device technologies, is 45 minutes according to 2020 data and 51 minutes in 2021. The main result is that the developed countries that produce the technology spend less time on social media platforms than less developed countries. The time spent on social media, which is one of the important surveillance tools, is high in underdeveloped countries, making those countries open to surveillance. Table 2 shows the daily time spent by social media users on these platforms. Remembering the words of the Facebook boss, who said that privacy is outdated here, it is necessary to consider that people spend the most time here.

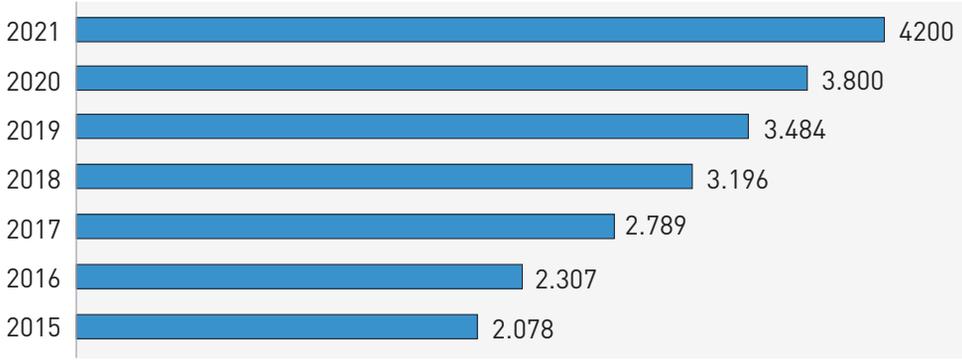
Table 2: Time Spent on Social Media by Year

Social Platforms / Years	2015	2016	2017	2018	2019	2020	2021
Facebook	1.336	1.550	1.871	2.167	2.271	2.449	2.740
Youtube	n.d.	n.d.	1.000	1.500	1.900	2.000	2.291
Twitter	284	320	317	330	326	340	353
Instagram	300	400	600	800	1.000	1.000	1.221
Snapchat	100	200	300	255	287	382	498
WhatsApp	600	900	1.000	1.300	1.500	1.600	2.000

Source: Hootsuite and We Are Social

According to January data in We Are Social and Hootsuite's report, 62.7 million internet users, are in Turkey. This number is 4 percent higher than in the same period of 2019. According to the 2019 data from the Turkish Statistical Institute (TUIK), 75.3 percent of the population in Turkey uses the Internet. This rate is 81.8 percent among men and 68.9 percent among women. When the data for the last ten years are analyzed, it is seen that the rate of internet usage has increased from year to year. According to the 'Digital 2020' report, looking at the world average, users' daily time on the Internet is 6 hours and 43 minutes. In Turkey, on average, 7 hours and 29 minutes are spent per day on the Internet. When the 16-64 age group is analyzed, Turkey ranks 12th among 42 countries regarding time spent on the Internet.

Graphic 1: Social Media Usage Data by Year in The World (In Billion)

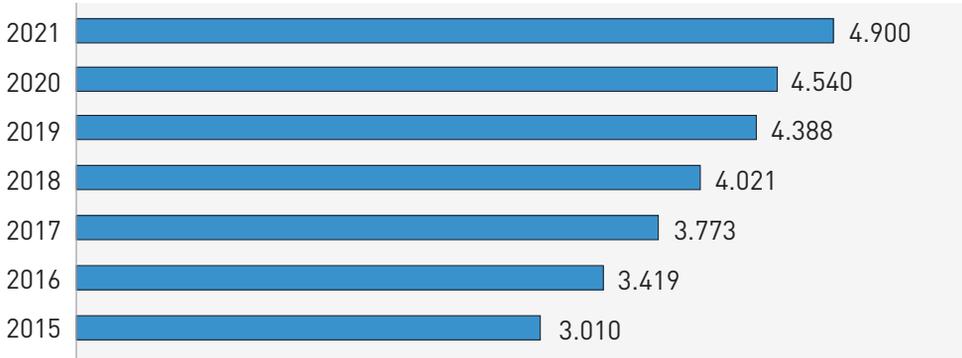


Source: Hootsuite and We Are Social

The number of users of social media platforms worldwide is given in Graph 1. As indicated in Chart 1, various social media platforms have increased between 2015 and 2021. According to the data for 2021, half of the world's 7 billion 837 million population are social media users.

4.2. Internet Usage Analysis

Graphic 2: Internet Usage Data by Year in The World (In Billion)



Source: Hootsuite and We Are Social

The internet usage analysis section of the research presents the usage rates and tools of the Internet, which is one of the surveillance practices without being seen in surveillance societies. As shown in Graph 2, a continuous increase in internet usage has been observed since 2015. According to the data for 2021, four billion 900 million people in the world are actively using the Internet. According to these data, it is understood that more than half of the world's population is under surveillance without being seen and is open to privacy violations.

Graphic 3: Data of Smartphone Users Worldwide (In Billion)



Source: Statista

Smartphones are the most widely used device among smart device technologies globally. In Graph 3, smartphone usage rates between 2015 and 2021 are given. In 2015, 1.86 billion smartphone users increased to 3.05 million in 2021.

Discussion and Conclusion

While people live together as a society, they seek the possibility of living together without harming each other. However, the question of how much this non-harming situation is possible with new communication technologies is of great importance. The features of new communication technologies such as interactivity, demassification and asynchrony make this non-harming situation significantly risky Everett (Rogers, 1986: 4–5). Mutual interaction enables the two-way communication process between the source and the receiver and differentiates new communication technologies from the one-way operation in mass communication. Individuals defined as the target audience in mutual interaction are no longer passive but active subjects in the communication process. Using these technologies by active subjects in line with their own will may cause privacy violations. Here, de-massification means the customization of messages sent to large user audiences. This privatization situation also poses the risk of sharing the private. The asynchronous feature of new communication technologies eliminates the necessity of sending messages reciprocally and instantly between the source and the receiver.

Digital manipulation resulting from the digitization of technology is an important ethical problem. This inevitably leads to an intense flow of disinformation. In social life shaped by new communication technologies, the perception of reality emerges as an illusion. It is possible to replace the real with the imitated fake reality with the desired and continuous reality production. Reality gradually moves away within the simulations that emerged in this process (Baudrillard, 2014: 41; Sartori, 2004: 24). Accordingly, as a result of the development and widespread use of new communication technologies,

the border between the real and the fake is gradually disappearing, and this situation causes the perception of privacy in the society to be damaged (Robins, 2013: 35). Unlimited sharing of information without the barrier of time and space touches the concept of freedom of information and communication and conflicts with the concepts of security and privacy within the scope of privacy on the other end.

Conceptualized as the culmination of a privacy breach, virtual surveillance is one of the major risks undermining personal security and privacy. Virtual surveillance, facilitated by new communication technologies and, in a way, making everyone volunteer to be visible in the global network, brings various dangers and risks. From this point of view, there are increasing doubts that private life and privacy will narrow even more in the future. Surrounded by these technologies, individuals are forced to choose between security and freedom; These tools, which promise freedom to individuals, also restrict privacy (Yüksel, 2003: 211; Çalık and Toker, 2016: 9). In a global network where information security cannot be provided, personal privacy is not taken care of, and continuous surveillance is possible, it becomes necessary to control and control digital crimes.

Another point regarding surveillance and privacy that should not be ignored is the cultural variable. Another issue is that the dimensions of privacy can change from society to society and from period to period. In Western culture, the privacy of the human body requires its inviolability in the public sphere, while in eastern societies, privacy requires protection from the gaze of the other. While privacy in the west is limited to the sense of touch, privacy is spread over a wide area, including the sense of sight in the east. Regardless of which sense it is associated with, privacy is related to immunity, and touching the body or the eye is an ethical violation of immunity.

As a result, digital technologies indeed bring many opportunities, and digital transformation is an indispensable part of our lives in today's reality. However, it should not be ignored that threats, dangers, and opportunities arise with every new technology (Merriam-Webster, 2021). Therefore, instead of reducing technology as a concept to just tools, it is an application of technology, an understanding that requires mastery of doing a job. Protecting personal data against threats and attacks from the digital environment and developing awareness of the privacy and confidentiality of personal data constitute an important pillar of information security. As digital technologies develop, the importance of increasing awareness about personal data privacy and protecting personal data is increasing.

Author Contributions: Hasan Tutar and Ceren Güler Çağıltay have contributed to all parts and stages of the study. The authors contributed equally to the study.

Conflict of Interest: No conflict of interest exists among the authors and /or any institution.

Acknowledgment: We would like to thank the referees who contributed to the publication process

Etik Beyanı: Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazar beyan eder. Aksi bir durumun tespiti halinde Kamu Yönetimi ve Teknoloji Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarlarına aittir.

Yazar Katkıları: Hasan TATAR ve Ceren Güler ÇAĞILTAY çalışmanın tüm bölümlerinde ve aşamalarında katkı sağlamışlardır. Yazarlar esere eşit oranda katkı sunmuştur.

Çıkar Beyanı: Yazarlar ya da herhangi bir kurum/ kuruluş arasında çıkar çatışması yoktur.

Teşekkür: Yayın sürecinde katkısı olan hakemlere teşekkür ederiz.

Ethics Statement: The author declares that the ethical rules are followed in all preparation processes of this study. In the event of a contrary situation, the Journal of Public Administration and Technology has no responsibility and all responsibility belongs to the author of the study.

Author Contributions: Hasan TATAR and Ceren Güler ÇAĞILTAY have contributed to all parts and stages of the study. The authors contributed equally to the study.

Conflict of Interest: There is no conflict of interest among the authors and/or any institution.

Acknowledgement: We would like to thank the referees who contributed to the publication process.

Bibliography

- Aimeur, E., Gambs, S. ve Ho, A. (2010). Towards a Privacy-Enhanced Social Networking Site. 2010 International Conference on Availability, Reliability and Security içinde (s. 172-179). <https://doi.org/10.1109/ARES.2010.97>
- Allen, D. S. (2008) "The Trouble with Transparency: The Challenge of Doing Journalism Ethics in a Surveillance Society," Journalism Studies, 9(3), s. 323-340. <https://doi.org/10.1080/14616700801997224>
- Amitay, G.,&Rahav, G. (2020). "The Map and the Territory: a Subversive Synopticon in an Alternative Educational Space," International Studies in Sociology of Education, s. 1-20.<https://doi.org/10.1080/09620214.2020.1766373>
- Baudrillard, Jean (2014). Simülakrlar ve Simülasyon, (Çev: Oğuz Adanır),Ankara: Doğu-Batı Yayınları.
- Bauman, Z. & Lyon, D. (2018) Akışkan Gözetim, İstanbul: Ayrıntı Yayınları
- Bazhair, A. (2014). "Factor Performance for ERP Systems Acceptance a Descriptive Statistical Analysis from Saudi Arabia Companies" International Journal of Managerial Studies and Research, 2(9), s. 14-22
- Bennett, C. J. (2018) "The European General Data Protection Regulation: An instrument for the Globalization of Privacy Standards?", Information Polity, 23(2), s. 239-246. <https://doi.org/10.3233/IP-180002>
- Bentham J. (2008) Panoptikon - Gözün İktidarı, (Z. Özarıslan ve B. Çoban çev.). İstanbul: Su Yayınevi.
- Berman, J. & Bruening, P. (2007) Is Privacy Still Possible in the Twenty-First Century? Social Research, 68(1), s. 306-318.
- Berkup, S. B. (2015) Sosyal Ağlarda Bireysel Mahremiyet Paylaşımı: X ve Y Kuşakları Arasında Karşılaştırmalı Bir Analiz. Doktora tezi, Ege Üniversitesi, İzmir, Türkiye
- Boyd, D. ve Hargittai, E. (2010) Facebook Privacy Settings: Who cares?. First Monday, 15(8). <https://doi.org/10.5210/fm.v15i8.3086>
- Bozkurt, V. (2014) Endüstriyel, Post Endüstriyel Dönüşüm, Bilgi, Ekonomi, Kültür, Bursa: Ekin Basım Yayın Dağıtım.
- Buchenscheit, A., Könings, B., Neubert, A., Schaub, F., Schneider, M., ve Kargl, F. (2014) Privacy Implications of Presence Sharing in Mobile Messaging Applications. Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia içinde (ss. 20-29). New York, USA: ACM. <https://doi.org/10.1145/2677972.2677980>

- Büyüköztürk, Ş.; Çakmak, E. K.; Akgün, Ö. E.; Karadeniz Ş. & Demirel, F. (2016) Bilimsel Araştırma Yöntemleri. 20. Baskı. Ankara: Pegem Akademi <https://doi.org/10.14527/9789944919289>
- Castells M., (2005) Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Ağ Toplumunun Yükselişi, Cilt 1. (Çev. Ebru Kılıç). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- Cormack, A. (2019) "See No..., Hear No..., Track No: Ethics and the Intelligent Campus", J. Inf. Rights Policy Pract, 41, s. 1-23. <https://doi.org/10.21039/irpandp.v3i1.59>
- Çakır, M. (2015) İnternette Gösteri ve Gözetim: Eleştirel Bir Okuma, Ankara: Ütopya Yayınevi.
- Çalık, D. & Toker, G. (2016) "Ekran Çağı İnsanı ve Dijital Toplum", XXI. Yüzyılda Türkiye'de İnternet Konferansı, 03-05 Kasım 2016, Ankara: TED Üniversitesi.
- Çaycı, A. E. & Çaycı, B. (2017) "Dijital İletişim Çağında Teknolojinin Açığa Çıkarttıkları: Gözetim ve Mahremiyet", The Turkish Online Journal of Desing, Art and Communication, 7(1), s. 36-46.
- Çaycı, B. & Karagülle, A. E. (2014) "X Kuşağından Z Kuşağına Değişen Mahremiyet Algısı", A. Z. Özgür, M. Barkan, A. İşman, E. Yolcu (Ed.), International Trends And Issues İn Communication & Media Conference (s. 190-196). Dubai, UAE.
- De Laat, P. B. (2008) "Online Diaries: Reflections on Trust, Privacy, and Exhibitionism," Ethics and Information Technology, 10(1), s.57. <https://doi.org/10.1007/s10676-008-9155-9>
- Dinev, T. & Hart, P. (2005) "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact," International Journal of Electronic Commerce, 10(2), s.7-29. <https://doi.org/10.2753/JEC1086-4415100201>
- Dolgun, U. (2005) İşte Büyük Birader, İstanbul: Hayy Kitap Yayınları.
- El Saddik, A. (2018) "Digital twins: The Convergence of Multimedia Technologies," IEEE Multimedia, 25(2), s.87-92. <https://doi.org/10.1109/MMUL.2018.023121167>
- Erdem, B. K. & Kaya, M. (2019) "Instagram'da Görülme ve Beğenilme Arzusu: Kullanıcı Bakış Açısından Değerlendirme", Uluslararası Sosyal Araştırmalar Dergisi, 12(62), s.1457-1464. <https://doi.org/10.17719/jisr.2019.3154>
- Flanagan, V. (2014) Surveillance Societies: Privacy and Power in YA Fiction. In Technology and Identity in Young Adult Fiction, London: Palgrave Macmillan. <https://doi.org/10.1057/9781137362063>
- Foucault, M. (1992) Hapishanenin Doğuşu, (Kılıçbay, M. çev.) Ankara: İmge Kitapevi.
- Fukuyama, M. (2018) "Society 5.0: Aiming For A New Human-Centered Society", Japan

Spotlight, 27, s.47-50.

- Gandy, Jr. & Oscar, H. (1989) The Surveillance Society: Information Technology and Bureaucratic Social Control. *Journal of Communication*, 39(3), s.61-76 <https://doi.org/10.1111/j.1460-2466.1989.tb01040.x>
- Giddens,. A. (2010). Mahremiyetin Dönüşümü, (Çev.: G. Şahin) İstanbul: Ayrıntı Yayınları.
- Giddens, A. (2005) *Ulus Devlet ve Şiddet*, (Atay, C. çev.), İstanbul: Kalkedon Yayınları
- Granrath, L. (2017) Japan's Society 5.0: Going Beyond Industry 4.0. <https://www.japanindustrynews.com/2017/08/japans-society-5-0-going-beyondindustry-4-0/>
- Grossberg, M. (1990) Some Queries About Privacy and Constitutional Rights. *Case W. Res. L. Rev.*, 41, s.857.
- Gücüyener, M. (2011) *Panoptik Gözetimden Synoptisizme Gözetim Toplumu (Yüksek Lisans Tezi)*, Afyon Kocatepe Üniversitesi Sosyal Bilimler Enstitüsü: Afyon.
- Güven, S. K. (2011) "Gözetimin Toplumsal Meşruiyeti", *Medya Mahrem.* İstanbul: Ayrıntı Yayınları
- Guetl, C. & Chang, V. (2008) "Ecosystem-based Theoretical Models for Learning in Environments of the 21st Century" *International Journal of Emerging Technologies in Learning (IJET)*, 3(1), 50-60. <https://doi.org/10.3991/ijet.v3i1.742>
- Hall, J. A., Kearney, M. W., & Xing, C. (2019) "Two Tests of Social Displacement Through Social Media use," *Information, Communication & Society*, 22(10), s.1396-1413. <https://doi.org/10.1080/1369118X.2018.1430162>
- Hughes-Roberts, T., & Kani-Zabihi, E. (2014) "Online Privacy Behavior: Using User Interfaces for Salient Factors," *Journal of Computer and Communications*, 02, s. 220. <https://doi.org/10.4236/jcc.2014.24029>
- Kaya, C. (2011) "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas Veriler ve İşlenmesi", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 69 (1), s. 317-334.
- Kokolakis, S. (2017) "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security*, 64, 122-134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Lyon, D. (2003) "Surveillance Technology and Surveillance Society," *Modernity and Technology*, s.161-184.
- Martin, A. (2008) "Digital Literacy And The "Digital Society." *Digital literacies: Concepts, Policies and Practices*, 30, s.151-176.
- Merriam-Webster. (2021) *Technology*. <https://www.merriamwebster.com/dictionary/technology>

- 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), s. 103-125. <https://doi.org/10.1057/ejis.2013.17>
- Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2008) *Digital Citizenship. The Internet, Society, and Participation*. Cambridge: The MIT Press. <https://doi.org/10.7551/mitpress/7428.001.0001>
- Orwell, G. (2004) *Bin Dokuz Yüz Seksek Dört*, (çev. Nuran Akgören) İstanbul: Can Yayınları.
- Ridley-Siebert, T. (2015) "Data privacy: What the Consumer Really Thinks. *Journal of Direct*", *Data and Digital Marketing Practice*, 17, s. 30-35. <https://doi.org/10.1057/ddmp.2015.40>
- Rigel, N. (2005) *Kadife Karanlık' 21. Yüzyıl İletişim Çağını Aydınlatan Kuramcılar*. İstanbul: Su Yayınevi, s.275
- Pitkänen, O., & Tuunainen, V. K. (2012) *Disclosing Personal Data Socially An Empirical Study on Facebook Users' Privacy Awareness*. *Journal of Information Privacy and Security*, 8(1), s.3-29. <https://doi.org/10.1080/15536548.2012.11082759>
- Robins, K. (2013) *İmaj: Görmenin Kültür ve Politikası*, (Çev: Nurçay Türkoğlu), İstanbul: Ayrıntı Yayınları.
- Robison, W. L. (2017) "Digital Privacy: Leibniz 2.0", *Orbit Journal*, 1(2), s.1-9. <https://doi.org/10.29297/orbit.v1i2.54>
- Rogers, E. M. (1986). *Communication Technology: The New Media in Society*, New York: The Free Press
- Saeri, A. K.,Ogilvie, C., La Macchia, S.T., Smith, J. R., & Louis, W. R. (2014). "Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior," *The Journal of Social Psychology*, 154(4), 352-369. <https://doi.org/10.1080/00224545.2014.914881>
- Salzmann-Erikson, M. & Erikson H.(2018) "A Descriptive Statistical Analysis of Volume, Visibility, and Attitu Dersearding Nursing and Care Robots in Social Media, Contemporary Nurse," *Social Media, Technology and Communication* 54(1) <https://doi.org/10.1080/10376178.2017.1388183>
- Sartori, G. (2004) *Görmenin İktidarı Homo Videns: Gören İnsan*, (Çev: Gül Batuş ve Bahar Ulukan), İstanbul: Karakutu Yayınları
- Sennett, R. (2002). *Kamusal İnsanın Çöküşü*. (2 b.). (S. D. Yılmaz, Çev.) İstanbul: Ayrıntı.

- Shead, S. (2019) "Facebook, On Yılın En Çok İndirilen Dört Uygulamasına Sahip", bbc.com,23.06.2021, [https:// www.bbc.com/news/technology- 50838013](https://www.bbc.com/news/technology-50838013)
- Snowden, E. (2018) "Facebook Bir İstihbarat Şirketi", Bianet, 23.06 2021. [https://m.bianet.org/bianet/dun ya/195348-snowden-facebook-bir-istihbarat-sirketi](https://m.bianet.org/bianet/dun_ya/195348-snowden-facebook-bir-istihbarat-sirketi)
- Spiegel, Murray R, & Stephens, Larry J. (2013) İstatistik, (Tr.Çev.: Çelebioğlu, Salih) İstanbul: Nobel Akademik Yayıncılık
- Swinton, J. J. (2020) "Extension Needs Outreach Innovation Free from the Harms of Social Media," Journal of Extension, 58(2), s.1.
- Tan, Q., & Pivot, F. (2015). Big Data Privacy: Changing Perception of Privacy. 2015 IEEE International Conference on Smart City içinde (ss. 860-865). <https://doi.org/10.1109/SmartCity.2015.176>
- Tutar, H. & Erdem, A. T. (2020) Örnekleriyle Bilimsel Araştırma Yöntemleri. Ankara: Seçkin Yayıncılık.
- Yüksel, M. (2003). "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi",Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi, 58 (1), s. 181-213 https://doi.org/10.1501/SBF-der_0000001619
- We Are Social &Hootsuite. (2015-2021). Digital 2015-2020: Global Digital Overview. Retrieved From: <https://datareportal.com/reports/digital-2015-global-digital-overview>