İletişim Kuram ve Araştırma Dergisi - Sayı 56 /Kış 2021
Ankara Hacı Bayram Veli Üniversitesi
İletişim Fakültesi
Süreli Elektronik Dergi
E-ISSN: 2147-4524

Digital Surveillance and Ethics as a New Risk Factor within the Context of Regulations on the Internet Law[*]

İnternet Yasası Düzenlemeleri Bağlamında Yeni Bir Risk Unsuru Olarak Dijital Gözetim ve Etik

Esra Serdar Tekeli, Öğr. Gör. Dr., Ankara Hacı Bayram Veli Üniveristesi, İletişim Fakültesi, E-posta: esraserdar84@gmail.com

https://doi.org/10.47998/ikad.981054

Keywords:

Surveillance,
Surveillance Society,
Internet Regulations,
Digital Risk,
Ethics.

Abstract

Surveillance, as an important matter in the modern era, continues its existence as a former phenomenon of the digital world with new forms. Another output of the modern era is the ever-increasing and diversified phenomenon of risk. In this study, internet regulations were discussed as digital surveillance practices in the context of concepts such as "risk" "supervision" and "control" based on Lyon's "Surveillance Society" theory. While internet regulations are addressed as a governmental action and an effort to gather information about people, they are also considered a new risk factor for the surveillance practice and surveillance parties in the modern era. Based on these statements, the aim is to reveal how concepts such as risk and supervision, which are the main antecedents of today's digital surveillance, can be associated with ethical values such as "confidentiality" and "privacy", which are also subject to legal regulations. It is identified in what ways the internet regulations are considered a surveillance practice and how digitalized risks meet with surveillance actors at the point of digital surveillance risk. On the other hand, the relationship was shown by demonstrating how the risks as surveillance actors can be categorized in terms of state and individual. The study examines the relationship between the regulatory framework and ethical elements in a descriptive way as well as shedding light on today's digital surveillance. The existence of risks is common to lawmakers, who are the surveillance actors, and people under the law and this legitimizes digital surveillance.

Anahtar Kelimeler:

Gözetim,
Gözetim Toplumu,
İnternet
Düzenlemeleri,
Dijital Risk,
Etik.

Öz

Modern dönemin önemli bir kavramı olarak gözetim, dijital dünyanın eski bir olgusu olarak yeni formlarıyla sürmektedir. Modern dönemin bir diğer getirisi de artan ve çeşitlenen risk olgusudur. Bu çalışma, dijital gözetim pratikleri olarak internet düzenlemelerini, Lyon'un "gözetlenen toplum" kuramından hareketle "risk" "denetim" "kontrol" gibi kavramlar bağlamında ele almaktadır. İnternet düzenlemelerini, bir devlet eylemi üzerinden bireyler hakkında bilgi toplama çabası olarak ele alırken, aynı zamanda modern dönem gözetim pratiği ve gözetim tarafları açısından yeni bir risk unsuru olarak değerlendirmektedir. Bu iki kabulden hareketle, bugünün dijital gözetiminin ana öncülleri olan risk ve denetim gibi kavramların, yasal düzenlemelere de konu olan "gizlilik", "mahremiyet" gibi etik değerlerle nasıl ilişkilendirilebileceğinin ortaya konması amaçlanmaktadır. İnternet düzenlemelerinin hangi açılardan bir gözetim pratiği olduğu ve dijitalleşen risklerin gözetim aktörleriyle dijital gözetim riski noktasında nasıl buluştuğu belirlenmektedir. Diğer taraftan risklerin, gözetim aktörleri olarak devlet ve birey açısından nasıl kategorileştirilebileceği ortaya konarak bu ilişki gösterilmeye çalışılmıştır. Makale, bugünün dijital gözetimine ışık tutarken, düzenleyici çerçeve ile etik unsurlar arasındaki ilişkiyi betimsel bir analizle incelemektedir. Risklerin varlığı, gözetim aktörleri olan yasa yapıcılar ve yasa muhatapları açısından ortaktır ve bu durum dijital gözetimi meşrulaştırmaktadır.

[*] This article was produced from the doctoral thesis titled "Surveillance in New Communication Tools: Twitter Ban and Internet Law" at Gazi University, Institute of Social Sciences, Department of Journalism.

Araştırmacı Orcid ID : 0000-0003-2909-4832
Geliş Tarihi : 10.08.2021
Kabul Tarihi : 16.11.2021

Introduction

With the developing technologies, surveillance processes have been integrated into our lives faster and more versatile. If the first condition of being a surveillance society is the routine monitoring of daily life, today's societies are now surveillance societies in every way. What makes today different oversight is its "invisibility", in parallel to its being more visible with increased risk factors. Invisibility can be defined as "non-perspectivity" from another point of view[1]. At this point, the "eyes" are everywhere in both points of view. Ones subjected to digital surveillance areas are the subject of this non-perspectivity, not by being closed in a virtual environment that promises unlimited freedom, but taking an active part in the action of exposing themselves. In this context, surveillance, as an important phenomenon of the modern world, is progressing with an emphasis that exists on a global and national scale and constantly transforms itself. This transformation creates a new surveillance culture with increasing information and ownership of knowledge through new communication technologies and circulates both individuals and states as parties to surveillance. At this point, while surveillance becomes digital, it abstracts its target audience as the watcher-watched. In this way, a culture of surveillance is formed and this concept is perfect for describing the modern digital surveillance world, because it is no longer an external factor of our lives, but a structure with which citizens interact in every positive and negative way (Lyon, 2017: 825). Surveillance, which has become a practice that is internalized and included in daily life rather than a disciplinary tool or control mechanism, has become the focus of different discussion topics with its new forms.

The first of these discussion topics is how surveillance, which has been taking place in all societies since the first ages of history, has become so dominant, as a phenomenon as old as the history of humanity. With the remarks of Foucoult-Deleuze, it is a matter of panoptic power that spies on the "existed" and the post-panoptic power that spies on "might exist" (Baştürk, 2016: 13). The urge to know towards a life that is placeless-homeless-codeless, and in which the norm is postponed, is the main subject of this issue[2]. What has brought the subject to its current state is the developments in new communication technologies. On the other hand, it can be said that state surveillance on a global scale became visible with the 9/11 attacks and became clear with the Snowden incident. The incident is the disclosure of documents regarding illegal surveillance by an employee of American Intelligence Organization and software expert Edward Snowden.

Another issue is the diversification of risks, which we can consider as a precursor to surveillance, with the modern period. This diversity provides the purpose of legitimizing surveillance, especially in terms of power and administration holders. Risk has a cultural significance in contemporary societies. There may be risks related to many issues such as health, safety, dangerous crimes, transportation, and the environment (Skinns, Scott, & Cox, 2011). For instance, security is a risk factor in all societies and ensuring security will lead to surveillance actions. Therefore, the risks positioned at the midpoint of the

[1] Chul- Han, in his study "The Society of Transparency", states that modern surveillance is a new panoptic process and defines this panoptic process as "non-perspectivity".

[2] For a detailed discussion, see. Baştürk, E. The Genealogy of Surveillance, A Postmodern Archaeology from Foucoult to Deleuze. Istanbul: Kalkedon Publications, 2016

surveillance society debates form the basis of the discussions. At this point, it would not be wrong to present the internet and all digital activities, which spread surveillance to all areas of society, as “new contemporary risk creators”. As a matter of fact, the internet is also unsettling as an area that contains many risks of the physical world and abstracts these risks. Therefore, surveillance can also be defined as the practice of dealing with risks.

In this new digital surveillance universe, where we have all become the object of categorical monitoring as digital citizens[3], new risk factors arise for those who use and provide internet platforms. Digitalized surveillance has expanded the boundaries of the concepts of surveillance state and surveillance society, and opened the discussion of risk society over the imbalance of security and freedom. In the axis of these discussions, the legal regulations on which the surveillance strategies used by the states to ensure the legitimate order and allocate security are based, are perhaps the most controversial areas. The Internet Law No. 5651, which regulates the Internet in our country, can be seen as a promise of security brought by the discourse of increasing risk. However, this point leads us to ethical violations, which is another problematic area of the digital world: Because while increasing risks lead to deeper surveillance, it brings up the violation of personal rights such as personal data security, privacy and privacy as an important issue of digital ethics. In this context, the study deals with “why are surveillance, risk, and auditing intertwined?”, “How are risks positioned in the relationship between the supervisor and the supervised within the framework of legal regulations?” Questions such as these were tried to be answered with a descriptive analysis. For this purpose, the study examines surveillance from a historical perspective and discusses legal regulations as a surveillance practice of late modern societies on the basis of concepts such as risk, control and supervision; it questions how risk and threat perceptions are managed through legal regulations in the security-freedom dilemma and how the mentioned digital risk elements can be positioned in the debates on the parties of surveillance and ethics.

From Traditional “Monitoring” to Digital “Eyeing”

In a general definition, surveillance is a control-oriented “predictability” system that takes place in the context of domination relations. There is a large literature studying the nature, causes, processes, global and historical transformation of surveillance (Lyon, 2006, 2012, 2013, Giddens, 2005, Fuchs, 2015, Bauman and Lyon, 2013, Marx (2002), Haggerty and Tetrault., 2017, Haggerty et al, 2011, Mattelart, 2012). However, Lyon’s work is of particular importance as it reveals how surveillance is transformed by computer and electronic communication networks. With the definition “All societies that depend on communication and information technologies for their management and control functions are ‘societies that are watched’”, Lyon describes a structure that puts different sub-dynamics next to technology, such as the information society, network society, and globalizing society, and that arises from the new modern system. In the thoughts that he asserted regarding surveillance, dominance of September 11 attacks are seen. To this end, Lyon states September 11 attacks are functional in terms of globalization and statification

[3] Emphasis belongs to David Lyon.

of surveillance and that it constitutes a starting point in the attempts to create surveillance systems to prevent future attacks (Lyon, 2013:28). In the evaluations that can be made for the parties of the surveillance, it can be mentioned about the follow-up cooperation. Stating that this cooperation is the most striking feature of contemporary surveillance, Lyon mentions that it succeeds in persuading the opposites and working together in reality (Bauman and Lyon, 2013:31). As a matter of fact, with the discourse of national security threat, individuals' perception of freedom and privacy may succumb to the need for security.

The tendency to classify surveillance as historical is evident in all publications that study the subject academically. James Rule, who is known to have implemented the first academic studies on surveillance, stated that surveillance practices emerged in England and America, especially with the 1960s, and discussed surveillance as a social control mechanism (Rule, 1974). This approach is important in that it reveals the beginning of modern surveillance. However, although surveillance is seen as a practice of modern society, it is known that it is based on a very old history. For example, surveillance practices in pre-modern societies are based on informal social control mechanisms. Small-scale communities are controlled by societal norms. In this period, surveillance rather aims to discipline. For this purpose, it counts, assorts, classifies and records individuals. In all these processes, writing has an important role, and the invention of writing has enhanced state power and increasingly systematized surveillance (Giddens, 2000). With the rise of modernity, surveillance as the basis of the nation-state has become an element of all types of organizations and historically dependent on capitalism (Giddens, 2018:64).

In this context, traditional surveillance, modern and post-modern surveillance can be mentioned in a general classification. Accordingly, while traditional surveillance aims to discipline individuals and events by keeping them in a certain framework through non-systematic data collection and classification, modern surveillance works with the element of "control" (Lyon, 1997; Dolgun, 2008; Çakır, 2015). Mattelart (2012) conducts this discussion on the axis of "discipline" and "control" societies. Accordingly, unlike the disciplinary society, which manages its authority over the human body and where the individual is not the subject of communication but the object of knowledge, the security society applies its power to the society and human lives as a whole (Mattelart, 2012:16). As a result, the security society improves surveillance by incorporating the application areas of the disciplinary society.

When the concepts of surveillance and discipline are considered together, Foucault comes to mind. According to Foucault (1979:201), discipline is essential in social modernity where "communities are broken down with divided individualities". In the analyses of Foucault, "supervision nets" are structured and spread under the monopoly of governmental power. Such a governmental power can be seen both at a micro and macro scale in all social relationships. Foucault does not directly point out the effects of new communication technologies on surveillance and control. However, Bentham's use of the panopticon metaphor shifts the focus of contemporary theory to surveillance and control processes (Turner, 1996). On the other hand, Foucault believes that the process of discipline has achieved its ideal form in the panopticon (Foucault, 2015:18). In this context, Faoucault, incorporating the panopticon architecture developed by Samuel and Jeremy Bentham into an academic discussion area, is a prominent figure who addresses the panopticon in discursive and philosophical aspects, and contributes to the institutionalization of surveillance.

In modern structures, where the citizen turns into an individual and the collective into an individuality (Bauman, 2017: 69), the features that are filed, transparent, sceptical, have a reduced tolerance for risk and emphasize protection, come to the fore (Marx, 2015:735). This phenomenon has created a process in which individuals follow each other in societies. Therefore, top-to-bottom discipline has been replaced by surveillance. As of the 19th century, multiple components such as nation-state formation, the desire of states to protect themselves against internal and external threats, the rise of the state will, bureaucratic order and military structure formed the modern period surveillance (Dolgun, 2008). As Lyon (2006:14) draws attention to this phenomenon, it is seen that surveillance includes both protection and precaution in terms of both enabling and setting limits, on the other hand, it has the purpose of control and supervision.

The post-modern dimension of surveillance, on the other hand, represents a post-panoptic surveillance structure as a "fluid" version of modernity (Bauman and Lyon, 2013: 11-12). In this new process, which we can also call the digital panopticon, surveillance is not only focused on "seeing", but also includes the desire to "know/be known". The important point here is not the increasing importance of knowing, but the simultaneous renewal, deepening and necessity of the state and society's claim to know, control and secure (Beck, 2011:359). In order to know, data and the potential to access data are important. Data access is also provided through the surveillance process.

The digital panopticon is more "personal data" oriented than the previous era. Because today, all the details of our personal lives are kept under record by the state or private institutions/organizations. Compared to previous years, these records are stored as digital records in addition to being written. As a post-panoptic archive, these records are a wide individual portfolio ranging from our demographic characteristics to the passwords we use, from our credit cards to our health information, from our educational status to all our personal areas. As individuals, we all voluntarily transmit this information. In this flow of information, Web 2.0 technologies, which transform communication into an interactive structure by introducing social media platforms into our lives, have a great impact. At this point, it is possible to face certain risk factors as digital citizens who have approved a kind of "voluntary surveillance" within a post- panoptic surveillance culture. On the other hand, the fact that states record and process this information has a significant relationship with the risk factor in terms of being measures against certain risks.

Slogobin's typification is also important in understanding today's post-modern surveillance. Accordingly, Slogobin (2007:3), who conceptually examines surveillance under three separate headings, calls them "communicative", "physical" and "operational" surveillance. "Physical surveillance" is the real-time monitoring of physical activities through devices such as the naked eye, video, camera. "Communication surveillance" is the monitoring of real-time communication for wiretapping, hacking, interception of verbal expressions in electronic media. “Operation surveillance” is, unlike the other two, involves accessing records obtained through physical and communicative surveillance. It also includes accessing the complementary elements of transactions (such as the address of the e-mail recipient) (Slogobin, 2005:2). In this context, transaction surveillance, as a post- panoptic surveillance element, shows the characteristics of the post-modern period. And, relative to other types, it encompasses the acquisition of deep and pervasive knowledge.

As can be seen, in all the classifications put forward, an increasing rate of supervision and control, protection and precaution are encountered. It can be said that the increase in supervision and control is a reaction to changes in social structure. With this determination, risk structures that have increased quantitatively and transformed qualitatively in the modern period cause more surveillance.

Digital Surveillance as a New Risk Aspect

Risk, as one of the four main themes that Lyon emphasizes in the scrutinized society discussions, constitutes the starting point of the theoretical discussions on surveillance. The concept, which appears in many aspects in surveillance processes, is getting rid of its previous meanings in the modern world as a part of the modernization process. Risk, which is the oldest phenomenon of human action and has transformed into a meaning and action that threatens all humanity and societies from its meaning that evokes courage and adventure in the past, is an allusion to the modernization process and is politically reflexive (Beck, 2011:24-25). In Beck’s theory of risk society, risks alter, consume and transform normative reality. This transformation causes the individual to be defined as more or less risky, not good or bad in the risk society. For this, the collection of personal data is necessary to keep possible threat elements within a certain framework. In the risk society, it is the states’ duty to prevent evil and minimize the undesirable consequences of technology. Modernity, as social systems structured within the framework of time-space, full of risks and dangers, has led to the emergence of technologies that process personal data in order to cope with increasing risk trends. Therefore, new technologies are not only new risk intermediaries, but also new sources of risk. In this context, there are important intersections between risk and digitality (Lupton, 2016:302). The first of these intersections is that risky phenomena have the opportunity to spread more through digital technologies. On the other hand, the use of digital technologies is a risk factor in itself. And also, the risk of “digital divide”, which arises as a result of the inequality of use of digital technologies, appears to be another type of risk. All these problems arise from the uncontrolled, uncertain and timeless nature of the new digital world. This raises concerns about more surveillance, rights violations and privacy.

Surveillance, which is based on two elements, the observer and the monitored, whether it is carried out by the state, an individual or a private organization, carries risks for the parties in every way. Surveillance arising from risks can benefit one party while threatening the interests of the other. For instance, Internet regulations made by the state as a modern period surveillance practice, while being a tool for the manageability of risks for states, may create new risk elements for individuals. In other words; the use of technology in risk management, especially in social areas, creates new risks (such as the risk of privacy violations created by recording e-mails). At this point, while the "risk asset" is common for both parties, the risks differ in the name of the parties and the risk cycle constantly renews itself. In the table below, as the starting point of this study, the risk factors for the surveillance parties are endeavoured to be revealed in the context of internet regulations.

Table.1 Elements of Risk For The Actors of Surveillance

Users – Data Objects (Society) ↓	← Risk →	Providers (State) ↓
Monitored Surveillance ↓		Observer - Surveillance ↓
Confidentiality/Privacy of Private Life Freedom of Expression-Share-Access		Actions Against the State
		Opposition
Security/Personal Data		Security/Terrorism/State Privacy

As can be seen, the risk factors for both surveillance actors vary. While the existence of surveillance systems creates different risk factors for individuals as data objects, the "unlimited" use of new technologies that augment surveillance systems also poses a risk for data collecting states. For example, digital risks for users may be violations of privacy or restrictions on freedom of expression, while risks for the state may appear as actions against the state, threats to state privacy or security concerns stemming from terrorism. Security is a common risk theme for both groups. The concept of "Security" is a risk factor for both groups, but its contents may differ. For states, especially terrorist threats and oppositional stances can be evaluated in this category. As a matter of fact, Bauman (2014:95) who states that the image of the "people" is seen by the states as an "agent" that is both oppressive and a problem of social policies, and this social actor, problematized as a rebellious power and the seed of uprising, or the defence of the social order and its stability, also states that it is seen as the object of various actions for whatever the point of view, the existence of risks in this chaotic cycle is common for the governed and the managers. In this whole cycle, the motivation of the parties to cope with the increasing risk tendency and applications that process personal data, which we can consider as modern era digital risks, emerge (Lyon, 2004:137). The regulations, which, in their updated form, create an important area of discussion and have been referred to as "transaction oversight", should be evaluated within the framework of risk factors and ethical discussions.

Internet Regulations and Ethical Discussions

The internet, which is the basic form of establishing a relationship with the rest of the world for its users (Dreyfus, 2016:7), is considered as a new social/public space with its technical possibilities and the number of users increasing day by day (Poster, 1997, Rheingold, 1994). This virtual public space, which is the most important creation of the new digital era, is also a space where individuals can share all kinds of thoughts and opinions, and it carries certain risks. These risks can be user-oriented violations of rights, as well as criminal acts stemming from the technology of the internet. For example, the concepts of "computer criminality[4]" and "internet criminality" are important in terms of the last sentence mentioned. While computer criminality is a technical term that covers all crimes related to computer data, internet criminality encompasses more individual and user-centred crimes. Hacking is a computer crime, and a virtual threat is an internet crime (Sieber, 2013). Due to these features of the internet, a system has emerged that minimizes the line between public and private space. This system also includes many positive/negative elements in physical life. In this context, this new field, which is very difficult to follow and control due to its technological features, and where uncertainties arising from time-space and user anonymity are quite high, causes radical changes in all areas from trade to education, from health to legal system, and affects forms of government and state-citizen relationships (İcel, 2018:492).

For these reasons, the internet is a medium controlled by legal regulations regulated by all countries of the world. Legal regulations[5], as a source of power use by states, are gradually expanding their dominance in modern societies where bureaucratic powers are dominant. The state is one of the many areas where surveillance data flows and is very active in monitoring daily life (Lyon, 2006:68). The reason is that states need surveillance strategies for national security and public peace. As an example of the hierarchical dimension of government control over the internet, surveillance includes the practice of observing our daily activities and recording these activities through advanced technologies. States legitimize these practices with legal processes regulating the field. Therefore, a network society has been created in which new techniques spread to surveillance strategies such as the use of society and individuals, and this network society links audit and control to the existence of risks.

The example of Internet regulations in our country is the Internet Law, which came into force in 2007. The law was enacted in order to regulate the content and publications on the internet and to prevent possible risk factors, and it has been subject to updates in parallel with the changing social and technological conditions in the process. The most controversial of these updates came into force in 2014. What makes the regulations controversial is the increasing powers of the administrative authorities and the reason that they interfere with the privacy of private life.

When we look at the areas of internet regulations, in general, for reasons such as pornography, piracy, terrorism,; it can be said that it includes certain decisions and sanctions aimed at preventing formations such as cyber war, mass protests carried

[4] The concept was used by Sieber. For a detailed reading, "Internet Law" p. 145

[5] Jessop cites the state's sources of use of force as violence, law, money and knowledge. For detailed information, see; Jessop, B. (2016). The State (Trans. A. Güney). Ankara: Epos Publications

out over the internet, civil unrest, virtual fraud and Internet espionage (Okeke, 2012). Although state regulation and control of the internet as an area of freedom of expression and sharing is seen as an anti-democratic practice, it is known that this mechanism works in many countries that have adopted democracy. Regulations differ from country to country, and these differences are shaped in the context of each country's political, economic and cultural characteristics. It can be said that the purpose of the applications for internet regulations has become universal within the framework of the current order protection discourse. In this regard, Mattelart (2012) talks about the "regulation" of each type of society and the mechanisms that naturalize this regulation, in his observations within the framework of surveillance. These are discourses, institutions, architectures, techniques, regulatory decisions and administrative measures as well as philosophical and moral arguments (2012:17). In this context, it can be repeated that internet regulations and filtering applications do exist without making a distinction between developed and underdeveloped countries.

Zitrain and Palfrey (2008), in their large-scale study, which deals with internet regulations from an academic, systematic and global perspective, made an observation that interventions towards the internet would increase. Undoubtedly, this foresight is a valid one considering the risks diversified by the developing technological systems. Because, while the internet was not subject to any control in the first years of its existence, it has turned into a structure where certain control policies have been developed and implemented as a result of its increasing relationship with all social, political and political fields. Another factor here is the increase in the number of users with the increasing level of digital literacy and the potential to shift towards an interactive space.

This study, in which internet regulations are evaluated as a surveillance practice, while trying to explain surveillance and the risk patterns with which its actors are in relation, touches on ethical debates from the parties, especially against the users. While these discussions are shaped within the framework of confidentiality and privacy, the discussions come to the fore in the dimension of violations. When the ethical problems of digital life surveillance are handled on the basis of states and individuals, it is mostly realised in terms of the second element. In order to keep all structures that pose a threat to their stability and legitimacy under control and to know the next move, the states that watch are performing surveillance by recording all digital transactions of their citizens and using them when necessary. However, this also creates some uneasiness at the point of exceeding personal space. The concept of privacy as a state of secrecy includes the idea that with the rise of capitalism and the separation of the private-public sphere, the autonomy and anonymity of the individual should be limited to the private sphere (Fuchs et al. 2013). However, it is very difficult to make this distinction, especially with the existence of social media platforms as a new public sphere. As a matter of fact, Lyon states that with the 20th century, this distinction became completely unclear (Lyon, 2013). The house, which is the shelter of the public, has entered the field of control over time, and existence of privacy and confidentiality has decreased (Dinev et al., 2008:218). Therefore, it becomes difficult to stay hidden in a world where the walls of the house become transparent. Within the framework of the concept of omnipticon, it turns out that it is not possible to remain secret and private in a world where everyone is watching everyone at any time and everywhere (Okmeydan, 2017: 61).

Bauman (2013:30), too, states that it is impossible to remain anonymous in this medium with the remarks “Everything that is private is now potentially done in the public domain and is open for public consumption; as it is impossible to make anyone forget anything recorded on any of the numerous servers, it will remain accessible forever”.

Mendel et al. (2012) explained the challenges related to protecting privacy in internet environments as follows: The internet makes it possible to collect personal data because computers and smart device technologies and tracking capacities have been perfected, which has created new privacy problems. Technological advances also enable systems that connect information databases that enable larger amounts of data to be processed, enabling the ability to easily store, combine and analyse large amounts of information. This creates new monitoring areas for governments and private companies. On the other hand, as the internet creates new opportunities for the commercial use of personal information, commercial enterprises can easily access user information thanks to these high technologies, and ensure the collection and marketing of information. Especially the spread of e-shopping strengthens this phenomenon. Finally, given the global dimensions of the Internet, new challenges arise in content regulation. Despite the establishment of good national and international standards on data protection, uncertainties regarding confidentiality continue (Mendel et al., 2012: 7-8).

As reinforced by this information, in one way, the Internet is a threat to privacy. Users should guide their usage practices by considering this unfavourable condition. For this, the concept of digital literacy comes to the fore. The lack of secrecy, which undermines the promise of the digital world to offer endless sharing and freedom of expression, makes surveillance convenient not only for states but also for commercial organizations.

In this context, the complex and uncertain nature of the network world distributes risks according to power ownership. States or governments develop counter-defences to the extent that they see security, citizens and their own integrity at risk. At this point, surveillance, which is necessary for the survival of the state, is controversial since it is applied to all individuals and not only to suspects or criminals. In the context of emerging ethical debates, rights violations can be grouped under several headings on the axis of discussion. The first of these is how states will determine the quantitative and qualitative contents of the data they take into custody. On the other hand, the uncertainty of the purposes for which the data obtained through surveillance will be used is another problematic area. In addition to these, it is expected that the balance of “freedom-security”, which is stated as an area to be protected in surveillance activities, will intensify in favour of “security” in terms of states and individuals. Because every event that threatens the security of the state will also threaten the security of the individual and freedoms may remain in the background for the sake of security.

On this subject, Marx (1998), in his study where he makes an ethical analysis for those who perform surveillance and data collection, states that the ethical element of a surveillance activity should be evaluated according to data collection tools, context-conditions and usage goals (Marx, 1998:2). Accordingly, Marx identified three main themes as data collection, context and uses in determining the ethics of surveillance.

In each of these themes, some sub-questions were developed. With these questions, surveillance ethics was tried to be revealed with different contents. In general, Marx endeavoured to set forth;

- Whether the means of surveillance (technical) will cause psychological and physical harm, whether they exceed personal areas,
- Regarding the collection of data; individual awareness and consent, whether data collectors would also agree to be an object of surveillance themselves,
- As a result of surveillance practices and use; whether those who perform the surveillance abide by the ethical elements with questions such as whether the surveillance object will serve the purposes or the personal goals of the data collector, whether the surveillance costs and risks are calculated, the nature of the relationship between the collected information and the target, and whether the secondary gains from the collected information are shared with third parties.

In this context, digital surveillance, by using new technologies flawlessly, affects individuals and states that are parties to the risks and threats created by these technologies. In the balance between the watcher and the watched, the power is concentrated on the watcher and this creates new risks in the context of the watched. In this cycle, the necessity of surveillance should be removed from the discussion, surveillance tools, surveillance context and "minimum harm" understanding should be developed in terms of those being watched.

Conclusion

The Internet is a medium that provides free access to information and the free circulation of information, and carries the freedom of expression and sharing to higher levels by offering endless sharing opportunities to its users. However, on the other hand, it is known that abuse of these unlimited freedoms provides an environment for illegal and unethical actions. In this context, the internet carries the potential of "using" and "restricting" freedoms together (Benedek and Kettemann, 2013:7).

It is a frequently debated issue how to regulate the structure of the Internet, which is suitable for undesirable actions and consequences, while protecting the personal rights of the users. Internet regulations, one of these discussion areas, can be considered as a tool to increase the effectiveness of surveillance systems. This requires more data and this means the continuity of relationships between users and users. This structure, which connects these two actors like no other democratic system, is also criticized for threatening democratic elements. Because of all these features, it can be said that the internet and connected technologies have an ambivalent structure.

It is one of the acknowledgments of this study that internet regulations are a "new era digital surveillance strategy". On the other hand, the study endeavours to exhibit that the controls on the internet are in a cycle with the increasing and transforming risk phenomenon. Digital surveillance, which takes its place from a disciplinary surveillance approach and leaves it to the logic of continuous control and supervision, defines a surveillance process that has been transformed in history. At this point, it is important that digital surveillance, as an important issue of monitored societies, includes which risk factors for users/watchers and users/followers, and which risk factors occur because of it. The answers to these questions take us to the relationship between surveillance and risk and the risk areas of surveillance actors. At this point, risk formation is common for individuals and states that are parties to internet regulations; the types of risks differ.

First of all, the internet, which carries all the risks of the physical world to the digital environment and updates the view of crime and criminality in this context, is a field that needs to be regulated and controlled. Because for a functional control, states need to know more. In digital societies, this information is obtained from online platforms. The aim of this surveillance should be to reduce the risks arising from the uncertain and unpredictable structure of the internet for the individual and society. However, there are ethical debates that have arisen and cannot be agreed upon. It is seen that these discussions are within the framework of rights violations against users. The fact that states control the risks originating from the internet by keeping them at a certain level creates new risks. At this point, the risk, control and surveillance relationship exhibits an intertwined structure.

References

Basturk, E. (2016). The Genealogy of Surveillance, A Postmodern Archaeology from Foucoult to Deleuze. Istanbul: Kalkedon Publications.

Bauman, Z., Lyon, D. (2013). Fluid Surveillance. Istanbul: Details Publications.

Beck, U. (2011). Risk Society Towards Another Modernity. Istanbul: Ithaki Publications.

Benedek, W., Ketteman, M. (2013). Freedom of Expression and the Internet, Joint Project of the European Union Council of Europe. Ankara: Matbam Agency.

Chul- Han, B. (2018). Transparency Society. (Trans. H. Barışcan), Istanbul: Metis Publications.

Cakir, M. (2015). Demonstration and Surveillance on the Internet, A Critical Reading. Ankara: Utopia Publications.

Dinev, T., Hart, P., Mullen, MR (2008). "Internet Privacy Concerns and Beliefs About Government Surveillance – An Empirical Investigation ". Journal of Strategic Information Systems, 17(3), 214-233.

Dreyfus, H. (2009). On the Internet. Istanbul: Küre Publications.

Dolgun, U. (2008). Transparent Prison or Surveillance Society, Surveillance in a Globalizing World, Social Control and Power Relations. Istanbul: Otuken Publications.

Foucault, M. (1979). Discipline and Punish: The Birth of Prison. New York: Vintage Books.

Foucault, M. (2015). Büyük Kapatılma. İstanbul: Ayrıntı Yayınları.

Fuchs,. C. (2015). " Social Media and Surveillance "., S. Coleman, D. Freelon (Eds.), Handbook of Digital Politics. Cheltenham: Edward Elgar, 395-414.

Fuchs, C., Sandoval. M. (2013). Introduction " chapter to the book Critique, Social Media&The information Society (ed) Christian Fuchs and Marisol Sandoval, Routledge http://fuchs.uti.at/wpcontent/1_Introduction_draft.pdf, Accessed 02.05.2018.

Giddens, A. (2018). Consequences of Modernity (8th Edition). Istanbul: Details Publications.

Haggerty, K., Tetrault, J. (2017). " Surveillance "., B. Turner. (Ed.). Wiley Blackwell Encyclopedia of Social Theory, Canada: John Wily and Sons Ltd.

Haggerty, K., Wilson, D., Smith, G. (2011). " Theorizing Surveillance in Crime Control". Theorotical Criminology, 15(3), 231-237.

İçel, K. (2018). Mass Media Law. Istanbul: Beta Publications.

Jessop, B. (2016). The State (Trans. A. Güney). Ankara: Epos Publications.

Lyon, D. (1997). The Electronic Eye: The Rise of Surveillance Societies. Istanbul: Sarmal Publishing House.

Lyon, D. (2013). Surveillance Studies. Istanbul: Kalkedon Publications.

Lyon, D. (2006). Controlling Daily Life: The Surveillance Society. (Trans. G. Soykan), Kalkedon Publications.

Marx, G. (1998). " Ethics for New Surveillance ". The Information Society, 14(3), 171-185.

Marx, G. (2002). " What's New About the "New Surveillance "? Classifying for Change and Continuity ". Surveillance & Society, 1(1), 9-29.

Marx, G. (2015). " Surveillance Studies ". International Encyclopaedia Of The Social & Behavioural Sciences, 23, 733–741.

Mattelart, A. (2012). The Origin of the Globalization of Surveillance Securitization Order. Istanbul: Kalkedon Publications.

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., Tores, N. (2012). Global Survey on Internet Privacy and Freedom of Expression. France: Unesco Series on Internet Freedom.

Okeke, I. (2012). Regulation and Censorship of The Internet, Bachelor's Thesis Guidelines DP in Business Information Technology. Helsinki: HAAGA-HELIA University.

Okmeydan -Bitirim, S. (2017). The Transformation of the Surveillance Society in Postmodern Culture¨: From the ' Panopticon to the 'Synopticon' and the 'Omnipticon'. AJI T-e: Online Academic Journal of Information Technology. Special Issue –Volume/ Vol: 8-Issue/ Num: 30.

Rheingold, H. (1994). The Virtual Community: Finding Connection in a Computerized World, London: Secker&Warburg.

Sieber, U. (2013). “Computer Guilt”, Y. Ünver (Editor). Internet Law. Ankara: Seçkin Publishing.

Slobogin, C. (2007), Privacy at Risk, The New Government Surveillance and the Fourth Amendment, The University of Chicago Press, Chicago an London.

Slobogin, C. (2005), Transaction Surveillance by The Government, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=670927, Accessed 11.02.2021.

Turner, J. (1996). Panopticism and Populer Culture: A Genealogy of New Surveillance Technology, Discourse and Ideology. The Faculty of the Collage of Communication of Ohio University, Ohio.

Zittrain, J., Palfrey, J. (2008). “ Introduction ”., In R. Diebert, J. Palfrey, R. Rohozinski, J. Zittrain, (Eds.). Access Denied The Practice and Policy of Global Internet Filtering. England: The MIT Press.

Destekleyen Kurum/Kuruluşlar: Herhangi bir kurum/kuruluştan destek alınmamıştır.

Çıkar Çatışması: Herhangi bir çıkar çatışması bulunmamaktadır.