



JATSS, 2026; 8(1), 169-188

First Submission:04.01.2026

Revised Submission After Review:16.03.2026

Accepted For Publication:24.03.2026

Available Online Since:25.03.2026

Research Article

**The Limits of the Digital State and Individual Privacy: A Public Sphere
Perspective**

Ejder Çetin ^a & Mustafa Demirkol ^b

Abstract

Introduction: Mutual trust lies at the heart of the social contract; yet, in the neoliberal era, this bond is being tested by the expanding limits of the digital state. This study problematizes the transformation of privacy not merely as a technical security breach, but as a deeper erosion of democratic legitimacy. It seeks to understand whether the digital sphere is evolving into a liberating 'agora' or a surveillance mechanism that threatens the individual's status as a political subject.

Method: Adopting a qualitative lens, the research weaves together a descriptive analysis with a theoretical critique grounded in political philosophy. The tension between the promise of digital freedom and the reality of surveillance society is interpreted through the comparative perspectives of Hannah Arendt's public/private distinction and Jürgen Habermas's communicative rationality.

Results or Findings: The analysis reveals a stark paradox: The digital sphere has morphed into a "transparency regime" reminiscent of a panopticon rather than a democratic public sphere. It is observed that the state is shifting from a service provider to a proactive structure of predictive policing, where privacy is commodified and ethical boundaries are redrawn by algorithms.

Discussion or Conclusion: The study concludes that privacy is not a luxury to be granted by the state, but a constitutive "constitutional threshold" that defines human dignity. To sustain legitimacy, policy must shift from data-hoarding to a privacy by design approach. Reclaiming the digital sphere as a space of freedom requires strictly limiting state authority through ethical and legal barricades.

Keywords: public sphere, private space, digital space, privacy, surveillance society

JEL Codes: H83, K24, H11, O33, O38

^a Independent Researcher Dr., Social Security Institution of the Republic of Türkiye İzmir Provincial Directorate, İzmir/Türkiye, ejdercet@gmail.com, <https://orcid.org/0000-0002-7185-4885>

^b Res. Asst. Dr., Tekirdağ Namık Kemal University, Faculty of Economics and Administrative Sciences, Department of Political Science and Public Administration, Tekirdağ/Türkiye, mustafademirkol@nku.edu.tr, ORCID ID: <https://orcid.org/0000-0002-9860-8836> (Corresponding Author)



JATSS, 2026; 8(1), 169-188

İlk Başvuru: 04.01.2026

Düzeltilmiş Makalenin Alınışı: 16.03.2026

Yayın İçin Kabul Tarihi: 24.03.2026

Online Yayın Tarihi: 25.03.2026

Araştırma Makalesi

Dijital Devletin Sınırları ve Bireysel Mahremiyet: Bir Kamusal Alan Perspektifi

Ejder Çetin ^a & Mustafa Demirkol ^b

Öz

Giriş: Karşılıklı güven toplumsal sözleşmenin özüdür; ancak neoliberal çağda genişleyen dijital devlet pratikleri bu hayati bağı tehdit etmektedir. Bu çalışma, mahremiyeti salt teknik bir güvenlik sorunu olarak değil, demokratik meşruiyetin bir krizi olarak sorunsallaştırmakta; dijital alanın özgürleştirici bir agora mı yoksa bireyi nesneleştiren bir "gözetim mekanizması" mı olduğunu sorgulamaktadır.

Yöntem: Nitel bir yaklaşım benimseyen araştırma, betimsel analizi siyaset felsefesi temelli teorik bir eleştiriyle harmanlamaktadır. Dijital özgürlük vaadi ile "gözetim toplumu" gerçekliği arasındaki gerilim, Hannah Arendt'in özel/kamusal alan ayrımı ve Jürgen Habermas'ın iletişimsel eylem kuramı üzerinden karşılaştırmalı olarak okunmuştur.

Sonuçlar ya da Bulgular: Analiz, dijital alanın demokratik bir tartışma zemininden ziyade, panoptikonu andıran bir "şeffaflık rejimine" dönüştüğünü ortaya koymaktadır. Devletin pasif bir hizmet sağlayıcıdan, yapay zeka destekli "öngörücü polislik" yapısına evrildiği; bu süreçte mahremiyetin metalaştığı ve etik sınırların algoritmalarca ihlal edildiği görülmektedir.

Tartışma ya da Yapılan Çıkarımlar: Çalışma, mahremiyetin devlet tarafından bahsedilen bir lüks değil, insan onurunu ve siyasal özne olma hakkını koruyan kurucu bir "anayasal eşik" olduğu sonucuna varmaktadır. Dijital meşruiyeti sürdürmek için veri istifçiliğinden vazgeçilmeli; "tasarımla mahremiyet" ilkesi ve bağımsız etik denetimlerle dijital alan yeniden bir özgürlük sahasına dönüştürülmelidir.

Anahtar Kelimeler: kamusal alan, özel alan, dijital alan, mahremiyet, gözetim toplumu

JEL Kodlar: H83, K24, H11, O33, O38

^a Dr., Bağımsız Araştırmacı, T.C. Sosyal Güvenlik Kurumu İzmir İl Müdürlüğü, İzmir/Türkiye, ejdercet@gmail.com, ORCID ID: 0000-0002-7185-4885

^b Arş. Gör. Dr., Tekirdağ Namık Kemal Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, Tekirdağ/Türkiye, mustafademirkol@nku.edu.tr, ORCID ID: <https://orcid.org/0000-0002-9860-8836> (Sorumlu Yazar)

Introduction

While seeking the conditions of the ideal “discursive public sphere” attained in the 18th century, Habermas critiqued mass society through the narrative of the bourgeois public sphere which began to deteriorate in the 19th century, yet he simultaneously established the principles for the possibility of a political public sphere in modern democracies. Arendt, on the other hand, offering a more pessimistic critique than Habermas with her analysis of the “Modern Age” dating back to the 17th century, presented a total critique of modernization by idealizing the specific forms of political organization in ancient Greek and Roman societies, where participatory democracy was experienced in the “real” sense.

A fresh look at old ideas about public debate emerges when we consider how online spaces now shape conversation - algorithms quietly shift who gets heard, how voices connect, what counts as reason (Margetts & Dorobantu, 2019). In this respect, the digital public sphere no longer merely extends earlier communicative arenas but restructures them through data-driven governance and platform power.

The research question of our study is as follows: “How do individual privacy spaces change due to digital state practices in the context of surveillance in the new public sphere and what can be said about this change in terms of the classical public sphere theory?” The use of artificial intelligence, data analysis and decision making algorithms in the digital state, which has become a global phenomenon, increasingly erases the borders between the state and the citizen and ambiguity in governance, security and individual freedoms arise (Lee et al., 2024). In our study, which is a qualitative study, descriptive analysis and literature review methods are used. In this context, within the scope of the “new surveillance” concept specific to the digital age, we comparatively and interpretively examine the works of Hannah Arendt and Jürgen Habermas, who are the leading names of the differences between the public and private spaces. Our study, which is an interdisciplinary theoretical study, aims to introduce a new approach to the privacy debate, which is reduced to a technical and legal level and limited to data security in developing countries such as Turkey. By incorporating key concepts in political philosophy, such as the agora, the panopticon, and rational communication, the study aims to reconceptualize privacy as an integral part of the crisis of trust that characterizes the digital state-individual relationship. See also Véliz (2021) and Margetts & Dorobantu (2019). In this respect, the argument of this study echoes recent normative discussions of privacy that depart from the traditional understanding of privacy as a right of the individual and opt for the understanding that privacy can also be a social good with democratic relevance. The latter perspective posits that in digital governance environments, privacy can serve to sustain the basic principle of trust among citizens, governments, technology providers, and third parties, which is indispensable for efficient and accountable governance in the digital age.

This study aims to conceptualize privacy as a foundational boundary of democratic legitimacy in the digital age by reinterpreting a debate primarily addressed at the legal and technical levels in the literature on digital government and privacy, within the framework of Arendt and Habermas' theories of the public sphere. This article makes three contributions to the on-going discussion in the literature on digital state practices and privacy. Firstly, it leaves the rather formal and technological focus on the discussion about digital state practices and privacy behind by considering privacy as a political and normative issue in the context of the theory of the public sphere. Secondly, it examines in the light of the theories of Hannah Arendt and Jürgen Habermas on the relation between the state and the public sphere, to what extent the digital sphere can be regarded as a space of civil society for democratic communication between citizens, in a world of digital surveillance technologies. Thirdly, it criticizes the prevailing

individual rights-based understanding of privacy in the literature and introduces a constitutional alternative based on a normative concept of privacy as a constitutional threshold limiting the democratic potential of the digital state. Methodologically, this article employs qualitative and theoretical analysis, drawing on conceptual analysis, in order to evaluate the theoretical framework of the public sphere in the context of digital state practices.

From “discriminatory designs” to the digital state of exception The digital state is no longer just a technological tool for public administration, but a new political and power relationship between the state and the citizen. Through the use of “discriminatory designs” disguised as “input neutral” and “technological” - which Benjamin (2019) describes as the digital architecture that, according to the norms of the public space defined by Arendt and Habermas, undermines it and turns the citizens into transparent beings and keeps the state obscure in the algorithms of the decisions. This study investigates the preservation of the boundaries of the public space in a data-driven model of governance, while linking the theories of the public space with the digital practices that are currently exercised and analysing the consequences of achieving algorithmic efficiency at the cost of the political effectiveness of citizenship according to Hannah Arendt.

Methodology and Analytical Framework

In this study, preferred research design for this study would thus be conceptual and normative rather than empirical or field-based. The focus here is less on frequency counts of digital surveillance and more so on the qualitative understanding about how fundamentally, through these practices of a digital state, that's being dramatically rearranged. By emphasizing the normative implications of these community-building practices, I explain how the 'digital limit' of both political and non-political communities substantively alters the conditions for (and limits to) democratic legitimacy.

I have created a dual-lens analytical framework grounded in the political philosophy of Hannah Arendt and Jürgen Habermas to meet this need for adequate scientific theory. Further, in this model, Arendt's public/private dichotomy is not the mere historical concept it has frequently been represented as; rather, it serves a diagnostic purpose to assess if any state intervention online would be an internal structural ‘invasion’ of the protected private domain (see Arendt, 2023). It also helps us see whether the individual is being shrunk from a political subject to a data object.

Conversely, Habermas's theory of communicative rationality serves as a normative standard against which this analysis can be measured. I then use this lens to evaluate if the digital public sphere engages anymore in a broad rational-critical debate or has devolved into an algorithmically mediated echo chamber. This top-down and bottom-up blend allows the study to go deeper than a descriptive narrative. It establishes a theoretical lens through which contemporary governance forms, like predictive policing and infrastructuralisation of large-scale data can be critically examined.

The findings of this research relate to the ideal understanding of the political, and not to the statistical level of the political. The unit of analysis of this research is the structural change in political subjectivity resulting from the exercise of algorithmic governance. By analyzing through the specific research prism the legal framework and the digital infrastructure of algorithmic governance, this research aspires to achieve an original contribution to the philosophical debates on digital governance. In this sense, the result of this philosophical research is not the expression of dogmatic theses, but the outcome of a meticulous philosophical inquiry.

Discussions on the Public Sphere

The historically qualified concept of the public sphere has continuously differentiated and transformed up to the present day. In Ancient Greece, politics was conducted in the common area, the public sphere, and the “polis” was this very public sphere where relationships were based on the interactions of equal citizens. These relationships emerged on the basis of freedom and equality, for the citizen (polites) was a member of the public sphere. In this period, public life was lived in agoras, which consisted of the assembly, the court (lexis), and common actions (praxis). The two activities constituting political life were “speech” and “action.” The life of the citizen in the public sphere was the “good life”, and to ensure this good life, the necessities of life had to be met in the private sphere; thus the private sphere was a precondition for ensuring the freedom of citizens in public life.

Aristotle approached the public sphere in the context of citizens engaging in politics collectively and its relationship with the private sphere. 17th and 18th-century philosophers like Locke, Hobbes, and Rousseau discussed the public sphere in the context of civil society, yet after these periods the distinction between public and social concepts became blurred and civil society was identified with political power. Kant defined the public sphere as the area formed by public opinion, while in the subsequent period civil society underwent a change to include family and economy. Marx used civil society in this sense and addressed its dialectical relationship with the state, whereas in the 20th century Gramsci examined the cultural and ideological aspects of civil society contributing to the current usage of this concept.

Arendt questions human life by sharply drawing the boundaries of the public and private spheres; the public sphere is the realm of political activities while the private sphere is that of non-political activities. Arendt attempts to remind humans of the experience related to the life of the “polis”, suggesting that the public sphere can be seen as the place where differences emerge, meaning the subjects constituting the public sphere exist with their differences. According to Arendt’s model wherever citizens have the opportunity to speak and act they possess the possibility to create a public sphere, a possibility that exists where individuals are in harmony and where there is equality and participation. In spaces devoid of harmony, trust, and participation, we cannot speak of a public sphere. For Arendt, the public sphere—understood as the space of discussion, speech, and action—constitutes the realm of politics, since it is through speech that individuals become political actors (2023). In Arendt’s public sphere model humans exist through their actions, and the understanding of doing politics based on differences—that is, justifications based on race, ethnic structure, or religion—is not valid here. The individual exists here on their own behalf and gains their identity in this sphere. In the public sphere the citizen freely defends their thoughts depending on their power of representation. In this sphere where equality prevails people come face to face having the opportunity to convey their thoughts to one another and to evaluate a problem from different angles.

The private sphere, on the other hand, possesses the quality of secrecy/privacy. The way to escape and hide from the transparency and openness of publicity is to own private property. Secrecy/privacy expresses the distinction between the private sphere and the public sphere, or in other words, the distinction between what is to be hidden and what is to be shown publicly. The condition of slaves and women determined the existence of secrecy/privacy in the private sphere. Arendt (2023) notes that individuals such as laborers, who were bound by biological necessities, and women, who ensured the physical survival of the species, were historically relegated to the hidden realms of the private sphere.

The situation that most clearly expresses the distinction between the private and public spheres is the existence of things that need to be hidden versus things that need to be displayed openly. The private sphere is closed to human knowledge and in one aspect keeps the hidden secret, harboring the realm of birth and death. This is primarily because the fundamental transitions of human existence, specifically the origins and ends of life, remain beyond the scope of certain knowledge (Arendt, 2023).

While grounding her model, Arendt emphasizes that “labor” and “work” activities, which she approaches dialectically, belong to the private sphere. Every human activity expresses the place it is located; labor and work belong to the private sphere while action belongs to the public sphere. Labor expresses activities aimed at meeting biological needs to sustain one's life, and according to this model labor is a concept distant from the public sphere and can be evaluated as a concept of the private sphere. Work expresses the world of needed objects. These two concepts belonged to the world of women, slaves, and merchants who continued their lives and occupations within the boundaries of the private sphere in the Ancient Greek period. In the private sphere secrecy and privacy were in question, and the citizen who was the head of the household applied force and violence in this sphere depending on secrecy.

We see that Arendt places the “polis,” which existed in Ancient Greece and expressed the public sphere in another way, at the foundation of the public sphere model she developed. For Arendt the “polis” is a historical fact, and while re-evaluating the “polis” that emerged in a specific period in Ancient Greece she was aware that it could not be repeated in today's world. The importance of the “polis” for Arendt lies in it being an organization that allows everything seen as a problem to be discussed by citizens and highlights solidarity rather than violence. For this reason, she places the “polis” at the center of her theory. According to Arendt (2023), the essence of the polis resides not in its physical or geographical boundaries, but in the collective existence and interaction of its citizens.

Speech in the political sphere is a speech with a special quality, not just any speech. Speech in this sphere is conscious speech based on knowledge regarding society. In Ancient Greece, the political sphere was the place where citizens' common words and deeds were shared. The polis is conceptualized by Arendt (2023) as a dynamic organizational structure that emerges whenever individuals engage in collective action and shared discourse. Action, speech, and freedom are the powers that complete the public sphere; if one of these is missing one cannot speak of a public sphere. Man can achieve immortality through his life in the public sphere. For Arendt, freedom is the most valuable quality of human life, and the public sphere must be recreated for freedom to be lived and human equality to be achieved. Participatory democracy and the concept of the active citizen are at the center of the understanding developed by Arendt.

Whether one is talking about the disappearance of public space or merely the loss of his own right to the future tense, in essence, this is how power operates today. Yes, as Zuboff (2019) says, the massive collection of human behavior data provides a new type of power that works underground, avoiding human awareness and effectively eliminating uncertainty. These methods, when utilized by the digital state, are nothing like Habermas's ideal of a public sphere where rational debate took place. Instead, it is transformed into a 'behaviorist mold' regime. Here things change. The state no longer gathers information about its citizens to manipulate them. It forces them to make decisions by influencing their choices through digital signals. All of this upends Arendt's understanding of politics and freedom as a “public life” understood as “activity and surprise.” A new, technological order establishes a new form of rationality that, as long as it remains imperceptible and concealed behind technology, can avert and eliminate

the dynamics and unpredictability of the public life of citizens, by turning their capacity for action into administrative efficiency. Wanting to remain private is therefore not the central issue at stake in this respect; rather, what is at stake is the defense of our freedom to oppose those anonymous systems that are devouring our democratic reality and thereby reducing politics to a purely ordinary affair.

One of the criticisms of Arendt's theory of the public sphere is that it portrays political activity in an unrealistic light. In her effort to portray political activity as being central to the everyday lives of citizens and to show that political activity is carried out in a space where citizens are seen as equals, she neglects to consider the structural inequalities and exclusions that actually exist in modern public spaces. While her framework remains normatively powerful, it provides limited analytical tools for understanding mediated and asymmetrical forms of publicity.

The public sphere defined by Habermas is the liberal bourgeois public sphere. He questions the rise and fall of this sphere which is specific within its historicity and limited to a certain period. Habermas's idea of the public sphere is an area at the level of legal rights where state intervention and market relations are absent. Habermas paints a picture of publicity separate from the state and society; this public sphere expresses an area separate from the political relations of family, market, and state.

Habermas's concept of the public sphere leads to the questioning of a category belonging to bourgeois society, and in this form, he is in an effort to reconstruct the public sphere as a historical category. The public sphere is an area open to everyone without the limitations of any social environment. According to Habermas, the public sphere is a specific area located within civil society. In this area, the citizen is located in a specific sphere open to freely explaining and publishing their thoughts, using the right to organize, and communicating with each other about problems concerning everyone. In the public sphere, citizens have the opportunity to discuss equally, rationally, and critically. According to Habermas, this form of discussion is the basis of democracy, and through discussion, the neutralization of social power is in question.

Habermas evaluates the category of the bourgeois public sphere as specific to a certain period. The establishment of institutional relations between parliament, press, and political parties is an indicator that the public acquired political functions in the 18th century. However, the nature of the public's political function must be evaluated in connection with the development history of the bourgeois class or society. In other words, the political function of the public can only be understood holistically by examining the historical phase in which commodity exchange and social labor achieved independence from state authority (Habermas, 2021). This structural transformation becomes particularly visible in contemporary digital platforms, where publicity is no longer mediated by deliberation but increasingly shaped by algorithmic visibility.

The public community is divided into a minority producing reason in a non-public form and a mass formed by consumers. In the name of making economic understanding and thought dominant, a literary, political, and consumer public was created, and the publicity of communication tools was destroyed. Habermas (2021) argues that the reality constructed by mass media maintains a public character only in superficial terms. Mass media has emptied the privacy of the private sphere by making it transparent.

According to Habermas, it is possible to read the structures of social integration in public spheres. The political publicity of the institution of democracy has a meaning for the integration of society. Habermas (2019) suggests that in modern societies where citizens lack personal

familiarity, the establishment and continuity of a fragile partnership depend on the collective process of forming public opinion and will. In this sense, the state of a democracy can be understood by listening to the pulse of public opinion politically.

According to Habermas's understanding, the function of the public sphere is communication. Today, the public sphere directed by mass media such as the media and advertising sector will reveal its critical political function based on reason in the direction of rationalizing communication. The aim in rationalization should not only be the rationalization of political power but beyond that, it should respond to the practice of life through scientific and technical developments. The relationship between technique and democracy should be questioned, and the possibilities of using technique should be arranged in a beneficial way for people. Communication in the public sphere is an activity showing that people have become aware of themselves as social subjects. The conditions providing communication and the public sphere are the same; these conditions are truth, reality, honesty, and intelligibility. These conditions are also the conditions of discourse ethics. Discourse ethics aims to solve political and legal problems fairly.

Habermas identifies the “social state” model belonging to capitalism as the structural transformation of publicity. In this model, mass media have developed sovereignty over publicity. Public and private spheres have intertwined. Here, organizations not only maintain their sovereignty in goods and the market; they also possess political functions in social environments. This process leads to the re-feudalization of the public sphere. Today, the boundaries between the public and private spheres have deteriorated in favor of mass culture. Mass media directs what is public. According to Habermas, fundamental rights are the guarantee of political publicity. In the public sphere, communication is important, and Habermas's understanding of communication expresses an interaction where consensus regarding the developed action plans of the participants is achieved. Consensus is achieved through rational discussion. Rational action is revived on the basis of communication in the public sphere.

The public sphere model developed by Habermas is open to criticism in certain aspects today. Although the public sphere seems open to everyone in the thinker's model, in practice it is open only to citizens who are “mature subjects”. The ambiguity of “everyone” carries within itself. Workers, women, and those from different ethnic groups do not take place in the public sphere because they are not mature subjects. In the said model, inequalities are bracketed. In this context, it is necessary to reconsider the concept of the citizen and think about whether a public understanding that includes differences should be developed. In the model developed by Habermas, the public sphere is accepted as an area separate from social environments. Habermas's understanding of the public sphere provides the possibility of a critical questioning of developments in the media and political world today.

The Digital Sphere As A New Public Sphere

In the context of the digital state, the concept of a 'limit' refers not to a geographical line of sovereignty but to a multi-layered threshold with legal, political, and ethical dimensions. The legal limit marks where the state's authority to collect data ends under legitimate laws (such as KVKK, GDPR); the political limit defines where the state's security reflex must be halted to prevent the violation of individual liberties; and the ethical limit represents the inviolable domain where an individual's digital footprint must be deemed 'private life'. In the neoliberal era, the state tends to continuously expand these limits to the detriment of the individual often under the guise of 'security' and 'service efficiency' thus the 'limit' problematized in this study

is not the limit of the state's technological capacity but rather the limit of its democratic legitimacy.

Just as Habermas discussed newspapers as a tool for the formation of the bourgeois public sphere in modern society in the 19th century, it is now in question that the internet, in a world rapidly individualizing under the influence of neo-liberalism, is revitalizing a global public sphere. Habermas's concept of publicity is brought to the agenda again with the spread of the internet, which is the resultant of new information and communication technologies, to society. The digital sphere is seen as the third stage of the public sphere coming after the newspaper and radio-TV. The thought regarding the internet creating a public sphere or spheres stems from the technological potential of the internet. The technological potential of the internet, characterized as the “network of networks” based on connecting computer networks to each other, has led to the revival of the positive relationship established between information and democratization.

The internet is a digital sphere where everyone with access can express themselves freely through different tools (e-mail, chat programs, forums, websites, etc.); it provides communication in every direction from person to person, person to group, group to group, and group to persons allowing for the global and simultaneous sharing of information. The abundance of information, the multiplicity of options, and the possibility of interaction on the internet have reactivated dreams of “participatory democracy”, “direct democracy”, and the “agora”.

The conceptualization of the digital sphere as a new public sphere requires a move beyond the assumption of technological neutrality. What Hildebrandt noted back (2018) still holds true – digital spaces now take shape through systems designed to act ahead of thought. These platforms block out the space where we can weigh competing ideas and perspectives against one another and they thereby undermine the notion that through the process of argumentation, ideas can be proven or strengthened. Through their unexamined design, social media undermines the ideals of deliberative democracy. We do not discuss or deliberate about the architecture of social media sites and therefore the architecture of these sites defines the nature of our deliberative practices. The social media space is not a democratic agora, a civic space, for the purpose of discussion and deliberation about politics. Rather it is a technological design that acts as a filter to our social and political discourse prior to that discourse ever taking place. When the digital state integrates its functions into these infrastructures, the 'limit' of state authority becomes invisible and automated. This transformation suggests that we are moving from a public sphere of discourse to a public sphere of 'management,' where the individual's role is no longer to participate in a rational-critical debate, but to be efficiently processed by algorithmic systems. Therefore, the digital public sphere must be re-evaluated not just as a tool for communication, but as a site of constitutional struggle where individual agency is at risk of being designed out of the system.

However, this dream of an agora was shattered by the realization that the digital sphere is not a neutral field for public deliberation but rather an algorithmically designed echo chamber (Maslej et al., 2025). Large-scale empirical mappings of AI systems demonstrate that engagement-optimizing algorithms systematically privilege affective polarization over rational-critical debate, thereby structurally undermining the Habermasian ideal of communicative rationality (Maslej et al., 2025). The rational-critical discussion ground idealized by Habermas (2021) has been replaced on digital platforms by a design aimed at fueling users' emotional reactions to generate more interaction (and thus, more data). In *The Transparency Society*, Byung-Chul Han contends that the digital age is not suffering from a communication crisis, but

from a crisis of privacy: our information is exposed and we are forced to provide explanations for our actions and personal details (Han, 2017). While the individual believes they are being liberated in the digital sphere, they are in fact imprisoning themselves in a digital panopticon through voluntary disclosure (Han, 2017). In this regard, the digital sphere has transformed into a market of consensual surveillance rather than a public square of freedom.

According to Timisi, authors emphasizing the internet-democracy relationship support their views around five main themes: easy access and sufficiency in information access, the internet's organization immune from authorities, unlimited freedom of expression on the internet and the technical difficulty of content control, increased political participation, and the expansion and globalization of civil society (Timisi, 2003). Revisiting the democratic potential of the internet, Fuchs (2023) suggests that the digital public sphere is currently characterized by a struggle between liberating deliberative spaces and institutionalized surveillance mechanisms. It is argued by liberal theorists that the internet, thought to lead to many positive transformations in society, will democratize society and apply direct democracy because it provides individuals with the information they want by overcoming national borders and time problems in the political sphere with its structure that multiplies information and is based on interaction, facilitates citizens' participation in politics "technically", creates a discussion environment through virtual forums, gives dissident voices and alternative groups in society the opportunity to communicate and express themselves at a much lower cost than dominant communication tools under capital control, and facilitates the organization of civil society.

The internet owes its designation as a free space from its early days to being relatively independent of market and state control compared to other communication environments. Yet this relative freedom has been narrowing for some time due to the coercion of both states and the market. In the first stage, to ensure a safe shopping environment suitable for the needs of the market, the internet environment began to be taken under control for secure money transfer and the prevention of internet piracy.

British sociologist Antony Giddens argues that the relationship between information and society precedes modern internet technologies; instead, he maintains that the origins of the nation-state are fundamentally rooted in information collection, suggesting the modern state has inherently been an information society from its inception (Giddens, 1985). Furthermore, Giddens contends that classical thinkers like Marx, Weber, and Durkheim overlooked the pivotal roles of violence and surveillance in the formation of modern society (Giddens, 1985). A highly organized nation-state must constantly collect information about citizens and share this data with citizens again to maintain its existence, and in this way, society will be able to develop a social self-perception by knowing itself (Webster, 2021). On the other hand, the state itself needs information about citizens incessantly to understand the limits of its sovereignty, collect taxes, and distribute resources, which requires "effective surveillance" (Webster, 2021). The need for surveillance is not only to ensure institutional continuity over a large population; another important feature of these structures is that a significant part of nation-states were established in wartime and developed based on defense needs, meaning war is one of the basic existence dynamics of the nation-state (Webster, 2021). Therefore, surveillance goes beyond an activity needed to complete its functions; nation-states try to collect information about the "enemy" incessantly citing threats that may come from outside.

Today, states' activities of collecting information about citizens are becoming increasingly complex. Collecting information with the justification of a threat is not only an activity directed outwards but also a situation concerning the nation-state's own citizens. It has been observed that activists, union leaders, and media workers can also be included in the scope

of security-justified surveillance (Webster, 2021). While some of this collected information is kept constantly secret, some of it—divorce rates, crime rates, education levels, etc.—is presented to citizens through the media. Thanks to this information citizens have knowledge about their own lifestyles and how to plan their futures, yet this informing allows states to manipulate citizens as much as inform them. Modern capitalist state relations carry such a complex nature that it is not possible for individuals to collect high rates of information without state-supported organizations. Politicians and bureaucrats holding state authority possess so much control over information that all modern nation-states face “danger of totalitarianism” (Webster, 2021).

Nevertheless, this surveillance mechanism established by the state and the market today is no longer limited to merely 'watching what is' (surveillance); the primary goal is predicting what will be (prediction). Recent systematic reviews indicate that predictive policing technologies not only reproduce existing social biases but also expand the discretionary power of the state by translating probabilistic risk assessments into pre-emptive interventions (Lee et al., 2024). In the digital age, the role of the state has evolved from simply keeping data as an archive record to a model of predictive policing that forecasts future risks, crimes, and social mobilities through artificial intelligence and big data analytics (Lee et al., 2024). In this new regime which Shoshana Zuboff defines as “Surveillance Capitalism”, not only the individual's current actions but also their future “behavioral surplus” are processed as raw material and converted into a commercial or political prediction product (Zuboff, 2019). The fact that we are being violated privacy means no longer that the intimate is being revealed but that our preferences are being formed before we are aware of it. Information about our preferences is already at the disposal of algorithms before we decide. This is fundamentally different from the classic concept of surveillance. Tore Velde of the Swedish Defence Research Agency has labeled this phenomenon “anticipatory governance”, i.e. a form of state governance that is aimed at citizens' future actions (Tallberg et al., 2023).

Today, with the significant contribution of internet-based technologies, the number of people who can be kept under surveillance can be quite high. Many internet-based technologies can go beyond entertainment or social relationship purposes and turn into tools for keeping users under surveillance. Some website can detect faces in photos uploaded to the page, compare them with thousands, perhaps hundreds of thousands of photos on the internet, and find other photos where the face in the photo appears. According to Morozov (2011), such technologies have been exploited by oppressive regimes, such as in Iran, to identify and target political activists. Similarly, the Indian government has utilized digital tracking to monitor Facebook users in the Kashmir region, employing automated alerts to summon suspected individuals to police stations (Morozov, 2011). With developing surveillance technologies, totalitarian tendencies are also emerging in democracies. With developing surveillance technologies, totalitarian tendencies are also emerging in democracies. According to Jean Claude Paye, legal regulations in America and England pave the way for e-mails to be inspected without any permission, and “general supervision has replaced punishing certain behaviors” (Paye, 2004, p.153). According to Paye, legal regulations paving the way for internet surveillance allow contents on the internet to be monitored before a criminal act occurs by emphasizing the terror threat and creating a “proactive” surveillance system with police logic (Paye, 2004). Although states' tendency to use the internet as a surveillance tool is a structural situation regarding the emergence of nation-states, the legal ground of this surveillance tendency has increased significantly especially with the terror attacks on New York and Washington on September 11, 2001.

The Privacy Problematic

It is possible to address privacy in different dimensions. Privacy as secrecy is the individual's desire to keep information about themselves and certain actions secret from everyone or some people they choose. Anonymous privacy is the individual's desire to perform certain behaviors (even if done in society) in a way that cannot be associated with the individual, that is, the desire to be anonymous. Autonomy privacy is the individual's preference for some of their behaviors to remain public or secret to depend on themselves (Teh, 2002). Susser further argues that in the digital age, this autonomy is under threat from “algorithmic manipulation,” where invisible data architectures diminish the individual’s capacity for self-governance (Susser et al., 2019).

The right to privacy against the state differs from the right to privacy against other people in two respects. First, although there are situations of violating another's privacy areas without their consent through theft, etc., among people, their relationships with each other are generally voluntary. The individual has control over the personal information they will disclose to another and possesses the power and measures to protect their privacy against other people. However, the state can perform forced interventions against individual privacy in a very wide area. The second difference is that the state has sovereignty based on applying physical force over citizens. It is possible for individuals to take some measures to protect their own privacy against third parties (they can protect themselves against other citizens, take measures like locks and burglar alarms); however, they are very powerless when it comes to protecting themselves and their personal information against the state. The only way they can resort to protect their personal information from the state is to try to hide it (Flaherty, 2000). As Tanczer (2020) observes, cybersecurity in the digital state must be redefined as a foundational pillar of the social contract; without it, the state’s intervention in personal domains loses its democratic legitimacy. The effects of this difference on privacy exhibit changes according to the point of view. If the state is thought to be well-intentioned, wanting the good of its citizens, and observing the public interest, then personal privacy will make it difficult for public officials to do what is good. However, on the other hand, if it is thought that the state can behave against citizens, in that case, personal privacy against the state and its protection is definitely a good thing. Although it is accepted that privacy can be used in hiding personal crimes, the view that it should be protected against the state is quite widely accepted.

Uslaner (2004b), in a study where he also addressed the relationship between trust in the internet and privacy anxiety, argued that individuals who are generally prone to trust have low levels of concern regarding privacy in transactions they carry out over the internet, whereas those with low propensity to trust have higher concerns regarding privacy and security. While trust tendency is effective on privacy perception, privacy perception is also an effective concept on trust towards e-government applications, for problems and concerns regarding privacy are among the critical obstacles to the implementation of e-government (Cullen & Reilly, 2007). While trust is vital, Lember ve Crompvoets (2023) notes that the 'black-box' nature of modern public service algorithms creates a legitimacy crisis that technical security alone cannot solve, as citizens feel alienated from the decision-making processes. Ensuring information security at the highest possible degree is of vital importance for information and communication technologies. Information security relates to the ability of personally identifiable information to be transmitted and disclosed over the internet and insecure networks and is the key to privacy, which is one of the most important elements of the trust environment that has become indispensable for the information society. The requirements of e-government systems to be established to ensure information security and reduce privacy anxiety as much as possible should be determined while the system is still being designed (Kalloniatis et al., 2004). In this

respect, e-government applications should not only offer better service opportunities for public institutions but also provide citizens with the guarantee of holding data ownership. Citizens do not want their personal information shared with third parties. The amount of information in the hands of the state and the sensitivity of this information is an important issue in terms of security, and the theft of citizens' data by hackers or access to such information by third parties must be prevented.

This security threat is not just a technical cybersecurity issue, but also has to do with the legal limbo that stems from combining “hybrid” relations between the state and tech behemoths. With states sharing data more and more with the tech giants in order to perform public services (smart cities, digital health etc.), it blurs the line of who actually owns and has sovereignty over public data. In Turkey, for example, the Law on the Protection of Personal Data (No. 6698, 2016), commonly known as KVKK, and GDPR in Europe became “digital shields” to protect ethical cookery as individual against this data tsunami (Tanışık & Bal, 2024). Véliz (2021) goes on to claim that privacy is not only a personal preference, but also a collective power essential for the survival of democracy, updating Arendt’s insistence upon political freedom in the digital age. But such legal writings may still prove to be insufficient to fully secure the privacy of the individual from the state insofar as differences in room for manoeuvre are much greater when it comes to data that are processed on public security or other grounds based on national interest than data from the private sector. At this juncture law is slow to move and data colonialism indemnifies itself with legal gaps.

These legal boundaries are drawn with varying approaches on a global scale. For instance, while the European Union (EU), through the General Data Protection Regulation (European Parliament & Council of the European Union, 2016), treats privacy as a fundamental human right—effectively telling both the state and the market to 'back off' when it comes to personal data—the United States (US) plays a different game altogether. There, you see a more market-driven, sectoral pragmatism at work. Especially in that foggy, post-9/11 atmosphere where 'national security' became the ultimate trump card, the boundaries of state digital surveillance were pushed to an almost unrecognizable extent under the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). Turkey, on the other hand, appears to have adopted the EU model (Directive 95/46/EC) with its Law No. 6698 (KVKK); however, due to broad exceptions such as 'state security and public order' in Article 28, it exhibits a hybrid model that leaves a wider margin of maneuver for state authority in practice (KVKK, 2016). This situation causes individual privacy in Turkey's digital state applications to remain in a more fragile position against the concept of public interest.

In fact, privacy is one of the most emphasized subjects in computer and information ethics. Privacy is directly related to information and access to information, and the problem must be handled through the relationship between personal information and personal identity. Like all types of information, personal information should be respected, and privacy should be ensured in this area. Moving from the fact that humanity is constantly developing, protecting the individual's information privacy also means recognizing their freedom to develop (Stahl, 2008). Tallberg et al., (2023) notes that the lack of algorithmic transparency in today's digital ecosystem makes Habermasian rational deliberation impossible. In other words, privacy is also one of the key concepts regarding development. Uslander (2004a) argues that trust in the internet and relationships established over the internet can be structured not over strategic trust, as he defines it, but rather over moral trust. There are many examples where trust in the internet yields good results and good intentions are abused, yet the way to make the progress of a technological development like the internet possible passes through trusting humanity rather than strategic

trust. However, in internet-based applications, information moves much faster than controllable limits.

In *Data Sovereignty and Structural Privacy Threats*, Lember and Cromptvoets (2023) argue that the lack of control over personal data (which they call data sovereignty in relation to citizens) experienced by citizens due to the automation of data processing systems constitutes a legitimacy crisis. They further argue that this lack of control over personal data, which we experience acutely especially after learning about the weaknesses of public infrastructure in the age of digitalisation, is what we call data sovereignty of citizens, a term first coined by Cullen and Reilly (2007). For instance, after all state institutions went online through e-government portals, it became apparent that the state's information is very exposed to potential internal leaks or third party cyber attacks (STM Defense Technologies Engineering and Trade Inc.,2025). Maalla (2021) highlights the lack of transparency in the use of AI within the public administration system, which may convert the administration system into an instrument of social control, turning public administration into an administrative system that does not provide any positive public service to citizens. Hence, this feeling of being in the data flow without control constitutes a structural privacy threat which is not something that the individuals or society can do anything about. Rather, it is a constraint that needs to be overcome for the modernisation of the public administration through the digitalisation of the state and for the citizens to adapt to the new digital government tools. As shown in the studies of social media users in Turkey (Turan, 2024), citizens' attitudes towards social media and privacy and trust issues in this regard may change over time as citizens become more aware of being under surveillance. As Margetts and Dorobantu (2019) argue in relation to the digital state, citizens cannot be expected to trust the digital state by merely installing firewalls and using encryption. Complex accountability mechanisms need to be developed to account for the AI systems that monitor citizens.

At this very moment, our privacy is no longer a constitutional right that needs to be defended, but rather a constitutional barricade which signals the boundaries of a surveillance state in the digital age. As far as Habermas is concerned, the digital world should be the "liberum veto" of our time – meaning free and unencumbered spaces for discussion. Privacy is not an entry ticket for these spaces. Rather it is a precondition for having a digital space of communication that is free of surveillance. When an individual calls on the state to implement state-wide end-to-end-encryption through means of cryptography, anonymity and data sovereignty, in a state where the citizen is continuously under surveillance by highly efficient algorithm-based crime prevention technology – then this call is, in the modern age, characterised by the same features that Arendt identified in civil disobedience as a "space of resistance". Therefore, the normative solution in digital democracies lies in constitutionally guaranteeing privacy not as a favor granted by the state but as a founding and untouchable 'negative liberty' that limits state power. Otherwise, the digital state carries the risk of transforming not into a servant for its citizens but into a warden who records every move.

Wide powers given to governments using terms such as national security or public order can quietly erode personal privacy. In real situations, those justifications tend to act like open permission slips for gathering private information. Without outside review or regular checks, officials may stretch their reach far beyond what laws intend. Over time, the lines meant to contain digital surveillance grow fuzzy, almost meaningless. Slowly, a space forms where rules about data access are bent, ignored, reshaped – simply because they can be.

Nowadays governments lean heavily on hidden algorithmic tools when making choices. Not even lawyers or ordinary people get to peek inside how those tools reach conclusions.

Hildebrandt pointed out back in 2018 that not being able to follow the reasoning shuts down fairness. When a machine tags your name without explanation, fighting its call becomes pointless. When power goes unchecked, it weakens what keeps democracies honest. Laws alone cannot fix this gap. To stay an active participant in politics, not just raw material for tracking, people need stronger moral limits on government access – limits shaped through ongoing public argument. If that tension fades, mass monitoring by authorities could settle into everyday life without challenge.

Conclusion

That privacy is a human right is a universally accepted premise. Individuals want to be sure that information regarding themselves will be processed and treated fairly, but the state's collection, storage, and management of personal data regarding citizens render the issue of privacy increasingly critical. Indeed, empirical findings demonstrate that there are numerous cases where personal information stored in public institutions could not be protected, was abused, or was leaked externally during the e-government process which is still in its developmental stage. This situation erodes individuals' sense of trust in e-government and negatively affects their behavioral patterns and sentiments. Therefore, problems in the storage and use of personal information collected in public institutions must be identified, and procedural measures and specialized institutions must be established to prevent damage to the right to privacy.

This study, conducted on the limits of the digital state and individual privacy, goes beyond these necessities to reveal that the tension between the state's role as a "service provider" and its "surveillance" nature in the neoliberal era has eroded classical public sphere theories. The fundamental theoretical conclusion reached by the study is that the digital sphere has transformed into a transparency regime in which visibility is no longer a condition of democratic accountability but a mechanism of normalization and control. In this regime, privacy erosion operates not merely as a technical side effect of digitalization but as a structural transformation of the relationship between the state and the citizen. This conclusion resonates with recent arguments emphasizing that democratic legitimacy in digital states depends not on technological efficiency, but on the preservation of epistemic autonomy and meaningful consent within data-driven governance structures.

In this context, the following policy recommendations are of vital importance for digital state applications to maintain their democratic legitimacy:

1. **Data Minimization and Purpose Limitation:** Public institutions must abandon the logic of "hoarding data in case it is needed one day"; data collection processes must be strictly limited to the minimum level required by the service provided.
2. **Independent Audit and Transparency:** The state's data processing activities must be audited by autonomous boards supported by civil society and academia, independent of the executive branch; algorithmic decision-making processes (black boxes) must be made transparent.
3. **Privacy by Design:** When establishing e-government systems, privacy must be constructed not as a patch added later but as the architectural foundation of the system.

How should we conduct research into privacy in the future? The answer is: by thinking about what the surveillance technologies of tomorrow could mean for society and thus what we need to do today to counterbalance them. The future of privacy research should explore, for

example, the ethics of the use of artificial intelligence in predictive policing or how blockchain technology could help give citizens control of their personal data. Privacy will be the civil rights battle of the digital age. Current literature on the effects of digitalisation generally describes privacy as a purely technological or security issue, while this article suggests that privacy should also be described as a political issue in the context of digitalisation. It uses the theories of Hannah Arendt and Jürgen Habermas on the public sphere as a theoretical basis and examines how privacy acts as a component of political subjectivity and the foundations of democratic politics in the digital age. In the context of the digital state in particular, a state that is increasingly governed through technology, it is no longer sufficient to look at whether a state has high-tech infrastructure or whether citizens have access to adequate online services. Instead the digital state must also be viewed in terms of ethics and politics. And the ‘limit of the digital state’ is not about reaching the limits of what is technically possible, but rather about the moment at which technology intrudes upon human existence as a human being, as a person, as something that is dignity-filled and therefore privacy-protected.

Privacy is about more than just technology. It is about politics and the political nature of the self. The possibility of a truly open digital life presupposes a fundamentally different understanding of the state and of state power. Thus, it is necessary to think about the technological means of realising epistemic autonomy — that is, the conditions under which one can constitute one's own knowledge and opinions independently of the structures of algorithmic processing or the statistical predictions of models. Stronger ethical and legal norms are needed in order to prevent the surveillance state from becoming the standard form of governance. Protecting private space is no secondary or third-order question of politics; it is rather a constitutional one, one that is fundamental to the very idea of democracy.

References

- Arendt, H. (2023). *İnsanlık Durumu*, (B. S. Şener.Çev.). İletişim Yayınları.
- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity Press.
- Cullen, R., & Reilly, P. (2007). Information privacy and trust in government: A citizen-based perspective from New Zealand. In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 109–119). IEEE. <https://doi.org/10.1109/HICSS.2007.271>
- European Parliament and the Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L119, 1–88. Retrived January, 01, 2026, from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Flaherty, D. (2000). Privacy impact assessments: An essential tool for data protection. *Privacy Law & Policy Reporter*, 7(5), 85–90.
- Fuchs, C. (2023). *Digital democracy and the digital public sphere*. Routledge.
- Giddens, A. (1985). *The nation-state and violence: Volume two of a contemporary critique of historical materialism*. University of California Press.
- Habermas, J. (2019). *Doğalcılık ve din arasında felsefi denemeler*, (A. Nalbant, Çev.). Yapı Kredi Yayınları.
- Habermas, J. (2021). *Kamusallığın yapısal dönüşümü*. (T. Bora & M. Sancar, Çev.). İletişim Yayınları.
- Han, B.-C. (2017). *Şeffaflık toplumu* (H. Barışcan, Çev.). Metis Yayınları
- Hildebrandt, M. (2018). Algorithmic regulation and the rule of law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2128), Article 20170355. <https://doi.org/10.1098/rsta.2017.0355>
- Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2004). Security requirements engineering for e-government applications: Analysis of current frameworks. In R. Traunmüller (Ed.), *Electronic government (EGOV 2004) (Lecture Notes in Computer Science*, Vol. 3183, pp. 66–71). Springer. https://doi.org/10.1007/978-3-540-30078-6_11
- Lee, Y., Bradford, B., & Posch, K. (2024). The effectiveness of big data-driven predictive policing: Systematic review. *Justice Evaluation Journal*, 7(2), 127–160. <https://doi.org/10.1080/24751979.2024.2371781>
- Lember, V., & Cromptvoets, J. (2023). Public services and management in the digital age. In T. Bovaird & E. Loeffler (Eds.), *Public management and governance* (4th ed., pp. 141–152). Routledge. <https://doi.org/10.4324/9781003282839-13>
- Maalla, H. A. (2021). Artificial intelligence in public sector: A review for government leaders about AI integration into government administrations. *International Journal of Academic Research in Economics and Management Sciences*, 10(4), 27–39. <https://doi.org/10.6007/IJAREMS/v10-i4/11911>

- Margetts, H., & Dorobantu, C. (2019). Rethink government with AI. *Nature*, 568 (7751), 163-165. <https://doi.org/10.1038/d41586-019-01099-5>
- Maslej, N., Fattorini, L., Perrault, R., Gil, Y., Parli, V., Kariuki, N., Capstick, E., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., Walsh, T., Hamrah, A., Santarlasci, L., ... Oak, S. (2025). *The AI Index 2025 annual report*. Stanford University, Institute for Human-Centered AI. <https://doi.org/10.48550/arXiv.2504.07139>
- Morozov, E. (2011). *The net delusion: Dark side of internet freedom*. PublicAffairs.
- Paye, J. C. (2004). Terörle mücadele ve özel hayatın denetimi. *Conatus Çeviri Dergisi*, 1(1), 153–165.
- Resmi Gazete. (2016, 7 Nisan). 6698 sayılı *Kişisel Verilerin Korunması Kanunu (KVKK)*
- Stahl, B. C. (2008). Discourses on information ethics: The claim to universality. *Ethics and Information Technology*, 10(2-3), 97–108. <https://doi.org/10.1007/s10676-008-9171-9>
- STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. (2025, Ocak-Mart). *Siber tehdit durum raporu*. STM. <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2025>
- Susser, D., Roessler, B., & Nissenbaum, H. F. (2019). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review*, 4(1), 1–45. <https://doi.org/10.2139/ssrn.3306006>
- Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M., & Lundgren, M. (2023). The global governance of artificial intelligence: Next steps for empirical and normative research. *International Studies Review*, 25(3), Article viad040. <https://doi.org/10.1093/isr/viad040>
- Tanczer, L. M. (2020). 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. *Contemporary Security Policy*, 41(1), 108–128. <https://doi.org/10.1080/13523260.2019.1669336>
- Tanışık, S., & Bal, S. (2024). Dijital mahremiyet ve kurumsal sorumluluk: Kişisel verilerin korunmasında iletişim teknolojilerinin kamusal rolü. *Yeni Medya*, (16), 268–285. <https://doi.org/10.55609/yenimedya.1424182>
- Teh, J. (2002). Privacy wars in cyberspace: An examination of the legal and business tensions in information privacy. *Yale Journal of Law & Technology*, 4, 1–96. <https://yjolt.org/volume/4>
- Timisi, N. (2003). *Yeni iletişim teknolojileri ve demokrasi*. Dost Kitabevi Yayınları.
- Turan, Y. (2024). Sosyal medyada gözetim ve mahremiyet algısı: Instagram kullanıcıları üzerine bir inceleme. *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, (47), 146–169. <https://doi.org/10.31123/akil.1427283>
- USA PATRIOT Act, Pub. L. No. 107–56, 115 Stat. 272 (2001). <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>
- Uslaner, E. M. (2004a). Trust online, trust offline. *Communications of the ACM*, 47(4), 28–29. <https://doi.org/10.1145/975817.975838>

- Uslaner, E. M. (2004b). Trust, civic engagement, and the internet. *Political Communication*, 21(2), 223–242. <https://doi.org/10.1080/10584600490443895>
- Véliz, C. (2021). *Privacy is power: Why and how you should take back control of your data*. Penguin Random House.
- Webster, F. (2021). *Theories of the information society* (4th ed.). Routledge. <https://doi.org/10.4324/9781315867854>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Information About the Article/Makale Hakkında Bilgiler

The Ethical Rules for Research and Publication / Araştırma ve Yayın Etiği

The authors declared that the ethical rules for research and publication followed while preparing the article.

Yazarlar makale hazırlanırken araştırma ve yayın etiğine uyulduğunu beyan etmiştir.

Conflict of Interests/ Çıkar Çatışması

The authors have no conflict of interest to declare.

Yazarlar çıkar çatışması bildirmemiştir.

Grant Support/ Finansal Destek

The authors declared that this study has received no financial support.

Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

Author Contributions/ Yazar Katkıları

The draft process of the manuscript/ Taslağın Hazırlanma Süreci E.Ç./M.D., Writing the Manuscript/ Makalenin Yazılması E.Ç./M.D., Submit, Revision and Resubmit Process/ Başvuru, Düzeltme ve Yeniden Başvuru Süreci M.D.