

Narrative Review
Received: 26.1.2026
Accepted: 25.2.2026

UDK: 316.74:004
340.134:351.86(470)
340.134:351.74/.75(470)
340.134:351.86(73)
340.134:351.74/.75(73)
DOI: <https://doi.org/10.58984/smb26021431>

Corresponding author: slobodan.penezic@fzs.edu.rs

INFORMATION-CONTROLLED SOCIETY AND ROLE OF THE MEDIA: A STUDY OF THE USA AND THE RUSSIAN FEDERATION

Tomislav Lunić¹, Slobodan Penezić²

Abstract: *This paper examines the transformation of contemporary networked societies through the emergence of the information-controlled society (ICS). The aim of the study is to conceptualize the notion of the ICS and to comparatively analyze its manifestations in the United States of America and the Russian Federation, with particular emphasis on legal regulation, traditional media structures, and the online public sphere. The research adopts a comparative narrative review design combined with qualitative case study analysis, integrating content analysis of legal and institutional sources with a systematic comparative method. The findings indicate that the United States operates through a hybrid state–market model of information control characterized by advanced technological infrastructure, corporate data exploitation, and normalized surveillance practices, while the Russian Federation relies on a predominantly centralized state-centered model marked by direct political influence over broadcast media and expanding regulatory oversight of the digital sphere. Despite structural differences, both cases demonstrate convergent tendencies toward the consolidation of informational power, increased surveillance capacities, and the gradual erosion of citizens’ autonomy within the public sphere. The study argues that contemporary systems of information control transcend the traditional dichotomy between democratic and authoritarian media models, revealing hybrid mechanisms of governance embedded in global digital infrastructures.*

Keywords: network society, electronic surveillance, digital governance, media concentration, privacy regulation

¹ Faculty of Security Studies, University of Belgrade, Belgrade, Serbia

² Institute for Social Sciences, Belgrade, Serbia; Department of Journalism, Faculty of Sport, Union – Nikola Tesla University, Belgrade, Serbia

Introduction

The concept of technofeudalism, advocated by Yanis Varoufakis, as a modern order in which technological platforms – driven by algorithms and data – turn users into subjects and undermine democracy through hidden power management and manipulation, introducing new forms of domination and relations, while generating immense wealth for those who understood this direction of human development early enough (2025), strongly signals the contours of the circumstances in which we all exist today, thus further underscoring the importance of this context.

At the core of contemporary society, therefore, is the importance of information management – their production, availability, and interpretation – essentially, control. Manuel Castells notes that the “control over information lies with corporations that control the networks on which information resides and through which it is transmitted, while governments (globally influential ones) control those corporations, thereby using combined TT and legal capacities to influence the availability and processing of information in the public sphere” (Castells, 2024: 31).

Through this lens we may view the foundational landscape of this paper, which turns toward the domain of the development of digital technologies, communication instruments, computers, the global network – i.e., the internet – and the increasingly significant influence of artificial intelligence (AI).

The accelerated development of digital technologies, global communication networks, and artificial intelligence has fundamentally reshaped contemporary societies. Information has become a central strategic resource, embedded in economic structures, political processes, and cultural production. Within this context, mechanisms of surveillance, data processing, and media influence increasingly determine the dynamics of governance and public life. As digital infrastructures expand, power is no longer exercised solely through traditional state institutions but also through the control of information flows within global networks.

Theoretical reflections on the information society and the network society – such as the works of Manuel Castells, Yanis Varoufakis, and Yuval Noah Harari – highlight the growing importance of data, algorithms, and communication infrastructures in shaping contemporary power relations. These transformations raise critical questions regarding the balance between security and privacy, efficiency and autonomy, and technological progress and democratic accountability.

In this broader framework, the notion of the information-controlled society (ICS) emerges as a conceptual tool for understanding how surveillance technologies, media systems, and regulatory mechanisms interact to shape citizen behavior and public discourse. The ICS does not refer merely to technological advancement, but to a structural configuration in which information becomes the primary medium of governance and control.

The aim of this study is to conceptualize the notion of the ICS and to comparatively analyze its manifestations in the United States of America and the Russian Federation, with particular

emphasis on legal regulation, traditional media systems, and the online public sphere. By focusing on these dimensions, the paper seeks to identify similarities and differences in the organization of information control within distinct socio-political contexts and to assess their implications for citizens' autonomy and the structure of the public sphere.

Methodologically, the study is structured as a comparative narrative review combined with qualitative case study analysis, whose detailed framework is presented in separated chapter.

The central research question guiding this study is whether contemporary systems of information control differ fundamentally between democratic and authoritarian environments, or whether they represent structurally different yet functionally convergent models embedded in the global network society.

By addressing this question, the study contributes to a more nuanced understanding of informational power in the digital age, moving beyond simplified binary classifications and examining hybrid configurations of state and market influence over communication infrastructures.

Theoretical Background

Information as a Key Resource of Contemporary Power

The concept of information was originally linked to problems of telecommunications technology and the study of algorithms for encoding, measuring, and assessing the quality of message transmission (particularly in the work of Claude Shannon and the so-called electro-engineering approach³). Information was thus reduced to the technical aspects of transferring content from sender to receiver, without touching other dimensions. Perhaps the most comprehensive definition is, therefore, given by Luciano Floridi, who defines information as “an objective, declarative, and syntactic content of varying size, type, format, and carrier, which can be produced, processed, stored, transmitted, and accessed in various ways”, emphasizing that “truthfulness is the key parameter in determining the difference between information and disinformation” (2005: 352).

Yuval Noah Harari notes that many scientific actors across different fields view information as “the basic building block of reality, more elementary than matter and energy” (2024: 39). Cybernetics, as the science grounded in information theory, studies feedback loops in communication and control, and its well – known first law – that those who possess information rule – can serve as a significant lens for our analysis. In this context, the reflections of Manuel Castells are especially significant. He argues that we live in a networked society in which key social functions are organized through digital communication networks, and information thereby becomes the primary resource of power (2018a).

Processed data produce information, while processed information yields knowledge. Information thus shapes one's understanding of reality – but also reality itself. “Information

³ More details at: Shannon, C E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27(3), 379–423. <https://doi.org/10.1002/j.1538-7305.1948.tb01338.x>.

has a dual nature and is primarily tied to the phenomenon of the information society" (Subotić, 2011: 16). The notion of the information society is, therefore, inevitably linked to information-communication technologies and their widespread use. Beniger (1986) points to numerous synonyms for the information society, such as "knowledge economy", "technological society", "computerized society", "information age", "industrial-technological society", "telematic society", and "post-industrial society". Therefore, Gilles Deleuze developed the concept of the society of control, whose foundation is "continuous monitoring and information management" (Mlađenović, 2025: 119).

The information society is thus an organic successor to the industrial society, transformed in structure while retaining essential characteristics. Such society may be defined in three principal ways. *The first* is based on the concept of information processing; *the second* is qualitative and concerns the adequate use of information-communication technologies; *the third* is quantitative and relies on measurable parameters that determine the degree of ICT application in various social processes.

The information society remains in continuous development. "Ultimately, we must place it within the modern framework of sustainability, where it is harmonized in ecological, social, economic, and cultural terms" (Shauer, 2003: 6). At this point, the previously mentioned first law of cybernetics ("Whoever has information – rules") receives new confirmation within the contemporary societal framework. Concretely, Castells believes that today, instead of the former geographical and hierarchical logic based on a monopoly of force in its traditional sense, there is a dominant logic of a global network through which capital, information, people, and symbols move. This is in line with Varoufakis' described concept of technofeudalism. In such a society, identities and power are in fact shaped through communication networks, which can serve both social control and resistance.

The key question, therefore, is no longer who owns the means of production, but who controls the infrastructure that generates meaning and attention. Harari thus quite rightly asks: "Can we trust computer algorithms to make good decisions and create a better world?" (2024: 24), and warns us about the growing influence of AI. He also notes that the main protagonist of our time is in fact not the human being (*homo sapiens*), but information itself, because of which the new information technologies might ultimately "take power away from us and destroy our physical and mental health" (Harari, 2024: 24).

The flip side of current global technologization thus becomes confirmation that once unconditional faith in the liberating potential of the internet – as it was predominantly perceived at the outset – was unfounded. It is, however, still alive, because "it has to some extent awakened the hope that citizenry would be reactivated and the superior aspects of digital communication are therefore still taken as a perfected guarantee of civil liberties in the present age" (Penezić, 2022: 6).

At this point, we can also focus on our primary domain of analysis. The phrase *information-controlled society (ICS)* points to a complex paradigm manifested through the controlled dissemination of mass-media messages on the one hand, and electronic surveillance on the other, for the sake of establishing a high degree of control and steering of population

behavior. Roger Clarke defines the conditions for establishing an ICS as follows: the creation of databases that record information about citizens and their various activities, an appropriate structure of computer networks (...) a reliable technological scheme that enables the formation of a virtual registry for every inhabitant through the combination of heterogeneous databases, and a population willing to accept all this (1997). The ICS thus also points us toward a “surveillance society” and a “society of total surveillance”, which we see as a result of the fact that “information-communication technologies of electronic surveillance and mass – media dissemination of messages are used in parallel in order to achieve the highest possible degree of control over the population and to shape a desirable model of citizens’ behavior on a mass scale” (Subotić, 2011: 32).

Taking into account these broader social dimensions and processes – and thereby underscoring their significance – we can turn more directly to the phenomenon of the ICS itself. In this sense, the first question that arises is whether it represents coercion and/or necessity, a question we may examine through the lens of the preconditions for the emergence of an ICS, the specificities of surveillance, and the role of media in the overall state of the public sphere.

Preconditions for the Emergence of an ICS

The preconditions for the emergence of an ICS primarily relate, as we see, to the influence of the technological factor as such, that is, to understanding the potential of technological solutions applied to the surveillance of the population for the purposes of planned governance and social shaping.

This specific attitude toward the technological factor became particularly important after the mass destruction of the 20th century, when questions of democratic control of the military and control of nuclear weapons came to the fore, while the issue of safeguarding freedom, relegated to the background in such circumstances, was simultaneously endangered and neglected.

This raises a rhetorical question: *Was a vast field for abuse and manipulation already opened at that time?* Perhaps the most significant classification of theoretical approaches to technology was given by Andrew Feenberg:

- “Determinism: technology is value – neutral and autonomous in its development;
- Instrumentalism: technology is neutral and controlled by humans;
- Substantivism: technology is value – laden and autonomous (Heidegger and Ellul are the most notable representatives);
- Critical theory: technology is value – laden, but with the possibility of human agency, with Marcuse as the key representative” (Feenberg, 1999: 9).

The preconditions for its emergence certainly include the legal framework that unites the phenomena of privacy and security culture. The classical legal definition of privacy is associated with U.S. judges Louis Brandeis and Samuel Warren at the end of the 19th century,

who characterized the right to privacy as “The right to be let alone”⁴ (1984: 76). From that period, privacy protection is linked to legal guarantees. Today, it belongs to the corpus of personal rights and is protected both by national and universal legal mechanisms. “Notable examples include:

- The International Covenant on Civil and Political Rights, whose Article 17 protects citizen privacy by stipulating that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation”;
- The Universal Declaration of Human Rights, whose Article 12 requires that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation,” and that everyone has the right to legal protection against such interference;
- The European Convention on Human Rights, which permits state interference in citizens’ privacy only to the extent that it is genuinely necessary” (Subotić, 2011: 51).

William L. Prosser defines practical violations of privacy in the legal sense through several parameters, the most important being: “intrusion into someone’s solitude or private affairs; public disclosure of private facts about a person; casting someone in a false light before the public; and appropriating someone’s name or likeness for personal benefit” (1984: 107). Beyond this, Edward J. Bloustein points to an integral approach, relating privacy violations to infringements of human dignity (1984).

In the context of contemporary circumstances, it is important to distinguish between the private and the public. In its basic sense, the private refers to family and personal matters, while the public refers to the state, civil society, and the market. The problem of privacy within an ICS involves institutional and corporate violations of privacy through the collection of large amounts of data on citizens. Thus, protecting the right to privacy is a demanding task – especially today.

It is therefore necessary to mention the affirmation of a security culture, which includes socially acceptable security behaviors and the acceptance of patterns of controlling such behavior. Here we encounter the necessity of establishing an ICS and affirming it for the sake of societal survival; otherwise, insecurity would be inevitable. In such a paradigm, the ICS “appears as a solution that prevents system disintegration and enables effective risk control, while also embodying the utopian dream of total control over harmful and uncontrolled tendencies (e.g., real dangers of terrorist attacks or threats against the state and the people)” (Subotić, 2011: 61).

There is, however, a danger of “suspending” privacy in the name of general goals of preserving public order. It is therefore necessary to balance and carefully calibrate the interplay between security culture and appropriate mechanisms of population control or surveillance within the concrete informational environment.

Another precondition for establishing an ICS is its acceptance among the wider population and the potential of various socio-political systems for forming such a society, including an uncritical attitude toward technology, relativization of the right to privacy, and the establishment of a corresponding security culture.

In totalitarian societies, the imposition of an information-controlled environment in its full scope is natural. In such systems, *de facto* (and often *de jure*) “free and spontaneous citizen action is prevented, and unquestioned, total loyalty is demanded from them” (Arendt, 1998: 332), primarily due to the need to control the opposition. “Authoritarian regimes are characterized by a paradigm that requires submission to authority, aggression toward nonconformists, cognitive rigidity, and intolerance of authoritarian personalities” (Peterson & Pang, 2006: 443–444). On the other hand, democratic capitalist societies and the application of ICS within them also include some totalitarian connotations, because surveillance measures are carried out over everyone. The goal is the rationalization of public administration, increasing productivity, improving sales of products and services, etc.

Our study focuses on contemporary conditions marked by the development of networked social structures – i.e., deterritorialization – where nation–states retain a monopoly on force within their borders. In this sense, determining the potential for implementing an ICS depends on defining statehood within a globalized world. At the same time, with the spread of modern democratic principles, the needs for political engagement of the driving forces of surveillance have increased, as well as the need to establish an appropriate bureaucratic apparatus (introduction of bureaucratic documentation and structures) and “support” through industrialization. What we see, therefore, is a thin line of “maneuvering” between coercion and objective necessity in a globally networked society, where local circumstances only further stimulate – or hinder – the application of one or the other logic.

The phenomenon of surveillance initially appeared with clearly defined objectives. At first, it was reduced to “locating malfeasance such as tax evasion or money laundering, and later to counterintelligence surveillance amid inter – bloc tensions” (Lyon, 1994: 89–90). With globalization, the classical paradigm of surveillance has been transformed. David Lyon also notes that the level of surveillance depends on five parameters: “economic factors, technological development, the legal system and specific regulations, colonial history, and relations with the USA” (2008: 45).

Oliver Subotić offers a basic classification of the phenomenon of surveillance in contemporary society according to “two criteria:

- according to the subjects of surveillance (those who conduct surveillance), their goals, and the objects of surveillance (those who are surveilled)⁵;

⁵ The focus shifts from the local to the global level, and the subject of surveillance from the state to corporations and the private sector (thus, surveillance is no longer carried out exclusively by the state). It should be noted that the object of surveillance in contemporary society may be an individual as such, but also an individual as a member of a particular social group. The “most extreme” objects of

- according to the surveillance technology used, the characteristics of the data collected, and the actions carried out in the process” (Subotić 2011: 72).

Perhaps the best definition of contemporary surveillance is again given by David Lyon, who states that modern surveillance is “a complex and combined activity of state administration, police – security structures, and corporations” (1994: 81).

The key event that changed the modern paradigm in the direction of creating a so-called security state is undoubtedly the terrorist attack on New York on 11 September 2001. The “Big Brother” paradigm, in which one center exercises complete surveillance, was reorganized into a polycentric form that includes various structures. In academic circles, this new structure is called the “Little Sisters” structure. “It is a networked structure of surveillance and information control in which each small center – a node in the network – reveals one segment of human identity and the sphere of privacy, while full exposure is possible through the coordination of all nodes’ activities together” (The Royal Academy, 2007: 19).

Long ago, Martin Heidegger announced such a change in the very essence of modern man, who changes in the direction of a “mere technologized animal” from the moment he becomes a primary resource of technological control (1977: 19–30). He warned of a “monstrous reversal that could lead us to a catastrophic outcome”, not only pointed to the practical threats brought by various new technologies, but also to a particular ontological threat to human reality and being, noting that “as we fear a catastrophe – it may already be taking place in our reality” (Пенеzić, 2022: 5). The current challenges posed by AI considerably revitalize that warning.

Namely, Joseph Stiglitz from the contemporary perspective points to similar consequences, speaking of the shifting of foundational logic and the failure of desired outcomes within today’s dominant techno-globalization tendencies, which – rather than producing positive results – lead instead to the emergence of new divisions, misunderstandings, and negativities across the world (2018). This is a conclusion we can often draw when observing technological progress, manifested in new communication tools and possibilities⁶, because of which, as Marcuse once concluded “every individual is thus forced to adapt to and conform with an imposed modality of living of a technological character” (1968: 153).

This overview of relevant reflections, therefore, gives us a possibility of recognizing objectively that today – given the technological context – also exists a real danger (perhaps greater than ever before) that the ICS is acquiring features of coercion, implicitly evident when anticipating the phenomenon of social control.

surveillance include, for example, prisoners or workers in highly secured facilities, as well as members of specific professions who wear electronic bracelets (Clarke, 2001).

⁶ It is a question of technology transfer (TT) as a process of conveying scientific discoveries from one organization to another for the purpose of further development and commercialization.

The Role of Media Organizations

The role of the media (media organizations) in ICS is probably crucial for shaping the attitudes of a population (and thus its behavior). Given their influence and specificities, we may say that they constitute a problem *sui generis*.

At the same time, their social role certainly also should be viewed through the lens of the media propaganda, especially in totalitarian and authoritarian regimes, because of which Subotić rightly notes that we also should consider the possibility of political and corporate influence on the media in democratic societies through the prism of media monopoly/oligopoly (2011).

Marshall McLuhan's well-known metaphor "The medium is the message" (2005: 262), originally structured in 1964, becomes a paradigm of contemporary society. Paul Levinson applied this idea to the television, placing it in the context of a factor that influences people's lives even "more comprehensively and on a broader scale" (2004: 35), while Graeme Burton emphasized that television affects "changes in human attitudes, the increase of anxiety, the acceptance of certain patterns of behavior, the support of particular ideologies, etc" (2005: 101).

It is clear that television (and to a great extent other so-called traditional media) still represents a powerful weapon, despite the strong influence of the internet. Therefore, it is important to point out the possibilities of the internet in this domain, since it "has the capacity to integrate all previous media and unique forms of communication – everyone with everyone (...) and to become the *par excellence* medium of the information-controlled society" (Subotić, 2011: 97).

Given the current communication context, we must also address certain formal innovations that have occurred in recent times, driven by IT challenges and directly relevant to our analytical framework. This is, first of all, the General Data Protection Regulation (GDPR)⁷, which concerns the protection of privacy of information in the European Union and the European Economic Area. It is a key component of EU privacy law and human rights law (in particular Article 8 of the Charter of Fundamental Rights of the EU), and also regulates the transfer of personal data outside the EU and EEA, which is necessary. This is important because it has prompted numerous operational changes in the world of communication, as well as in the media sphere (and global communication as a whole). All this was intended to protect individuals' privacy and personal data, which in reality, however, has not been fully achieved, since abuses still occur in the online sphere, with the new regulatory framework being skillfully circumvented.

We must then mention the latest changes in this area: the Digital Markets Act (DMA) and the Digital Services Act (DSA)⁸. The DMA, namely, concerns the platform that allows traders to

⁷ More details at: GDPR, n.d. *What is GDPR, the EU's new data protection law?*. <https://gdpr.eu/what-is-gdpr/>. Accessed 2 April 2025.

⁸ More detail at: European Commission, n.d. *The Digital Services Act package*. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. Accessed 3 April 2025.

communicate directly with marketers and exchanges, enabling faster and more precise trading, while the DSA, linked to the DMA, allows automated trading strategies to enter the so-called execution channel of operations. Both are also attempts to regulate the contemporary social context while simultaneously protecting basic human rights – but, as in the case of the previously described changes, it will be important to observe whether they will bring substantive changes that keep pace with the times *and* the protection of human rights and freedoms, or whether they will simply further complicate the functioning of all actors, while still allowing those who profit in the fog of the newly created confusion to further appropriate these aspects for the sake of profit.

The described innovations and their consequences can again be analyzed through the lens of Castells' network society. In it, power shifts from centralized institutions to networks that control information flows, which is also visible in contemporary phenomena such as manipulation via social networks, algorithmic management of attention, and the so-called platform economy (e.g. Uber, Amazon). In such an ICS, digital surveillance and datafication become new forms of control, replacing traditional institutional mechanisms. At the same time, new forms of resistance appear through hacker movements, online activism, and alternative networked communities that attempt to reclaim narratives and redefine identity. Castells thus emphasizes that networks in themselves are neither democratic nor authoritarian; their social effect depends on who controls them and how they are used (2018a, 2018b) – a crucial remark toward which our analysis also tends.

We believe that such an interpretation can be perfectly applied to current considerations of the development and consequences of the changes brought by new media tools and AI. On the other hand, this new type of power – arising from influence over the formation of meaning and identity through so-called networked communication – also brings us to the described Castells' concept of "communication power". This theory illuminates the tension between emancipation and control in the contemporary digital age, which we also highlight here through the dynamics of choosing between the logic of necessity and that of coercion.

We shall therefore next turn to case studies of the USA and the Russian Federation, which we will analyze through the prism of legal regulations, the role of the media, and the influence of new technologies in determining the degree of social surveillance. Both the USA and the Russian Federation are unquestionably global driving forces of 21st – century civilization and are among the key actors in the global socio-political spectrum. Hence, analyzing these elements is essential for understanding their potential and capacities (and, more broadly, their power).

The Case of USA

Legal Framework

The Constitution of the USA does not directly regulate the issue of surveillance (info-control), but it does so indirectly through several amendments (the First covers freedom of speech, religion, and association; the Fourth protects individuals from unlawful surveillance by

government agencies; the Fifth concerns private property; the Fourteenth further protects the private life of citizens from the government).⁹

Other relevant regulations pertain “primarily to the Report of the Special Committee on the Code of Fair Information Practices from 1973, which mainly concerns the use of personal data, as well as the Freedom of Information Act from 1966, which relates to the protection of the right to privacy” (Holtzman, 2006: 109). Alongside these is the Privacy Act of 1974, which regulates the right of citizens to be informed when information about them is collected, arising from the concerns expressed in the Special Committee’s Report a year earlier, and which provides “the possibility of access and correction where necessary, except in cases where data are collected for national security purposes” (Holtzman, 2006: 110).

The Electronic Communications Privacy Act of 1986 protects citizens from the “interception of electronic information, providing protection from the federal government” (Committee on Privacy, 2007: 136)¹⁰.

In the USA there is no institution comparable to the Commissioner for Information of Public Importance and Personal Data Protection (as in Serbia), so citizens are particularly endangered in the field of human rights concerning surveillance conducted by the private sector.

Traditional Media Sphere

We take the USA as the setting in which the influence of the so-called mass media reached its culmination over the previous century. Ben Bagdikian reminded at the beginning of this century that global media ownership is in the hands of “around fifty corporations, and that the USA had more than 1,700 daily newspapers, 11,000 magazines, about 9,000 radio stations, 1,000 television stations, 2,500 publishers, and seven film studios” (2000: 4–22).

Perhaps the greatest problem for the media in the USA in 21st century is the dual influence of so-called big capital, which exerts pressure on advertisers on the one hand, and influences editorial policy on the other. As a consequence, media markets become increasingly concentrated, meaning ownership concentration and the creation of media monopolies. The consequences for the quality of reporting in such an environment are easy to imagine. Jeremy Tunstall and Michael Palmer, therefore, pointed out to the problem of capital being grouped into media cartels, i.e. the establishment of classic media monopolies (2001). For example, in 1989 there was a merger between Time and Warner, after which “this corporation became a leader in the music industry and Hollywood films, and the second largest national operator of local cable systems in the USA” (Tunstall & Palmer, 2001: 39), while Bagdikian also warns of

⁹ It should be noted that the first ten amendments constitute the Bill of Rights. More details at: U.S. Senate (n.d.). *The Constitution of the United States of America*. https://www.senate.gov/civics/resources/pdf/US_Constitution-Senate_Publication_103-21.pdf. Accessed 8 January 2025. Amendment 1, 4, 5 (all 1971), and 14 (1868).

¹⁰ More details at: Committee on Privacy. (2007). *Engaging Privacy and Information Technology in a Digital Age*, ed. J. Waldo et al. Washington, D.C.: The National Academies Press.

the emergence of one of the largest communication conglomerates, tied to the merger of Time Warner and America Online (2000: 11).

It is also considered that the largest media lobby in the world is likewise based in the USA – the Motion Picture Association (MPA), which includes: Amazon MGM Studios and Amazon Prime Video, Netflix, Paramount Pictures, Sony Pictures, Universal Pictures, Walt Disney Studios, and Warner Bros. From 1922 to 1945 it was called the Motion Picture Producers and Distributors of America, and from 1945 to 2019 the Motion Picture Association of America. It is worth noting that the MPA plays a major role in combating copyright infringement.

We should also not omit Rupert Murdoch, a media mogul of global proportions. In addition to practically controlling 175 newspapers worldwide through his NewsCorp, via DirecTV he also controls cable and satellite television in the USA. He owns Fox, which represents a paradigm of his media power. According to *Forbes* magazine, Murdoch is “the 38st richest person in the USA and the 87st richest in the world” (Forbes, n.d.)¹¹.

Almost all types of media content in the USA – from music videos and TV programming to films, magazines, and books – have for some time been controlled by a handful of media magnates: General Electric, Viacom, Disney, Bertelsmann, AOL Time Warner, NewsCorp. The print media and news service in the USA are largely under the control of the Associated Press (AP).

The influence of some of these actors extends into the domain of the internet and online media, so in the field of internet regulation the greatest potential likewise lies with American companies such as AOL Time Warner, along with AT&T and Microsoft. Of course, control of the internet is not possible to the same extent as with other media, but it is important to emphasize that the USA still remains the most developed in terms of internet capacity and infrastructure.

The list of examples that could further confirm these trends is certainly much longer than what is presented here. It is expanded by the roster of contemporary technological and communication giants that today exert enormous influence in the media industry¹², and more recently also by those working in the field of AI development, whose impact is increasingly felt in this domain as well.

In examining the media landscape in the USA, we should also highlight the influence of the American government on the media. Ever since the emergence of the print press, the US establishment has relied on it through various methods of lobbying and pressure, often entering into conflicts of interest. The goal has always been the same: to establish and maintain power and keep public opinion at a level favorable to the authorities. On the other hand, opposition forces and critical voices of influential individuals have most often been reduced or minimized as far as possible. Citizens have consistently been given a narrowed

¹¹ For more detail: Forbes. (n.d.). *Rupert Murdoch*. <http://www.forbes.com/profile/ruPERT-murdoch/>. Accessed 12 January 2025.

¹² Foremost among these are the companies of the so-called “Big Five”: Alphabet, Amazon, Apple, Meta, and Microsoft, which also rank among the economically wealthiest in the world.

range of information, tailored to the so-called mainstream media aligned with the government.

Good examples include the bombing of the FRY in 1999 or the Iraq War in 2003, when the propaganda machinery did much of the work through anti-war propaganda materials but also through censorship of opposition voices. It can also be observed that some media tend to cover up incidents when the USA or its allies are behind them.

Russian Federation Case

Legal Framework

The protection of personal data, the right to privacy, and the prohibition of collecting, processing, and forwarding data without the knowledge of the person concerned, except in cases provided by law, are regulated by the Constitution of the Russian Federation.

Therefore, when it comes to the broadest and most general legal-formal framework influencing dynamics in this context, it primarily rests on the content of the Constitution. Article 29(1) of the Russian Constitution guarantees freedom of thought and speech; Article 29(4) guarantees the right to freely seek, receive, transmit, produce, and disseminate information; and Article 29(5) guarantees freedom of the mass media and prohibits censorship.¹³

This area is further regulated by a package of laws from 2006, which includes: the Law on Personal Data, the Law on Information, and the Law on Information Technologies and the Protection of Information.

“We should also mention SORM – 1 (1995) and SORM – 2 (1998). SORM – 1 represents a combination of CALEA and the Patriot Act legislation and is, in a way, their counterpart, while SORM – 2 presupposes the existence of a court order for the surveillance of the communications of a particular person, which often is not the case in practice” (Deibert, 2008: 181).

“The government controls communication resources and channels through the 2000 Information Security Doctrine, but due to the low level of development of information – communication infrastructure this has been reduced to two main areas: the monitoring of internet communications and government control of the media” (Subotić 2011: 159).

Traditional Media Sphere

In Russia, the influence of the government on media organizations is generally strong, especially on those operating within the traditional media framework. Zassoursky notes that the state focuses on controlling the media sphere because of its clear perception that the media are an important instrument for maintaining the stability of the entire state system,

¹³ More details at: The Ministry of Foreign Affairs of the Russian Federation (3 July 2000). *The Constitution of the Russian Federation*. https://mid.ru/en/foreign_policy/fundamental_documents/1750525/. Accessed 8 January 2025.

and that an additional argument is found in the “consequences from the period immediately after the Cold War” (2009: 29).

As for media monopolies, perhaps the most influential figure at one time was Boris Berezovsky, who became rich during the privatization of state assets in Russia in the 1990s. He owned Channel 1, TV – 6, and numerous publishing houses. With the arrival of Vladimir Putin to power, a crackdown on the oligarchs began, and the media sphere came under the tight control of the state apparatus.

The emphasis of state control is primarily on television and less on the print media. Zassoursky believes that the state “directly or indirectly controls all major television stations: Channel One and Channel Two, TV Center, Rossiya, Kultura, Sport, NTV, and TNT” (2009: 31–32). Radio and print media in Russia are under noticeably less direct state control. The largest magazine publisher in Russia is Independent Media, whose content mostly encourages opposition forces.

Ellen Mickiewicz warns that there is a serious problem of self – censorship and press freedom in Russia, and that investigative journalism is also “at a low level, primarily due to frequent and unresolved murders of journalists” (2008: 31).

The media role of the internet and online media in this segment of the media market is still at a lower level, primarily because the Russian population has only recently gained broader, mass access. In this sense, it should be noted that this field is developing, digital channels are being improved, and therefore the possibilities for criticizing the government are growing in both scope and importance.

Methodological Framework

This research adopts a comparative case study approach, focusing on the United States and the Russian Federation as distinct socio-political environments in which information control and electronic surveillance are exercised. The primary aim is to identify similarities and differences in the ways information is utilized as a tool of social regulation and governance, also as the general use of information as a tool of social regulation and governance within contemporary society.

Three complementary methods were employed to ensure a comprehensive analysis. First, case studies allowed for an in-depth examination of electronic surveillance practices within the selected countries. Second, content analysis was applied to relevant legal documents, policy reports, scholarly literature, and media sources to uncover patterns of control and regulation. Third, a comparative analytical framework facilitated the systematic juxtaposition of findings from both cases to highlight key distinctions and commonalities.

Within each case study, the research predominantly focused on three aspects: the legal framework governing information and surveillance, the traditional media sphere, and the Internet and the online public sphere. By examining these dimensions, the study assessed both formal regulations and practical implementations of information control, as well as their impact on public discourse and civil liberties.

The narrative review component enables the synthesis of interdisciplinary theoretical perspectives, including political theory, media studies, surveillance studies, and information ethics. The qualitative case study approach allows for contextualized analysis of specific regulatory frameworks, media structures, and digital governance mechanisms in the selected countries. The narrative review is based on a systematic search of relevant academic and policy literature. Additional sources include official government documents, constitutional texts, legislative acts, policy reports, and publications of international organizations.

Data collection relied on publicly available sources, including government reports, legal texts, and media system and coverage characteristics, which were classified according to thematic relevance. While this approach enabled detailed insights into observable patterns and trends, it is acknowledged that certain covert aspects of surveillance remain inaccessible. Furthermore, the comparative scope is limited to the two selected countries, and conclusions may not be universally applicable.

Overall, this methodology allows for a nuanced understanding of how information functions as a primary resource in contemporary networked societies – and its impact on citizens – and how it can simultaneously serve as a framework for improvement of contemporary living, but also as a mechanism of social control.

Results with Discussion

USA Case: ICS within the Contemporary Public Sphere

The USA allocates substantial funds for the protection of information-communication networks, with emphasis on safeguarding telecommunications infrastructure, which closely follows the development of the internet. In the context of online communication, the surveillance system in the USA is therefore “on an impressively high level” (Deibert, 2008: 232).

It is important to draw attention to the fact that ICANN is tied to the USA through several substantive elements (mechanisms, membership, territory), so the USA has the greatest capacity for controlling communication via the internet¹⁴.

An additional important element that supports US dominance in this field is the requirement that internet service providers comply with CALEA legislation, which “enables law enforcement authorities easy access to their surveillance infrastructure” (Bloss, 2007: 219)¹⁵.

The government filters prohibited content (illegal pornography, various offensive materials, etc.) with the aim of protecting children and morality, national security, intellectual property, and computer security. “Within libraries and schools, this field is regulated in an institutional domain” (Deibert, 2008: 226). The “Patriot Act” legislation obliges third parties that maintain

¹⁴ *The Internet Corporation for Assigned Names and Numbers* (ICANN) is the leading organization in Internet governance infrastructure (IP addresses, domains, servers).

¹⁵ *The Commission on Accreditation for Law Enforcement Agencies* (CALEA) is an agency that issues accreditations with the aim of ensuring public safety through law enforcement.ri

databases on particular individuals to provide such data when needed, without a court order. This includes the identity of the person using a specific IP address, internet messages, etc. The data must be provided to state authorities in a timely manner, without any obligation to inform the person being monitored.

In the commercial sector, we can single out companies that produce specialized software for tracking and recording an individual's activities, including all websites visited and emails received. It is clear that these frameworks allow certain companies to occupy an almost monopolistic position in monitoring internet content – for example, the RIAA, which primarily deals with identifying potential piracy involving audio material. "In the event that pirated content is discovered, the provider is contacted and the internet user's service is terminated due to illegal activities" (Katyal 2003: 341)¹⁶.

An additional problem in controlling internet content is that it is burdened with a multitude of irrelevant topics that further relativize the correctness of data usage. It is therefore necessary to conduct a thorough analysis of the available information.

¹⁶ *The Recording Industry Association of America* (RIAA) is a trade organization that supports and promotes the creative and commercial vitality of music publishers in the United States. Its membership includes several hundred companies, ranging from small and medium-sized firms to global enterprises. It creates, produces, and/or distributes sound recordings. The RIAA works to protect intellectual property and the rights of artists and publishers.

Table 1. Key Characteristics of the ICS: The Case of the United States of America.

Analytical Dimension	Key Actors / Frameworks	Information Control Mechanisms	Implications for Citizens and the Public Sphere
Constitutional and legal framework	U.S. Constitution (1st, 4th, 5th, 14th Amendments); FOIA; Privacy Act; ECPA; USA PATRIOT Act	Limited constitutional privacy protections; expansion of surveillance under national security exceptions	Formal rights coexisting with extensive surveillance powers; reduced transparency
Institutional privacy safeguards	Federal agencies; judiciary	Lack of an independent data protection authority	Weak institutional oversight; limited legal remedies for citizens
Traditional media system	Major media conglomerates	Concentrated ownership; commercial and advertising pressures on editorial autonomy	Reduced media pluralism; weakening of investigative journalism
Media lobbies and entertainment industry	Motion Picture Association	Strong lobbying in copyright enforcement and digital regulation	Restrictive circulation of content; punitive approaches to digital practices
Political influence on media	Government; military and security institutions	Agenda-setting, framing, and marginalization of dissent	Alignment of dominant discourse with state interests
Online public sphere and internet governance	ICANN; ISPs; U.S.-based technology corporations	Structural dominance in internet governance and infrastructure control	Asymmetrical global communication power; limited user sovereignty
Digital surveillance and security	CALEA; intelligence and law-enforcement agencies	Large-scale data access and monitoring with limited judicial oversight	Normalization of surveillance; erosion of privacy and autonomy
Commercial surveillance and data economy	Technology firms; RIAA	Behavioral tracking; monetization and enforcement practices	Convergence of state and market surveillance; data commodification
Cognitive dimension of information control	Algorithmic platforms; mass media	Algorithmic filtering; information overload	Weakened capacity for informed and critical public judgment

Source: Authors' processing, 2025.

4.2 Russian Federation Case: *ICS within the Contemporary Public Sphere*

In Russia, the number of internet users is growing rapidly nowadays, although most usage is still concentrated in the Moscow and St Petersburg regions. All providers are obliged, in accordance with SORM – 2 regulations, to supply the Federal Security Service¹⁷ with precise data on internet traffic. Otherwise, they lose their license.

The Russian online sphere is not typically subject to classical censorship of political content, but government produced material in Russian is heavily promoted. Content filtering primarily concerns pornography, spam, and piracy, which are censored.

Government agencies do monitor internet content, but this surveillance is significantly less advanced technologically than that in the United States, mainly due to insufficient infrastructure and capacity. In this regard, the Russian Federation is allocating increasing funds to improve this sector.

It should be mentioned that the internet space is to a great extent still free, although “there is a tendency to place it under greater state control” (Deibert, 2008: 180).

By following the analysed social context and two dominant and fairly divergent interpretations of the meaning of information, this study has demonstrated that one perspective sees information as an attempt to represent reality, which, when accurate, becomes truth, while the other suggests that information itself can produce reality, shaping the perception of truth.

More concretely, those who control information control the production of reality. At the same time, both perspectives confirm the central role of information as a resource in contemporary society, but also remain incomplete, as “increased connectivity has not necessarily led to greater truthfulness or rationality” (Harari, 2024: 55).

The functioning matrix of the ICS shapes global patterns of human behavior through the combined effects of modern surveillance technologies and targeted media activities. Namely, information and communication technologies (ICTs) play a dual role: they facilitate positive outcomes, such as crime prevention and rapid public administration, but their ubiquity and invisibility also pose risks to fundamental human rights and freedoms.

¹⁷ *The Federal Security Service* (Russian: *Федеральная служба безопасности Российской Федерации*, ФСБ РФ) is the federal executive authority of Russia, an intelligence service that performs tasks related to maintaining the security of the Russian Federation.

Table 2. Key characteristics of the ICS: The case of the Russian Federation.

Analytical Dimension	Key Actors / Frameworks	Information Control Mechanisms	Implications for Citizens and the Public Sphere
Constitutional and legal framework	Constitution of the Russian Federation; data and information laws	Formal privacy guarantees combined with broad statutory exceptions	Legal protection of privacy accompanied by extensive state discretion
Surveillance legislation and enforcement	SORM system; Federal Security Service (FSB)	Mandatory interception infrastructure; provider access obligations with limited judicial oversight	Systematic monitoring of communications; low transparency
State doctrine and information security	Information Security Doctrine	Centralized monitoring and regulation of information flows	State stability prioritized over individual informational autonomy
Traditional broadcast media	State authorities; national television networks	Direct and indirect state ownership and control	Dominance of pro-government narratives; restricted pluralism
Media ownership and consolidation	State-controlled media structures	Elimination of independent ownership; consolidation under state supervision	Reduced editorial autonomy; political alignment of media content
Journalistic practice and press freedom	Journalists; print and radio outlets	Self-censorship; weak institutional protection	Chilling effects on investigative and watchdog journalism
Online media development	Internet portals; digital platforms	Expansion of digital communication under delayed and uneven access	Conditional space for alternative and critical discourse
Online public sphere and infrastructure	ISPs; FSB	Mandatory traffic data retention and disclosure	Institutionalized monitoring of online communication
Content regulation and agenda-setting	State regulatory bodies	Selective filtering and prioritization of state-aligned content	Managed visibility of narratives; limited political pluralism
Technological capacity of surveillance	State security services	Less advanced but expanding surveillance capabilities	Partial effectiveness of control with increasing reach
Trajectory of information control	Russian state institutions	Gradual expansion of internet regulation and centralization	Increasing state dominance over the digital public sphere

Source: Authors' processing, 2025.

Furthermore, this matrix demonstrates a shift from local to global focus, with power increasingly residing not only in state institutions but also in multinational corporations and digital platforms.

Table 3. Level of development of the ICS: USA and Russian Federation.

Analytical Dimension	United States	Russian Federation
Constitutional basis	Indirect constitutional protection of privacy and expression	Explicit constitutional regulation of privacy and data protection
Surveillance legislation	ECPA; CALEA; USA PATRIOT Act	SORM system; data and information laws
Judicial oversight	Broad surveillance powers with limited transparency	Formal court authorization, frequently bypassed
Institutional privacy safeguards	No independent national data protection authority	Centralized security-based oversight; no independent authority
Dominant model of information control	Hybrid state-market model	State-centered model
Primary locus of control	Market power, advertising, and political influence	Political authority and security apparatus
Media ownership structure	Concentrated private media conglomerates	Direct and indirect state control of broadcast media
Television sector	Commercial dominance with political influence	Centralized and state-controlled
Print and radio media	Formally free, economically constrained	Limited pluralism under self-censorship
Media elites and lobbying	Strong corporate lobbies and media magnates	Marginalized oligarchic influence; state dominance
Online public sphere	Globally dominant, technologically advanced	Expanding under increasing state oversight
Internet governance	Structural dominance via platforms and ICANN	National regulation and provider obligations
Content regulation	Surveillance-based control with selective filtering	Agenda-setting with limited political censorship
Surveillance capacity	Highly developed and comprehensive	Less advanced but rapidly expanding
Impact on citizens	Normalized surveillance and data commodification	Restricted pluralism with conditional online freedom
Overall trajectory	Expansion of algorithmic and market-based control	Intensification of centralized state control

Source: Authors' processing, 2025.

Comparative analysis of the USA and Russia highlights both similarities and differences.

In the USA, ICT infrastructure is highly developed, and surveillance is exercised both by the state, under legal regulation for national security, and by private actors seeking profit. The media landscape is dominated by corporate capital, while internet communication is subject to regulation, especially after the events of September 11, 2001.

In Russia, ICT infrastructure is less advanced, yet electronic surveillance occurs and produces significant social control effects. Particularly television remains largely state-controlled, while print media are somewhat freer but constrained by self-censorship. Internet development is still nascent, though investment in digital spaces is increasing.

Both cases demonstrate that technological capacity alone does not determine the extent of social control, because political, institutional, and societal factors act synergistically to shape outcomes.

Conclusion

This study has examined the emergence of an ICS, comparing the United States of America and the Russian Federation, with a focus on the legal framework, traditional media, and the online public sphere. By analyzing these dimensions, the paper aimed to understand how information flows shape social control, influence citizen behavior, and redefine the power dynamics among states, corporations, and the global network society.

Its ambition it to conceptualize the notion of the information-controlled society (ICS) and to comparatively analyze its manifestations in the United States of America and the Russian Federation, with particular emphasis on legal regulation, traditional media systems, and the online public sphere.

The analysis demonstrates that both cases exhibit structured systems of information control, though organized through different institutional logics. In the United States, information control operates predominantly through a hybrid state–market model characterized by advanced technological infrastructure, corporate concentration in the media sector, and extensive data-driven surveillance practices. In the Russian Federation, information control is primarily centralized within state institutions, with direct political influence over broadcast media and expanding regulatory oversight of digital communication.

Despite these structural differences, the comparative findings reveal functional convergence. In both contexts, information increasingly serves as a mechanism of governance, surveillance capacities are expanding, and asymmetries in access to communication infrastructures shape public discourse. The study therefore confirms that contemporary systems of information control cannot be adequately understood through a simple democratic–authoritarian dichotomy. Instead, they represent distinct yet comparable configurations of informational power embedded within networked societies.

By demonstrating these convergences and divergences, this paper contributes to a more precise understanding of how information functions as a central resource of power in contemporary digital environments and how its control reshapes the relationship between

institutions, media systems, and citizens. Aligning TT development with privacy protection, promoting civic engagement, and fostering critical understanding of information's role in shaping reality are, therefore, essential for securing a safer, more equitable, and sustainable future for citizens worldwide.

References

1. Arendt, H. (1998). *Izvori totalitarizma (Sources of totalitarianism)*. Belgrade: Feministička izdavačka kuća. In Serbian
2. Bagdikian, B. H. (2000). *The Media Monopoly*. 6th ed. Boston: Beacon Press.
3. Beniger, J. (1986). *The Control Revolution*. USA: President and Fellows of Harvard College.
4. Bloss, Wi. (2007). Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects. *Surveillance & Society*, 4(3), 208–228. <https://doi.org/10.24908/ss.v4i3.3448>.
5. Bloustein, E. J. (1984). Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology*. (pp. 156–202). Cambridge: Cambridge University Press.
6. Burton, G. (2005). *Media and Society: Critical Perspectives*. Berkshire: Open University Press/McGraw-Hill House.
7. Castells, M. (2024). *Advanced Introduction to Digital Society*. Cheltenham: Edward Elgar Publishing.
8. Castells, M. (2018a). *Uspon umreženog društva (The rise of the networked society)*. Belgrade: Službeni glasnik. In Serbian
9. Castells, M. (2018b). *Mreže revolta i nade (Networks of revolt and hope)*. Belgrade: Službeni glasnik. In Serbian
10. Clarke, R. (1997). *Promises and Threats in Electronic Commerce*. Rogerclarke.com. Accessed 1 January 2025. <http://www.rogerclarke.com/DV/PaperAuthism.html>.
11. Clarke, R. (2001). *While You Were Sleeping ... Surveillance Technologies Arrived*. Rogerclarke.com. Accessed 5 January 2025 at the: <http://www.rogerclarke.com/DV/AQ2001.html>.
12. Committee on Privacy. (2007). *Engaging Privacy and Information Technology in a Digital Age*, edited by J. Waldo et al. Washington, D.C.: National Academies Press.
13. Deibert, R. (2008). Regional Overviews. In R. Deibert et al. (Eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (pp. 151–432). Cambridge: MIT Press.
14. European Commission (n.d). *The Digital Services Act package*. Europa.eu. Accessed 3 April 2025. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.
15. Feenberg, A. (1999). *Questioning Technology*. London: Routledge.
16. Forbes (n.d). *Rupert Murdoch & Family*. Forbes.com. <https://www.forbes.com/profile/rupert-murdoch/>. Accessed 12 January 2025.
17. Floridi, L. (2005). Is Semantic Information Meaningful Data?. *Philosophy and Phenomenological Research*, 70(2), 351–370. <https://doi.org/10.1111/j.1933-1592.2005.tb00531.x>

- Lunić, T., & Penezić, S. (2026). Information-controlled society and role of the media: A study of the USA and the Russian Federation, *Sport media and business*, 12(2), 120-143
-
18. GDPR. n.d. *What is GDPR, the EU's New Data Protection Law?*. Gdpr.eu. <https://gdpr.eu/what-is-gdpr/>. Accessed 2 April 2025.
 19. Harari, Y. N. (2024). *Neksus (Nexus)*. Belgrade. Laguna. In Serbian
 20. Heidegger, M. (1977). *The Question Concerning Technology and Other Essays*. New York & London: Garland Publishing.
 21. Holtzman, H. D. (2006). *Privacy Lost: How Technology Is Endangering Your Privacy*. San Francisco: Jossey – Bass.
 22. Katyal, S. K. (2003). The New Surveillance. *Case Western Reserve Law Review*, 54(2), 297–385. Retrieved 4 April 2025 at: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1335&context=faculty_scholarship
 23. Levinson, P. (2004). *Digital McLuhan: A Guide to the Information Millennium*. USA: Routledge/Taylor & Francis.
 24. Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
 25. McLuhan, M. (2005). *Understanding Media: The Extensions of Man*. London & New York: Routledge/Taylor & Francis.
 26. Mickiewicz, E. (2008). *Television, Power, and the Public in Russia*. Cambridge: Cambridge University Press.
 27. Mladenović, N. (2025). *Medijatzacija: Krovni pojam medijskih studija?* (Mediatization: The umbrella term of media studies?). Belgrade: Faculty of Sport, Union University - Nikola Tesla. In Serbian
 28. Penezić, S. & Vasiljević, J. (2022). Socijalna getoizacija kao tačka preseka savremenih veza arhitekture i komunikacije (Social ghettoization as a point of intersection of modern connections of architecture and communication). *Politički život*, 23(2), 111–129. https://doi.org/10.18485/fpn_pz.2022.23.7. In Serbian
 29. Peterson, B, & Pang, J. (2006). Beyond Politics: Authoritarianism and the Pursuit of Leisure. *The Journal of Social Psychology*, 146(4), 443–461. <https://doi.org/10.3200/SOCP.146.4.443> – 461.
 30. Prosser, W. L. (1984). Privacy (A Legal Analysis). In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology*1. (pp. 104–155). Cambridge: Cambridge University Press.
 31. Shannon, C E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27(3), 379–423. <https://doi.org/10.1002/j.1538-7305.1948.tb01338.x>.
 32. Shauer, T. (2003). *The Sustainable Information Society: Vision and Risks*. Ulm: Universitätsverlag.
 33. Stiglitz, J. (2018). *Globalizacija i njene protivrečnosti (Globalization and its contradictions)*. Belgrade: Miba Books. In Serbian
 34. Subotić, O. (2011). *Informaciono kontrolisano društvo (Information controlled society)*. Stari Banovci, Belgrade: Finegraf. In Serbian

Lunić, T., & Penezić, S. (2026). Information-controlled society and role of the media: A study of the USA and the Russian Federation, *Sport media and business*, 12(2), 120-143

35. Tunstall, J. & Palmer, M. (2001). *Media Moguls*. London: Routledge/Taylor & Francis.
36. The Ministry of Foreign Affairs of the Russian Federation (3 July 2000). *The Constitution of the Russian Federation*. https://mid.ru/en/foreign_policy/fundamental_documents/1750525/. Accessed 8 January 2025.
37. The Royal Academy of Engineering. (2007). *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*. London: The Royal Academy of Engineering.
38. U.S. Senate (n.d.). *The Constitution of the United States of America*. https://www.senate.gov/civics/resources/pdf/US_Constitution-Senate_Publication_103-21.pdf. Accessed 8 January 2025.
39. Varoufakis, Y. (2025). *Tehnofeudalizam (Technofeudalism)*. Belgrade: Publik Praktikum. In Serbian
40. Warren, S. D., & Brandeis, L.D. (1984). The Right to Privacy (The Implicit Made Explicit). In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 75–103). Cambridge: Cambridge University Press.
41. Zassoursky, I. (2009). Free to Get Rich and Fool Around. In B. Beumers et al. (Eds.), *Post-Soviet Russian Media: Conflicting Signals* (pp 29–41). Routledge/Taylor & Francis.
42. Penezić, S. (2022). Nove tehnologije, novi narativi i novi potrošači (New technologies, new narratives and new consumers). *Kultura*, 176(4), 5–9. <https://www.casopiskultura.rs/wp-content/uploads/2023/05/0-%D0%A3%D0%B2%D0%BE%D0%B4.pdf>