

Digital Constitutionalism in Creating a New Constitutional Equilibrium^(*)

Yeni Bir Anayasal Denge Oluřturmada Dijital Anayasacılık

İlyas Fırat CENGİZ^(**)

Abstract:

Digital technologies have reshaped society towards an online. The Internet is an essential launching pad for implementing and promoting human rights. Yet, digital technologies also create some conflicts with respect for human rights, such as the increase of digital surveillance infrastructures, dissemination of hate speech, cyberbullying, cyber terrorism and the growing spread of disinformation. Digital technology makes some changes in the constitutional ecosystem. Constitutional equilibrium relies on two essential functions of constitutional law: protecting fundamental rights and balancing powers. Technological advancements adopt their nature into a constitutional ecosystem, creating a new equilibrium between constitutional institutions/human rights and digital technology. They increase the potential for information transmission yet heighten the risk of threats to fundamental rights due to information exchange. The significant role of private companies in the digital realm increases the likelihood of human rights abuses by non-state actors. Therefore, how do constitutions in the digital age work with global digital companies? The dominant role of private companies is to limit arbitrary power and protect fundamental rights. Digital constitutionalism deals with constitutional challenges with the principles of the rule of law, legitimacy-representation, and remedies. The international human rights law system considers digital technology a drastic component of constitutionalism, which requires states to regulate digital technology on both counts of supporting and hindering human rights.

Keywords:

Digital Constitutionalism, Constitutional Equilibrium, Human Rights, Constitutional Powers, and Digital Companies.

^(*) Arařtırma Makalesi / *Research Article*
Yayın Kuruluna Ulařtıđı Tarihi: 26.11.2024
Yayınlanmasının Kabul Edildiđi Tarihi: 29.01.2025
DOI: <https://doi.org/10.58733/imhfd.1591701>

Bu makaleye atf için: CENGİZ, İlyas Fırat, "Digital Constitutionalism in Creating a New Constitutional Equilibrium", *İMİHFD*, C. 10, S. 1, 2025, s. 69-92

^(**) *Dr. Öğr. Üyesi*, Yalova Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, Yalova - Türkiye
E-posta: ilyas.cengiz@yalova.edu.tr
Orcid: <https://orcid.org/0000-0001-5367-8112>

Öz:

Dijital teknolojiler toplumu çevrimiçi bir topluma doğru yeniden şekillendirmektedir. İnternet, insan haklarının uygulanması ve teşviki için olmazsa olmaz bir hal almıştır. Ancak dijital teknolojiler, dijital gözetim altyapılarının artması, nefret söyleminin yaygınlaşması, siber zorbalık, siber terörizm ve dezenformasyonun giderek yaygınlaşması gibi insan haklarına saygıyla ilgili bazı zorlukları beraberinde getirmektedir. Gelişen dijital teknolojiler anayasal ekosistemde bazı değişimlere ve dönüşümlere neden olmaktadır. Anayasal denge temel hakların korunması ve güçler dengesi gibi anayasa hukukunun iki temel işlevine dayanmaktadır. Dijital teknolojiler anayasal ekosistemin bir parçası haline gelerek anayasal kurumlar ve insan hakları ile yeni bir denge oluşturmak durumunda kalmaktadır. Dijital teknolojiler bilginin iletim potansiyelini artırırken, aynı zamanda bilgi alışverişi nedeniyle temel haklara yönelik bazı riskleri ortaya çıkarmakta veya artırmaktadır. Özel şirketlerin dijital alanda oynadığı önemli rol nedeniyle, devlet dışı aktörler tarafından insan hakları ihlallerinin gerçekleşme olasılığını artırmaktadır. Dolayısıyla dijital çağda anayasaların küresel dijital şirketlerle nasıl işlediği, özel şirketlerin baskın rolü, keyfi gücün sınırlandırılması ve temel hakların nasıl korunacağı gibi hususlar önem arz etmektedir. Dijital anayasacılık, anayasal sorunlarla hukukun üstünlüğü, meşruiyet-temsil ve yasal yollar/düzeltilme yolları gibi ilkeleri kullanarak başa çıkabilir. Uluslararası insan hakları hukuku sistemi, dijital teknolojiyi anayasacılığın temel bir bileşeni olarak görmek durumundadır ve devletlerin dijital teknolojiyi hem insan haklarını desteklemesi hem de engellemesi açısından düzenlenmesi gerektirmektedir.

Anahtar Kelimeler:

Dijital Anayasacılık, Anayasal Denge, İnsan Hakları, Anayasal Erkler, ve Dijital Şirketler.

INTRODUCTION

Global access to the internet has been a new phenomenon since the 1990s, creating enormous digital space as a gateway for information and communication. Digital technologies have reshaped society towards an online. This process reshapes the domains of enacted rights and powers, leading to constitutional challenges. Online digital content has surged, making it easily accessible, consultable, and shareable through Information and Communication Technologies (ICTs). The modern world has become surprisingly wide due to these developments. The impacts of ICTs on the information and communication environments provide the advent of many-to-many communication systems, which differ from traditional media's "one-to-many" communication system¹. Hereafter, the international system has developed around the expansion and dissemination of ICTs.

The internet is an essential launching pad for implementing and promoting human rights. Individuals enjoy the full range of online rights (such as privacy,

¹ AMBLE John Curtis, "Combating Terrorism in the New Media Environment", *Studies in Conflict & Terrorism*, Y. 2012, V. 35(5), p. 339-353, p. 340.

‘thought, conscience and religion’, association and peaceful assembly, education, culture and freedom from discrimination). Yet, digital technologies may also create conflicts with human rights, such as the increase of digital surveillance infrastructures, dissemination of hate speech, cyberbullying and the growing spread of disinformation. Governments have justified disrupting internet access through the arbitrary use of digital technologies. Legal interferences then cause profound adverse impacts on the freedom of expression and the enjoyment of economic, social, and cultural rights.

The core principles behind the rise of the constitutional system are to limit state power, create a separation of powers, oversee the application of fundamental rights and freedoms, emphasise national sovereignty via elections, and promote participation in governance through political engagement. Digital technology makes some changes in the constitutional ecosystem. Constitutional equilibrium relies on essential functions of constitutional law: 1) limiting power, 2) the protection of fundamental rights and 3) the balancing of powers². For instance, digital technology expands the possibility of transmitting information, implying that all fundamental rights are based on freedom of expression, religion, assembly, and business conduct³. Yet, digital technology amplifies the risk of threats to fundamental rights due to the exchange of information⁴. The rise of digital technology tools among individuals, coupled with the predominant influence of private companies in the digital space, heightens the risk of human rights violations by non-state actors⁵. This disrupts existing power-balancing mechanisms focusing on relations between individuals and nation-states⁶.

Technology grinds its nature into a constitutional ecosystem, creating a new equilibrium between constitutional institutions/human rights and digital technology. The exercise of powers emerging from the digitalisation of society relies on online speech and ICT platforms governance, which encompasses other rights beyond freedom of expression, such as data protection, non-

² See, PETERS, Anne, “Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures”, *Leiden Journal of International Law*, Y. 2006, V. 19(3), p. 579-610, p. 579.

³ CELESTE, Edoardo, **Digital constitutionalism: Mapping the Constitutional Response to Digital Technology’s Challenges**, HIIG Discussion Paper Series 2018-02, p. 4. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3219905, A.D. 10.10.2024.

⁴ CELESTE, Edoardo, “Digital Constitutionalism: A New Systematic Theorisation”, *International Review of Law, Computers & Technology*, Y. 2009, V. 33(1), p. 76-99, p. 79.

⁵ CELESTE, **Digital constitutionalism: Mapping...**, p. 4.

⁶ CELESTE, **Digital constitutionalism: Mapping...**, p. 4.

discrimination, property, security, or access to the internet, etc. Therefore, how constitutions in the digital age work with global ICT platforms, the dominant role of private companies, limiting arbitrary power and protecting fundamental rights. Digital constitutionalism is analysed to seek answers to these questions, with the principles of the rule of law, legitimacy-representation, and remedies. The international human rights law system considers digital technology as a drastic component of constitutionalism. This system is evaluated with consideration of its progressive reflection on digital technologies.

I. DIGITAL TECHNOLOGY WITHIN CONSTITUTIONALISM

The digital revolution was achieved in the next wave after the industrial revolution in the 1980s. Technological “revolutions are rapidly transforming economic, social and personal domains, now and even more so in the imminent future”⁷. ICT is a product of progress and developments in computer science and telecommunication technology. ICTs are all forms of tools, techniques, and technology to transmit, store, process, and disseminate information⁸. This technology combines equipment and procedures to “facilitate the acquisition, creation, retrieval, storage, searching, viewing, updating and transmission of information using electronic means”, making communication more efficient, reliable, cost-effective and increasing coverage⁹. ICTs have enhanced the processes of data collection, analysis, and processing, shaping human opinions and thinking¹⁰. Today, ICTs have become the most critical tools for education, employment, commerce, health care, civic participation, entertainment, and more, creating an information society¹¹. The web is a vital tool that enables individuals to communicate, interact, and access information in society¹². The vital component of the digital revolution is artificial intelligence (AI), which is a machine or computer program that thinks and learns. Here, machine learning is the general name of the algorithms that a machine or computer program creates by model-

⁷ ROCO, Mihail C. / BAINBRIDGE, William Sims, **Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science**, Kluwer Academic Publishers, 2003.

⁸ SHARMA, Dhiraj, **Communication in IT Age**, Himalaya Pub. House, Mumbai, 2020, p. 133.

⁹ SHARMA, p. 133.

¹⁰ SHARMA, p. 136.

¹¹ BREWER, Judy, “Standards Bodies, Access to Information Technology, and Human Rights”, **Disability, Human Rights, and Information Technology**, (Eds) Lazar Jonathan, and Stein Michael Ashley, University of Pennsylvania Press, 2017, p. 13.

¹² BREWER, p. 13.

ling a given problem according to the data it obtains from the environment related to the problem¹³. AI makes the digital revolution a more complex and unpredictable phenomenon in terms of constitutionalism.

ICTs have created a new status-quo and challenges for global governance. This created an enigma in regulating economic, cultural, legal, and political relations at all stages of relationships¹⁴. The internet has a global nature, which has made it difficult for national authorities to legislate cyberspace. The world's political momentums, such as the 'Global War on Terrorism', 9/11¹⁵ and 7/7¹⁶, were the main reasons that ICTs must be regulated for security reasons¹⁷. Since the war on terror relocated to the digital world as a new battlefield, the complex and dialectic relationship between law and technology is a new phenomenon¹⁸. In the normative context, these two are not rivals, and the law must be adequately revised in the digital world¹⁹. Indeed, the law is mainly challenged by and often lags behind new technologies²⁰. The capacity of legal institutions to adapt to changing technologies is slowing down²¹. The laws created before the internet are frequently referenced to resolve disputes regarding the use of ICTs and must adapt to the challenges posed by emerging technologies²².

¹³ ATALAY, Muhammet / ÇELİK, Enes, "Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları", Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Y. 2017, V. 9(22), p. 155-172, p. 161.

¹⁴ CONWAY, Maura, "Terrorist Use of the Internet and the Challenges of Governing Cyberspace", **Power and Security in the Information Age: Investigating the Role of the State in Cyberspace**, (Eds.) Dunn Myriam, Victor Mauer, & Felisha Krishna-Hensel, Ashgate, London, 2007, p. 308.

¹⁵ The September 11 attacks, commonly known as 9/11, were four coordinated suicide attacks and carried out by al-Qaeda against the United States in 2001.

¹⁶ The 7 July 2005 London bombings, also referred to as 7/7, were a series of four coordinated suicide attacks that targeted commuters travelling on London's public transport during the morning rush hour.

¹⁷ CLIVE, Walker / CONWAY, Maura, "Online terrorism and online laws", **Dynamics of Asymmetric Conflict**, Y. 2015, V. 8(2), p. 156-175, p. 159.

¹⁸ GOLUBIC, Martin Charles, **Fighting Terror Online the Convergence of Security, Technology, and the Law**, Springer, 2008, p. 10.

¹⁹ ELKIN-KOREN, Niva, "Making Technology Visible: Liability of Intent Service Providers for Peer-to-Peer Traffic", **Journal of Legislation and Public Policy**, Y. 2006, V. 9(15), p. 15-74, p. 16-17.

²⁰ GOLUBIC, 2008, p. 10; MOSES Lyria Bennett, "Recurring dilemmas: The law's race to keep up with Technological Change", **University of Illinois Journal of Law, Technology & Policy**, Y. 2007, V. 21, p. 239-285.

²¹ MARCHANT, Gary E., "The Growing Gap Between Emerging Technologies and the Law", **The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight**, (Eds) Gary E. Marchant, Braden R. Allenby, Joseph R. Herker, Springer, 2011, p. 23.

²² GOLUBIC, p. 11.

The digital revolution created a major transformation in fundamental rights and freedoms²³. Indeed, certain countries now recognise Internet access as a distinct right, granting it independent status²⁴. Digital technology is an ecosystem playing a central role in determining the extent of our fundamental freedoms. The ‘digital rights’ should also be included in the bundle of constitutional rights. These rights can be listed as providing the right to internet access, protection of personal data, the right to be forgotten, public monopoly of all kinds of data belonging to the state, digital public order, the right to digital participation, and the right not to use the internet²⁵. These examples can be multiplied and associated with online safety, digital citizenship, the role of Artificial Intelligence, the Internet of Things, and education Technologies. The primary purpose of digital rights should be to eliminate threats from the digital environment and ensure the healthy existence of society and the state²⁶. This also affects the constitutional ecosystem, protecting fundamental rights and regulating the exercise of power in contemporary constitutionalism²⁷. Digital technology creates disorder in the constitutional ecosystem and disrupts constitutional stability²⁸. Digital technology generates four effects: (1) “reinforces the power of states to control our digital lives;” (2) “promotes powerful tech multinationals to the level of dominant actors by allowing them to shape our digital selves;” (3) “enhances a broad range of fundamental rights based on the exchange of information;” and (4) “at the same time, increases the risk of violations of several individual rights.”²⁹. Consequently, digital technology initiates a multilevel process of constitutionalisation, which extends from adopting traditional constitutional instruments to more innovative tools that emerge even beyond the realm of the state³⁰. Thus, digital constitutionalism essentially appears as a response seeking better protection of fundamental rights, freedoms and public values in

²³ KAMA IŞIK, Sezen, “Klasik Anayasacılıktan Dijital Anayasacılığa: Anayasa Hukukunun Dönüşümü”, **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı**, Adalet Yayınevi, Ankara, 2021, p. 42.

²⁴ KAMA IŞIK, p. 44.

²⁵ ÇATLI, Mehmet, “Yapay Zekânın Anayasası: “Akıllı Anayasa” Üzerine”, **Adalet Dergisi**, Y. 2023/1, V. 70, p. 369-383, p. 373-4.

²⁶ ÇATLI, p. 373.

²⁷ CELESTE, Edoardo, **Digital Constitutionalism: The Role of Internet Bills of Rights**, Routledge, 2023, p. 92.

²⁸ CELESTE, **Digital Constitutionalism: The Role...**, p. 25.

²⁹ CELESTE, **Digital Constitutionalism: The Role...**, p. 25.

³⁰ CELESTE, **Digital Constitutionalism: The Role...**, p. 92-93.

the digital age³¹. This concept aims to protect fundamental rights and freedoms and appropriately limit the power of private corporations gaining increasing power due to these technologies³². In this new technological framework, private companies operating in the digital environment fulfil semi-public functions and compete with public actors in a transnational context³³. As transnational corporations develop, state power is weakening³⁴. The state cannot protect itself against the consequences of decisions taken by these actors that have roots outside its borders³⁵.

The widespread availability of digital technology among individuals and the significant influence of private companies in the digital landscape heighten the risk of human rights violations by non-state actors^{36,37}. The fundamental challenge facing constitutional democracies in the algorithmic society no longer comes solely from public authorities but mainly from the fact that they are formally private actors³⁸. As Suzor observes, '*digital constitutionalism requires us to develop new ways of limiting abuses of power in a complex system that includes many different governments, businesses, and civil society organisations*'³⁹. This disrupts existing power-balancing mechanisms focusing on relations between individuals and nation-states⁴⁰. The international nature of the Internet has posed challenges to the traditional concepts of modern constitutionalism. New information and communication settings have questioned consolidated notions such as sovereignty and power⁴¹ and enhanced the exercise of

³¹ KAMA IŞIK, p. 49.

³² KAMA IŞIK, p. 52.

³³ DE GREGORIO, Giovanni, "The Rise of Digital Constitutionalism in the European Union", **International Journal of Constitutional Law**, Y. 2021, V. 19(1), p. 41-70, p. 41-42.

³⁴ AKAD, Mehmet, / VURAL DİNÇKOL, Bihterin / BULUT, Nihat, **Genel Kamu Hukuku**, Der Yayınları, 2021, p. 218.

³⁵ AKAD / VURAL DİNÇKOL / BULUT, p. 217.

³⁶ Non-state actors are entities and individuals that frequently wield considerable political power and territorial control, operating independently of any sovereign government in terms of direction, affiliation, or funding. Non-state actors (NSAs) usually encompass corporations, private financial institutions, non-governmental organisations (NGOs), paramilitary groups, armed guerrilla resistance groups, and terrorist organisations, all of which may resort to violence to achieve their objectives.

³⁷ CELESTE, **Digital constitutionalism: Mapping...**, p. 4.

³⁸ DE GREGORIO, Giovanni, "Digital Constitutionalism across the Atlantic", **Global Constitutionalism**, Y. 2022, V. 11(2), p. 297-324, p. 303-304.

³⁹ SUZOR, Nicolas, **Lawless: The Secret Rules That Govern Our Digital Lives**, Cambridge University Press, 2019, p. 173.

⁴⁰ CELESTE, **Digital constitutionalism: Mapping...**, p. 4.

⁴¹ SASSEN Saskia, "On the Internet and Sovereignty", **Indiana Journal of Global Legal Studies**, Y. 1998, V. 5(2), p. 545-559.

fundamental rights and freedoms⁴². For instance, digital technology enhances the ability to transmit information, indicating that all fundamental rights rely on exchanging information, including freedom of expression, religion, assembly, and the freedom to conduct business⁴³. Yet, digital technology increases the risk of threats to fundamental rights due to information exchange. Disinformation, defamation, hate speech, cyberbullying, cyber-terrorism, and child pornography such risks can be apparent when freedom of expression is abused illegally through digital instruments⁴⁴.

II. CONSTITUTIONAL EQUILIBRIUM BY DIGITAL CONSTITUTIONALISM

Cyberspace remained a largely unregulated jurisdictional outpost in the 2000s⁴⁵. For instance, artificial intelligence cannot be adequately regulated and is the world's largest unmanaged area⁴⁶. The trend towards introducing regulations on digital technologies should be viewed within the normative boundaries of constitutional and human rights perspectives⁴⁷. Even though such regulations have extraordinary features due to technological reasons, these laws must be compatible with the general theory of the state and international human rights law. Whether the nation-state is melting down, disappearing, or the concept of sovereignty is entirely over is controversial⁴⁸. Therefore, it is difficult to say that globalisation has rendered the state ineffective. Technology has even increased the state's capacity to monitor and control its citizens⁴⁹.

The Constitution aims to establish a system of limitations on political powers and guarantee individuals' freedom from interference by public authorities⁵⁰. The Constitution safeguards citizens' essential rights and liberties against the state; it serves to restrict authority, not essential rights and freedoms⁵¹. However,

⁴² BALKIN, Jack, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", *New York University Law Review*, Y. 2004, V. 79(1), p. 1-55.

⁴³ CELESTE, *Digital constitutionalism: Mapping...*, p. 4.

⁴⁴ CELESTE, *Digital constitutionalism: Mapping...*, p. 4.

⁴⁵ FRASER, Sampson, "Cyberspace: the New Frontier for Policing", *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Eds, Akhgar Babak, Staniforth Andrew, and Bosco Francesca, Elsevier, 2014, p. 1.

⁴⁶ ZUHOFF Shoshana, *The Age of Surveillance Capitalism*, Profile Books, Londra, 2019, p. 103.

⁴⁷ WALKER / CONWAY, p. 159.

⁴⁸ AKAD / VURAL DİNÇKOL / BULUT, p. 225.

⁴⁹ AKAD / VURAL DİNÇKOL / BULUT, p. 229.

⁵⁰ SAJÓ, András / UITZ, Renáta, *The Constitution of Freedom: An Introduction to Legal Constitutionalism*, Oxford Academic, 2017, p. 23.

⁵¹ GÖZLER Kemal, *Anayasa Hukukunun Genel Esasları*, Ekin Basım Yayın, 2024, p. 70.

this mission has traditionally focused on limiting public authorities. Modern constitutionalism aims to protect fundamental rights and limit the emergence of powers beyond control. Yet, the expression ‘digital constitutionalism’ refers to two dimensions⁵². The first concerns the focus on digital technologies (a specific time frame of the advent of the Internet). The second dimension is a constitutional theory that views powers as the exclusive expression of public authority. At the same time, rights and freedoms serve as safeguards against the discretionary exercise of these powers. Combining these two dimensions offers insight into how digital technologies and constitutional law influence one another. Digital constitutionalism establishes a new theoretical and practical field that explores the dynamic relationship between constitutionalism and technology⁵³. It illustrates how constitutional law responds to the power exerted by public and private actors in the digital age. This also leads to a normative approach that reframes protecting fundamental rights and exercising powers within the algorithmic society⁵⁴.

The digital revolution with algorithms influences the scope of constitutional rights, yet the misuse of algorithms leads to serious consequences for protecting human rights⁵⁵. IA alters the concept of human rights while creating new ones in constitutions, such as the right to autonomy, choice and oversight, or demand transparency and explainability of artificial intelligence outputs⁵⁶. A key aspect of states’ digital transformation initiatives is delivering services by public administrations in a digital setting. Yet, the main discussion revolves around how the possible opportunities and problems that arise with AI in the law-making process affect constitutions’ implementation and amendment processes⁵⁷. AI presents opportunities (fast and transparent auditing, fast and problem-free alteration, ease of digital consensus, and more participatory democracy) and problems (biases and disagreements arise due to superficial information, weakening constitutional values, the idea that living together is limited to digital

⁵² DE GREGORIO, p. 303.

⁵³ DE GREGORIO, p. 303.

⁵⁴ DE GREGORIO, p. 303.

⁵⁵ BEDUSCHİ, Ana, Human Rights and the Governance of Artificial Intelligence, (2020), (Online), <https://www.geneva-academy.ch/research/publications/detail/513-human-rights-and-the-governance-of-artificial-intelligence>, A.D. 18.01.2025.

⁵⁶ MULLER, Catelijne, The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law, Ad Hoc Committee on Artificial Intelligence (Cahai), (2020), (Online), <https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da>, A.D. 18.01.2025.

⁵⁷ ÇATLI, p. 378.

environments only, the formation of a mechanical constitution, and the erosion of the perception of the state) regarding the process of making and implementing constitutions⁵⁸. Constitutional alterations are regarded as mechanisms to address the damages caused by AI, such as mass surveillance, indiscriminate facial recognition, and other forms of biometric identification.

The digital revolution must be subject to constitutional regulations as a factor transforming constitutionalism, so there should be a two-way interaction. Digital constitutionalism must rely on a normative perspective that proposes ways to protect fundamental rights and limit powers in the digital age⁵⁹. Digital constitutionalism proposes a normative understanding that ensures the rule(s) of law, legitimacy-representation and remedies to set a constitutional equilibrium considering the digital revolution⁶⁰.

A. Rule of Law

The rule of law is a crucial reason for online laws to regulate digital technology. Human conduct within society may cause disputes even in the cyber world. There is no absolute freedom within society, so restrictions might be necessary. The actual issue here is who will make the regulation and who will set the limits comes to the fore⁶¹. According to the fundamental rule that has long been accepted and established in a democratic state governed by the rule of law, only the legislative body, through law, restricts freedoms⁶².

In the digital age, hierarchy rules and the separation of public and private are unclear; consequently, in digital constitutionalism, the rule of law frequently aims to limit specific powers of both public and private entities⁶³. Some questions can be asked concerning the rules of law, such as: what distinguishes rules as “digitally constitutional” in a transnational setting occupied by public, private, or global normative orders? Who creates the rules as law? Does any rule affecting the digital realm instantly become “digital constitutionalism”?⁶⁴ To

⁵⁸ ÇATLI, p. 380.

⁵⁹ DUARTE Francisco de Abreu / DE GREGORIA Giovanni / GOLIA Angelo Jr, “Perspectives on Digital Constitutionalism”, **Research Handbook on Law and Technology**, Eds. Bartosz Brozek, Olia Kanevskaia, and Przemyslaw Palka, Edward Elgar Publishing, 2024, p. 317.

⁶⁰ DUARTE, DE GREGORIA and GOLIA, p. 317.

⁶¹ KAPANİ, Münci, **Kamu Hürriyetleri**, Yetkin Yayınları, 1993, p. 230.

⁶² KAPANİ, p. 230.

⁶³ DUARTE / DE GREGORIA / GOLIA, p. 323-4.

⁶⁴ DUARTE / DE GREGORIA / GOLIA, p. 323.

secure the rule of law, public and private institutions must hand in their power. Whenever an organised power threatens fundamental rights, regardless of the nature of the force, principles such as transparency, accountability, representation or due process should be considered⁶⁵. This also includes the intertwining of public and private powers that lead to forms of cooperation and conflict⁶⁶. Constitutionalism, with the principle of the rule of law, has experience in eliminating the concentration of power and has ways and methods to turn threats created by the digital environment to the advantage of the state and citizens⁶⁷.

Online laws resolve the boundaries of forbidden conduct and secure the rule of law⁶⁸. The national laws applicable within the state's boundaries challenge cyber-space, which has no border within the infinite global communications network⁶⁹. Thus, the rule of law is a challenging target to qualify at the national level due to the international nature of the cyber world. National jurisprudence within the national boundaries where national and international "principles, behaviour, and jurisprudence" have developed, applied and interpreted over time⁷⁰. Not certainly, but states have been developing their selves in digital abilities⁷¹. However, this is not the case in cyberspace yet, where there have been initiatives to implement these legal norms in cyberspace⁷².

In the early stage of digitalising, state power declined and weakened due to the lack of traditional governmental tools in the new digital arena. Private entities in the digital world are powerful enough to push governments to change national laws according to their interest⁷³. The state cooperates with these private entities to regulate and enforce cyberspace, report unwanted content, and implement various filtering systems⁷⁴. This is the case, especially since international companies are subject. When the state does not enforce its law in the first place and hands over its power to private entities, it limits its power, while the

⁶⁵ DUARTE / DE GREGORIA / GOLIA, p. 324.

⁶⁶ DUARTE / DE GREGORIA / GOLIA, p. 324.

⁶⁷ ÇATLI, p. 373.

⁶⁸ WALKER / CONWAY, p. 160.

⁶⁹ AKHGAR, Babak / STANIFORTH, Andrew, / BOSCO, Francesca, **Cyber Crime and Cyber Terrorism Investigator's Handbook**, Elsevier, 2014, p. 3.

⁷⁰ AKHGAR / STANIFORTH / BOSCO, p. 3.

⁷¹ GOLUMBIC, p. 7.

⁷² AKHGAR / STANIFORTH / BOSCO, p. 3.

⁷³ GOLUMBIC, p. 8.

⁷⁴ GOLUMBIC, p. 8.

state's power is based on the law and limited by the law⁷⁵. Yet, as the natural law-maker, the state has kept this right. The state can regulate the digital space where digital platforms have become a centre of power, primarily through the principle of rule(s) of law.

B. Legitimacy - Representation

Democracy is a phenomenon based on popular sovereignty, in which the people are the noble and supreme actors of political power⁷⁶. It also considers the people participating in the functioning of the political order by placing them as the bearers and implementers of current political power. It requires active participation in political affairs or focusing more on policy outcomes. Indeed, the internet can be an extension of participatory democracy by expanding the boundaries of representative democracy as it facilitates the institution of representation and increases the means of representation. In this respect, it is important for direct democracy⁷⁷. It is applied in two ways: 1) the administration shares information about its citizens, and 2) elections are held to determine public opinion⁷⁸. Democracy involves a blend of an ideal and a procedural arrangement⁷⁹.

The law serves as the language of an invisible handshake that relies on legitimacy. Legitimacy is needed for effectiveness and to limit power through the rule of law. This may consist of representation in rulemaking, adjudication or enforcement of regulations. It may mean representing individuals, private companies, social structures, or states⁸⁰. So, if the state uses private entities to implement the law without constitutional check and balance settings, this is out of the context formed by legitimate actors in the state⁸¹. To maintain the existence of statehood and protect state sovereignty, states must establish a mechanism and operation that will not depend on private companies and process data belonging to their own country⁸².

⁷⁵ GOLUMBIC, p. 8.

⁷⁶ DETLEF HORN Hans, "Demokrasi", Çev. Hüseyin Yıldız, içinde Anayasa Teorisi, Ed. Otto Depenheuer ve Christoph Grabenwarter, Çev. Ed. İlyas Doğan, Lale Yayıncılık, 2014, p. 762.

⁷⁷ IŞIK, Alper, **Dijital Demokrasi**, Oniki Levha Yayınları 2020, p. 83.

⁷⁸ ZENGİN, Mehmet Ali. "Bilgi İletişim Teknolojilerinin Demokrasi İçerisinde Kullanımı ve Dijital Demokrasiye Geçiş", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, Y. 2013, V. 17(4), p. 271-304. p. 274.

⁷⁹ CINI, Michelle, and NIEVES Pérez-Solórzano Borragán, **European Union Politics**. Oxford University Press, 2010, p. 379.

⁸⁰ DUARTE / DE GREGORIA / GOLIA, p. 324-5.

⁸¹ GOLUMBIC, p. 8.

⁸² ÇATLI, p. 373.

Representation meant representation of citizens, legitimising the rule-making authority and giving the government the authority to make decisions on their behalf. Yet, representation is challenging for digital constitutionalism due to the powerful different actors in play. Without a defined territory in the digital age, “citizens’ representation”, one of the fundamental premises of classical liberal constitutionalism, disappears⁸³. Online platforms develop community standards and rules, while norms at the international level are shaped by influences distant from the local dimension. In these cases, the user or citizen plays a marginal role⁸⁴.

The rules of the digital environment are not determined primarily through transparent and democratic processes⁸⁵. The digital revolution relies on single-sided imposition in terms of representation. During the process, some other parties (especially states) get involved in regulating, which might be regarded as representation. Digital technologies cause three core challenges to democratic participation: 1) digital platforms monopolise communication and the content by avoiding national regulatory measures, 2) algorithmic engines interfere with what we want to see and hear and influence what we think and do, with little transparency are using vast quantities of personal data to make ever more precise predictions about, 3) the dominant business model of digital platforms prioritises attention economy which amplifies the content that is best at capturing our attention⁸⁶. Rights and powers are shaped and limited in a situation where the individual is weak. Given the limits of achieving full representation in a networked system of normativity and power, it is critical to rebalance the individual’s position in the digital age⁸⁷. This is crucial for the representation of individuals. Digital platforms positively affect citizens to participate, improve government transparency and rebuild trust in democratic processes⁸⁸. Yet, states are armed with myriad technologies to limit and constrain how dissidents can use ICTs. States can actively censor internet content, control the internet infrastructure, or combine the two⁸⁹. This means that governmental filtering through

⁸³ DUARTE / DE GREGORIA / GOLIA, p. 325.

⁸⁴ DUARTE / DE GREGORIA / GOLIA, p. 325.

⁸⁵ DUARTE / DE GREGORIA / GOLIA, p. 325.

⁸⁶ **Digital Threats to Democracy**, by, (Online) digitaldemocracy.nz, 2019, p. 34, A.D. 02.10.2024. See also, İŞİK, p. 84-88.

⁸⁷ DUARTE / DE GREGORIA / GOLIA, p. 325.

⁸⁸ **Digital Threats to Democracy**, by, (Online) digitaldemocracy.nz, 2019, p. 35-6, A.D. 02.10.2024.

⁸⁹ MCLAUGHLIN, W. Sean, **The use of the Internet for Political Action by Non-State Dissident Actors in the Middle East**, (2007), (originally published in November 2003), (Online), <https://firstmonday.org/ojs/index.php/fm/article/view/1791/1671>, A.D. 21.11.2024.

an index of websites blocks citizens from accessing⁹⁰. Filtering through private or public entities in both ways produces limitations and constraints for individuals' use of ICTs. The question here is which one is most legitimate.

C. Remedies

A remedy has multiple meanings, yet it signifies a condition that requires improvement⁹¹. States are expected to identify the remedies (not only judicial remedies) available to individuals and show at least a prima facie case for their effectiveness. States are in charge of a negative obligation to refrain from violating rights and a positive obligation to ensure the enjoyment of rights. States' positive obligations mean that public authorities take necessary measures to protect persons from violating rights by private parties⁹². The possibility of horizontal expansion of the protection of fundamental rights or the state's positive obligation to protect rights and freedoms drives the courts and legislators to protect rights and freedoms actively in the digital age⁹³. Giant digital companies claim to produce the remedies from autonomous orders and processes of constitutionalisation beyond the state. So, this progresses outside a system of transparency and accountability; the role of control and review, namely ensuring the constitutional values accepted by society, is losing its power and primary role⁹⁴. If the national judicial system is outsourced and managed by private organisations' rules and standards, ICTs are beyond classical constitutionalism. In this case, states become less important for remedies, which is critical for users (citizens)⁹⁵. Digital constitutionalism plays a role in developing a remedy system that ensures no lack or fragmentation of remedies in digital spaces for persons⁹⁶. Redress mechanisms for persons through the review of content moderation is an example of how digital constitutionalism expands its boundaries by considering social and global changes. Remedies are carried by the party who set the rule. Thus, the private sector or state plays a significant role in remedying power. Here, digital technologies have made some advances in digital platforms regard-

⁹⁰ CONWAY, p. 327-28.

⁹¹ ZAN, Qianglong. "Birks, Rights, Wrongs and Remedies." *Oxford Journal of Legal Studies*, Y. 2004, V. 20(1), p. 1-37, p. 9.

⁹² Human Rights Committee, General Comment No. 31 [80], The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, (29 March 2004), (CCPR/C/21/Rev.1/Add.13).

⁹³ DUARTE / DE GREGORIA / GOLIA, p. 326.

⁹⁴ DUARTE / DE GREGORIA / GOLIA, p. 326.

⁹⁵ DUARTE / DE GREGORIA / GOLIA, p. 326.

⁹⁶ DUARTE / DE GREGORIA / GOLIA, p. 326.

ing remedies. Yet, states have progressed to some extent in ruling out digital technologies, which ensures the main state's duty of remedy. If the analogy between disease and medicine is taken into account, anything that alleviates, eliminates or prevents a violation of constitutional rights can be called a remedy⁹⁷.

III. INTERWEAVING DIGITAL CONSTITUTIONALISM AND INTERNATIONAL HUMAN RIGHTS LAW

The UN Universal Declaration of Human Rights (UNDHR) 1948, the European Convention on Human Rights 1950 (ECHR), the International Covenant on Civil and Political Rights 1976, and the EU Charter of Fundamental Rights 2000 set key obligations for signatory states, no matter if the world is real or cyber. The legal challenge arises from factual differences between the "real" and "cyber" worlds⁹⁸. There are technical differences between the two worlds, such as whether the current laws regulate the cyber world as they regulate the real world. However, as many countries have enacted online laws, this trend reveals that *"the internet requires specific legislation tailored to its specific characteristics which impart differences in terms of risk and legal attributes. The risk factors include quantity (potential audience size and accessibility without the intercession of editors or otherwise) as well as quality (the intensity and instantaneity of messages and the facility for personal interaction)"*⁹⁹. While digital technology provides new ways to exercise human rights, they are too often used to breach them through data protection, privacy issues, digital identity, surveillance technologies, cyberterrorism, online violence, and harassment. Due to the dubious efficacy of many provisions for real-world conduct and the absence of more innovative responses¹⁰⁰, online laws are criticised as creating a "surveillance society" that introduces disproportionate power of interference¹⁰¹. Introducing online laws disturbs human rights, not only the relevant person¹⁰².

⁹⁷ ZAN, p. 9.

⁹⁸ WALKER / CONWAY, p. 159.

⁹⁹ WALKER / CONWAY, p. 159-160.

¹⁰⁰ WALKER / CONWAY, p. 160.

¹⁰¹ See FUCHS, Christian / BOERSMA, Kees / ALBRECHTSLUND, Andres / SANDOVAL, Marisol (eds), **Internet and Surveillance: The Challenges of Web 2. 0 and Social Media**, Taylor & Francis Group, London, 2011.

¹⁰² WALKER, Clive / AKDENIZ, Yaman, "Anti-terrorism laws and data retention: War is over?", **Northern Ireland Legal Quarterly**, Y. 2003, V. 54, p. 159-182, p. 162.

International human rights instruments have not been considered alongside digital technology for decades since its birth. The UN-sponsored World Summit on the Information Society, which briefly references ‘rights to privacy, data, and consumer protection’, made a prior consideration of it in the Geneva Plan of Action (2003)¹⁰³. In 2019, ‘Joint Declaration Challenges to Freedom of Expression in the Next Decade by UN, OSCE, OAS and ACHPR’ recognised “*the right to access and use the Internet as a human right as an essential condition for the exercise of the right to freedom of expression*”¹⁰⁴. This declaration relies on the concern that exercising freedom of expression requires a strong, universal and regulated digital infrastructure that ensures that it remains a free, accessible and open space for all parties¹⁰⁵. Following a milestone in the discourse of the United Nations, the UN-HRC’s Resolution 20/8 of 5 July 2012 on the ‘promotion, protection and enjoyment of human rights on the Internet’ expressed the applicability of international human rights norms to the Internet¹⁰⁶. This Resolution confirms that human rights, especially freedom of expression, have a place not only in the physical world but also in the digital world. In other words, ‘the same rights that people have offline must also be protected online’¹⁰⁷. While the Human Rights Committee has adopted in 2011 General Comment No. 34 recommends that states ensure that information and communication technologies such as “*internet and mobile-based electronic information dissemination systems, all necessary steps to foster the independence of these new media and to ensure access of individuals thereto*”¹⁰⁸. The Rabat Plan of Action developed by the UN OHCHR in 2013 highlights new technologies (such as digital

¹⁰³ World Summit on the Information Society Geneva 2003, Tunis 2005, Declaration of Principles: Building the Information Society: a global challenge in the new Millennium, (WSIS-03/GENEVA/DOC/5-E).

¹⁰⁴ The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade.

¹⁰⁵ The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade.

¹⁰⁶ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (2011, 16 May), (A/HRC/17/27).

¹⁰⁷ Human Rights Council, Resolution 20/8, The Promotion, Protection, and Enjoyment of Human Rights on the Internet, (2012, 16 July), (A/HRC/RES/20/8).

¹⁰⁸ Human Rights Committee, General Comment No. 34 Article 19: Freedoms of Opinion and Expression, 12 September 2011, (CCPR/C/GC/34).

broadcasting, mobile telephony, the Internet and social networks) enhancing the dissemination of information and opening new forms of communication¹⁰⁹. With such UN materials, international human rights instruments must be considered in relation to digital technologies.

However, in the UN system, concerns are raised over digital technologies and the right to freedom of expression. The Human Rights Council and the General Assembly have emphasised that offline rights must be respected online, but online rights are deteriorating¹¹⁰. Private industries with possible authoritarian tendencies have tremendous influence in the digital realm, serving as mediators for online communication¹¹¹. Private companies should be evaluated on supporting and hindering freedom of expression¹¹². States and private actors facilitate or demand content removal, censorship and unnecessary or disproportionate restrictions on the right to freedom of expression. States regulate digital content through various legal, political and technical means of vague laws, excessive intermediary liability, extra-legal restrictions, filtering, network or service shutdowns, and non-neutral networks¹¹³. Terms of service, design and engineering choices of digital platforms are used as intermediary policies and rules that affect content delivery¹¹⁴. Digital communications and data stored or transmitted over private networks are increasingly vulnerable to surveillance and interference by both state and private entities¹¹⁵. Various communications surveillance modalities are identified as ‘targeted communications surveillance’, ‘mass communications surveillance’, ‘access to communications data’, ‘internet filtering and censorship’, and ‘restrictions on anonymity’¹¹⁶. Excessive and un-

¹⁰⁹ Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred, 11 January 2013, (A/HRC/22/17/Add.4).

¹¹⁰ The United Nations (UN) General Assembly, Promotion and protection of the right to freedom of opinion and expression, 6 September 2016, (A/71/373), para 56.

¹¹¹ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38).

¹¹² VICTORIA, Ionita Claudia / MACHIKO, Kanetake, “International human rights law in the digital age: perspectives from the UN human rights system”, **Research Handbook on Law and Technology**, Eds. Bartosz Brozek, Olya Kanevskaia, and Przemyslaw Palka, Edward Elgar Publishing, 2024, p. 240.

¹¹³ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38), para 38-50.

¹¹⁴ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38), para 51.

¹¹⁵ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38), para 57.

¹¹⁶ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (17 April 2013), (A/HRC/23/40).

warranted surveillance can jeopardise online safety and hinder access to information and ideas¹¹⁷. Surveillance can have a chilling effect on ordinary citizens' online freedom of expression, who may censor themselves for fear of being constantly monitored¹¹⁸.

The states are expected to be concerned about adapting their domestic law to global human rights standards¹¹⁹. They are responsible for complying with international standards in human rights. Digital constitutionalism interweaves with the international human rights system by adopting digital technology into the constitutional ecosystem. The global human rights system progressively considers digital technology as transforming relations between parties and powers. Digital technology generates some alterations to support and hinder human rights in the opposite ways. Thereby, states are responsible for complying with the international human rights system's concerns over digital technology in the practice of human rights. Digital constitutionalism, through these concerns, requires states to regulate private companies on both counts of supporting and hindering human rights.

CONCLUSION

Digital technology brings about significant changes in the constitutional ecosystem. The widespread availability of digital tools among individuals, coupled with the dominant role of private companies in the digital environment, heightens the risk of human rights violations by non-state actors. This shift disrupts established power-balancing mechanisms that traditionally focus on the relationships between individuals and nation-states. Hence, digital technology integrates itself into the constitutional ecosystem, resulting in a new equilibrium between constitutional institutions, human rights, and the realities shaped by digital technology.

Digital constitutionalism must rely on a normative perspective, which proposes protecting fundamental rights and limiting powers in the digital age. It suggests that the state can regulate the digital space where digital platforms have become a central power, primarily through the principle of rule(s) of law,

¹¹⁷ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (17 April 2013), (A/HRC/23/40).

¹¹⁸ Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38), para 57.

¹¹⁹ AKAD / VURAL DİNÇKOL / BULUT, p. 230.

the monopoly of legitimacy and remedies. First, establishing the rule of law at the national level is a complex challenge due to the international nature of the cyber world. This raises several important questions regarding the rules of law: What distinguishes rules as “digitally constitutional” in a transnational environment governed by public, private, or global normative orders? Who is responsible for creating these rules as law? Does any rule that affects the digital realm automatically qualify as “digital constitutionalism”? In the early stages of digitalisation, state power decreased as traditional governmental tools proved ineffective in the new digital landscape. While it is not certain, states have been working to enhance their digital capabilities. The legislative body must enact any restrictions on freedom through formal law. Second, legitimacy is crucial in ensuring effectiveness and limiting power through the rule of law. It serves as the basis for the invisible handshake of governance, relying on acknowledgement as legitimacy. However, the challenge of digital constitutionalism arises from the influence of powerful actors. When the state employs private entities to carry out the law without proper constitutional checks and balances, it strays from the framework established by legitimate state actors. Legitimacy is also essential for representation, as it involves validating the authority that creates rules and granting the government the power to make decisions on behalf of the people. Unfortunately, processes that lack transparency and democratic participation often shape the regulations of the digital landscape. As a result, the digital revolution tends to impose rules one-sided, undermining genuine representation. The evolution of remedies expands the protection of fundamental rights and the obligation of the state to uphold these rights and freedoms, particularly in the digital age. This has prompted courts and legislators to take an active role in safeguarding individual rights. In this context, digital constitutionalism is crucial for establishing a comprehensive remedy system that addresses gaps or inconsistencies in digital spaces. Remedies are typically provided by the entity that creates the regulations, which positions the private sector and the state as key players in enforcing these remedies. While digital technologies have led to advancements in the provision of remedies through various platforms, it is noteworthy that states have also made progress in integrating these technologies to fulfil their fundamental duty to provide remedies.

The international human rights law system recognises digital technology as a crucial aspect of constitutionalism. States are responsible for adapting their domestic laws to align with global human rights standards. They are accountable for adhering to international norms surrounding human rights. Digital constitutionalism integrates digital technology into the constitutional framework,

reflecting its influence on the international human rights system. The global perspective increasingly views digital technology as transforming interactions between individuals and authorities. This technology may support and hinder human rights in different ways. As such, states must address the concerns of the international human rights system regarding digital technology in their human rights practices. Digital constitutionalism mandates that states regulate private entities to ensure they neither impede nor undermine human rights.

Hakem Değerlendirmesi : Dış bağımsız.

Çıkar Çatışması : Yazar çıkar çatışması bildirmemiştir.

Finansal Destek : Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review : *Externally peer-reviewed.*

Conflict of Interest : *The author has no conflict of interest to declare.*

Grant Support : *The author declared that this study has received no financial support.*

BIBLIOGRAPHY

AKAD, Mehmet / VURAL DİNÇKOL, Bihterin / BULUT, Nihat, **Genel Kamu Hukuku**, Der Yayınları, 2021.

AKHGAR, Babak / STANIFORTH, Andrew / BOSCO, Francesca. **Cyber Crime and Cyber Terrorism Investigator's Handbook**, Elsevier, 2014.

AMBLE, John Curtis, "Combating Terrorism in the New Media Environment", **Studies in Conflict & Terrorism**, Y. 2012, V. 35(5), p. 339-353.

ATALAY, Muhammet / ÇELİK, Enes, "Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Y. 2017, V. 9(22), p. 155-172.

BALKIN, Jack, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", **New York University Law Review**, Y. 2004, V. 79(1), p. 1-55.

BEDUSCHİ, Ana, **Human Rights and the Governance of Artificial Intelligence**, (2020), (Online), <https://www.geneva-academy.ch/research/publications/detail/513-human-rights-and-the-governance-of-artificial-intelligence>, A.D. 18.01.2025.

BREWER, Judy, "Standards Bodies, Access to Information Technology, and Human Rights", **Disability, Human Rights, and Information Technology**, Eds. Lazar Jonathan, and Stein Michael Ashley, University of Pennsylvania Press, 2017.

ÇATLI, Mehmet, "Yapay Zekânın Anayasası: "Akıllı Anayasa" Üzerine", **Adalet Dergisi**, Y. 2023/1, V. 70, p. 369-383.

CELESTE, Edoardo, **Digital Constitutionalism: The Role of Internet Bills of Rights**, Routledge, 2023.

CELESTE, Edoardo, **Digital constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges**, HIIG Discussion Paper Series 2018-02, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3219905.

CELESTE, Edoardo, "Digital Constitutionalism: A New Systematic Theorisation", **International Review of Law, Computers & Technology**, Y. 2019, V. 33(1), p. 76-99.

CINI, Michelle, and NIEVES Pérez-Solórzano Borragán, **European Union Politics**. Oxford University Press, 2010, p. 379.

- CLIVE, Walker / CONWAY, Maura, “Online terrorism and online laws”, **Dynamics of Asymmetric Conflict**, Y. 2015, V. 8(2), p. 156-175.
- CONWAY, Maura, “Terrorist Use of the Internet and the Challenges of Governing Cyberspace”, **Power and Security in the Information Age: Investigating the Role of the State in Cyberspace**, Eds. Dunn Myriam, Victor Mauer, & Felisha Krishna-Hensel, Ashgate, London, 2007.
- DE GREGORIO, Giovanni, “Digital Constitutionalism across the Atlantic”, **Global Constitutionalism**, Y. 2022, V. 11(2), p. 297-324.
- DE GREGORIO, Giovanni, “The Rise of Digital Constitutionalism in the European Union”, **International Journal of Constitutional Law**, Y. 2021, V. 19(1), p. 41-70.
- Digital Threats to Democracy, by, digitaldemocracy.nz, 2019.
- DUARTE, Francisco de Abreu / DE GREGORIA Giovanni / GOLIA Angelo Jr, “Perspectives on Digital Constitutionalism”, **Research Handbook on Law and Technology**, Eds. Bartosz Brozek, Olia Kanevskaia, and Przemyslaw Palka, Edward Elgar Publishing, 2024.
- ELKIN-KOREN, Niva, “Making Technology Visible: Liability of Intent Service Providers for Peer-to-Peer Traffic”, **Journal of Legislation and Public Policy**, Y. 2006, V. 9(15), p. 15-74.
- FRASER, Sampson, “Cyberspace: the New Frontier for Policing”, **Cyber Crime and Cyber Terrorism Investigator’s Handbook**, Eds. Akhgar Babak, Staniforth Andrew, and Bosco Francesca, Elsevier, 2014.
- FUCHS, Christian / BOERSMA, Kees / ALBRECHTSLUND, Andres / SANDOVAL, Marisol (eds), **Internet and Surveillance: The Challenges of Web 2.0 and Social Media**, Taylor & Francis Group, London, 2011.
- GOLUMBIC, Martin Charles, **Fighting Terror Online the Convergence of Security, Technology, and the Law**, Springer, 2008.
- GÖZLER Kemal, **Anayasa Hukukunun Genel Esasları**, Ekin Basım Yayın, 2024.
- Human Rights Committee, General Comment No. 31 [80] The Nature of the General Legal Obligation Imposed on States Parties to the Covenant Adopted on 29 March 2004, (CCPR/C/21/Rev.1/Add.13).
- Human Rights Committee, General Comment No. 34 Article 19: Freedoms of Opinion and Expression, 12 September 2011, (CCPR/C/GC/34).
- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (2011, 16 May), (A/HRC/17/27).
- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38).

- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38).
- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38).
- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38).
- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (17 April 2013), (A/HRC/23/40).
- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (11 May 2016), (A/HRC/32/38).
- Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred, (11 January 2013), (A/HRC/22/17/Add.4).
- Human Rights Council, Resolution 20/8, The Promotion, Protection, and Enjoyment of Human Rights on the Internet, (2012, 16 July), (A/HRC/RES/20/8).
- İŞİK, Alper, **Dijital Demokrasi**, Oniki Levha Yayınları 2020.
- KAMA İŞİK, Sezen, “Klasik Anayasacılıktan Dijital Anayasacılığa: Anayasa Hukukunun Dönüşümü”, **Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı**, Adalet Yayınevi, Ankara, 2021.
- KAPANİ, Münci, **Kamu Hürriyetleri**, Yetkin Yayınları, 1993.
- MARCHANT, Gary E., “The Growing Gap Between Emerging Technologies and the Law”, **The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight**, Eds. Gary E. Marchant, Braden R. Allenby, Joseph R. Herker, Springer, 2011.
- MCLAUGHLIN, W. Sean, **The use of the Internet for Political Action by Non-State Dissident Actors in the Middle East** (2007) (originally published in November 2003), <https://firstmonday.org/ojs/index.php/fm/article/view/1791/1671> A.D. 21.11.2024.
- MOSES, Lyria Bennett, “Recurring dilemmas: The law’s race to keep up with Technological Change”, **University of Illinois Journal of Law, Technology & Policy**, Y. 2007, V. 21, p. 239-285.
- MULLER, Catelijne, **The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law**, Ad Hoc Committee on Artificial Intelligence (Cahai), (2020), (Online), <https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da>, A.D. 18.01.2025.

- PETERS, Anne, “Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures”, **Leiden Journal of International Law**, Y. 2006, V. 19(3), p. 579-610.
- ROCO, Mihail C. / BAINBRIDGE William Sims, **Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science**, Kluwer Academic Publishers, Dordrecht, 2003.
- SAJÓ, András / UITZ, Renáta, **The Constitution of Freedom: An Introduction to Legal Constitutionalism**, Oxford Academic, 2017.
- SASSEN, Saskia, “On the Internet and Sovereignty”, **Indiana Journal of Global Legal Studies**, Y. 1998, V. 5(2), p. 545-559.
- SHARMA, Dhiraj, **Communication in IT Age**, Himalaya Pub. House, Mumbai, 2020.
- SUZOR, Nicolas, **Lawless: The Secret Rules That Govern Our Digital Lives**, Cambridge University Press, 2019.
- The United Nations (UN) General Assembly, Promotion and protection of the right to freedom of opinion and expression, 6 September 2016, (A/71/373).
- The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade, <https://www.osce.org/files/f/documents/9/c/425282.pdf>,
- VICTORIA, Ionita Claudia / MACHIKO, Kanetake, “International human rights law in the digital age: perspectives from the UN human rights system”, **Research Handbook on Law and Technology**, Eds. Bartosz Brozek, Olya Kanevskaia, and Przemyslaw Palka, Edward Elgar Publishing, 2024.
- WALKER, Clive / AKDENİZ, Yaman, “Anti-terrorism laws and data retention: War is over?”, **Northern Ireland Legal Quarterly**, Y. 2003, V. 54, p. 159-182.
- World Summit on the Information Society Geneva 2003, Tunis 2005, Declaration of Principles: Building the Information Society: a global challenge in the new Millennium, (WSIS-03/GENEVA/DOC/5-E).
- ZAN, Qianglong. “Birks, Rights, Wrongs and Remedies.” **Oxford Journal of Legal Studies**, Y. 2004, V. 20(1), p. 1-37.
- ZENGİN, Mehmet Ali. “Bilgi İletişim Teknolojilerinin Demokrasi İçerisinde Kullanımı ve Dijital Demokrasiye Geçiş”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, Y. 2013, V. 17(4), p. 271-304.
- ZUHOFF Shoshana, **The Age of Surveillance Capitalism**, Profile Books, Londra, 2019.