ano 24 – n. 98 | outubro/dezembro – 2024
Belo Horizonte | p. 1-224 | ISSN 1516-3210 | DOI: 10.21056/aec.v24i98
A&C – R. de Dir. Administrativo & Constitucional
www.revistaaec.com

A&C

Revista de Direito ADMINISTRATIVO & CONSTITUCIONAL

A&C – ADMINISTRATIVE & CONSTITUTIONAL LAW REVIEW

FORUM

A&C – REVISTA DE DIREITO ADMINISTRATIVO & CONSTITUCIONAL

IPDA
Instituto Paranaense
de Direito Administrativo

INSTITUTO DE DIREITO ROMEU FELIPE BACELLAR

FÓRUM
Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Rua Paulo Ribeiro Bastos, 211 – Jardim Atlântico – CEP 31710-430 – Belo Horizonte/MG – Brasil – Tel.: (31) 99412.0131
www.editoraforum.com.br / E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil / Distribuída em todo o Território Nacional

Os conceitos e opiniões expressas nos trabalhos assinados são de responsabilidade exclusiva de seus autores.

A246 A&C : Revista de Direito Administrativo & Constitucional. – ano 3, n. 11, (jan./mar. 2003)- . – Belo Horizonte: Fórum, 2003-

Trimestral
IISSN impresso 1516-3210
ISSN digital 1984-4182

Ano 1, n. 1, 1999 até ano 2, n. 10, 2002 publicada pela Editora Juruá em Curitiba

1. Direito administrativo. 2. Direito constitucional. I. Fórum.

CDD: 342
CDU: 342.9

Coordenação editorial: Leonardo Eustáquio Siqueira Araújo
Thaynara Faleiro Malta
Capa: Igor Jamur
Projeto gráfico: Walter Santos
Revisão: Bárbara Ferreira
Diagramação: Derval Braga

Periódico classificado no Estrato A1 do Sistema Qualis da CAPES - Área: Direito.

Qualis – CAPES (Área de Direito)
Na avaliação realizada em 2022, a revista foi classificada no estrato A1 no Qualis da CAPES (Área de Direito).

Entidade promotora
A *A&C – Revista de Direito Administrativo & Constitucional*, é um periódico científico promovido pelo Instituto de Direito Romeu Felipe Bacellar com o apoio do Instituto Paranaense de Direito Administrativo (IPDA).

Foco, Escopo e Público-Alvo
Foi fundada em 1999, teve seus primeiros 10 números editorados pela Juruá Editora, e desde o número 11 até os dias atuais é editorada e publicada pela Editora Fórum, tanto em versão impressa quanto em versão digital, sediada na BID – Biblioteca Digital Fórum. Tem como principal objetivo a divulgação de pesquisas sobre temas atuais na área do Direito Administrativo e Constitucional, voltada ao público de pesquisadores da área jurídica, de graduação e pós-graduação, e aos profissionais do Direito.

Linha Editorial
A linha editorial da A*&C – Revista de Direito Administrativo & Constitucional*, estabelecida pelo seu Conselho Editorial composto por renomados juristas brasileiros e estrangeiros, está voltada às pesquisas desenvolvidas na área de Direito Constitucional e de Direito Administrativo, com foco na questão da efetividade dos seus institutos não só no Brasil como no Direito comparado, enfatizando o campo de intersecção entre Administração Pública e Constituição e a análise crítica das inovações em matéria de Direito Público, notadamente na América Latina e países europeus de cultura latina.

Cobertura Temática
A cobertura temática da revista, de acordo com a classificação do CNPq, abrange as seguintes áreas:
- Grande área: Ciências Sociais Aplicadas (6.00.00.00-7) / Área: Direito (6.01.00.00-1) / Subárea: Teoria do Direito (6.01.01.00-8) / Especialidade: Teoria do Estado (6.01.01.03-2).
- Grande área: Ciências Sociais Aplicadas (6.00.00.00-7) / Área: Direito (6.01.00.00-1) / Subárea: Direito Público (6.01.02.00-4) / Especialidade: Direito Constitucional (6.01.02.05-5).
- Grande área: Ciências Sociais Aplicadas (6.00.00.00-7) / Área: Direito (6.01.00.00-1) / Subárea: Direito Público (6.01.02.00-4) / Especialidade: Direito Administrativo (6.01.02.06-3).

Indexação em Bases de Dados e Fontes de Informação
Esta publicação está indexada em:
- Web of Science (ESCI)
- Ulrich's Periodicals Directory
- Latindex
- Directory of Research Journals Indexing
- Universal Impact Factor
- CrossRef
- Google Scholar
- RVBI (Rede Virtual de Bibliotecas – Congresso Nacional)
- Library of Congress (Biblioteca do Congresso dos EUA)
- MIAR - Information Matrix for the Analysis of Journals
- WorldCat
- BASE - Bielefeld Academic Search Engine
- REDIB - Red Iberoamericana de Innovación y Conocimiento Científico
- ERIHPLUS - European Reference Index for the Humanities and the Social Sciences
- EZB - Electronic Journals Library
- CiteFactor
- Diadorim

Processo de Avaliação pelos Pares (*Double Blind Peer Review*)
A publicação dos artigos submete-se ao procedimento *double blind peer review*. Após uma primeira avaliação realizada pelos Editores Acadêmicos responsáveis quanto à adequação do artigo à linha editorial e às normas de publicação da revista, os trabalhos são remetidos sem identificação de autoria a dois pareceristas *ad hoc* portadores de título de Doutor, todos eles exógenos à Instituição e ao Estado do Paraná. Os pareceristas são sempre Professores Doutores afiliados a renomadas instituições de ensino superior nacionais e estrangeiras.

DOI: 10.21056/aec.v24i98.1931

IT Giants vs. states in human rights regulation in digital space: a comparative review

Gigantes de TI vs. Estados na regulamentação dos direitos humanos no espaço digital: uma análise comparativa

Vadim Vinogradov*
HSE University (Moscow, Russia)
vadim.a.vinogradov@gmail.com
https://orcid.org/0000-0001-8490-2893

Estelle Chambas**
Université Paris Panthéon-Assas (Paris, France)
https://orcid.org/0000-0003-2913-0792

Recebido/Received: 05.04.2024 / 5 April 2024
Aprovado/Approved: 11.09.2024 / 11 September 2024

Abstract: The extensive power of IT Giants in the digital domain requires national governments to strengthen regulatory measures. This article addresses the critical debate on the parallelism between IT Giants and sovereign states, with an emphasis on the governance of human rights in digital space. The analysis engages with the regulatory landscapes within the European Union, with a specific look at France's legal mechanisms, and contrasts these with the regulatory environment in Russia. The research evaluates the effectiveness of both nation-states and IT Giants in upholding human rights in

Como citar este artigo/*How to cite this article:* VINOGRADOV, Vadim; CHAMBAS, Estelle. IT Giants vs. states in human rights regulation in digital space: a comparative review. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 98, p. 11-38, out./dez. 2024. DOI: 10.21056/aec.v24i98.1931.

* Dean of the Law Faculty of the HSE University (Moscow, Russia). Doctor of Law, Professor at HSE University (Moscow, Russia).

** Research fellow at Centre d'études et de recherches de sciences administrative, Université Paris Panthéon-Assas (Paris, France). PhD, Université Paris Panthéon-Assas (Paris, France).

digital space, scrutinizing statutory norms alongside corporate governance policies. The objective is to determine if IT Giants are comparable to nation-states in their role in human rights protection.

Keywords: GAFAM. Human rights. Big Tech. IT Giants. Digital human rights.

Resumo: O amplo poder dos gigantes da TI no domínio digital exige que os governos nacionais fortaleçam as medidas regulatórias. Este artigo aborda o debate crítico sobre o paralelismo entre as gigantes da TI e os Estados soberanos, com ênfase na governança dos direitos humanos no espaço digital. A análise aborda os cenários regulatórios da União Europeia, com um olhar específico sobre os mecanismos legais da França, e os compara com o ambiente regulatório da Rússia. A pesquisa avalia a eficácia tanto dos estados-nação quanto das gigantes de TI na defesa dos direitos humanos no espaço digital, examinando as normas estatutárias juntamente com as políticas de governança corporativa. O objetivo é determinar se as gigantes de TI são comparáveis aos Estados nacionais em seu papel na proteção dos direitos humanos.

Palavras-chave: GAFAM. Direitos humanos. Big Tech. Gigantes da TI. Direitos humanos digitais.

1 Introduction

The digitization encompassing all societal sectors emerges as a global trend, manifesting through the accelerating integration of digital technologies into various facets of daily life. Currently, over 64% of the global population engages with the internet, nearly 60% participate actively on social media platforms, dedicating more than six and a half hours to online activities daily.[1] This digital ascendancy is underscored by the market dominion of the GAFAM conglomerates (Google, Apple, Facebook, Amazon, and Microsoft),[2] colloquially known as the "IT Giants", highlighting the digital industry's progression alongside the power wielded by these corporations.

In this evolving landscape, the IT Giants transcend their economic influence, actively permeating the realms of politics and geopolitics (exemplified by the account suspension of the former President of the United States, Donald Trump). The dual-edged sword of digital technology offers convenience and process optimization, yet concurrently raises potential human rights infringements within the digital domain due to the rapid pace of digitalization. This scenario positions the law and legal frameworks as reactive guardians of human rights, a challenge shared across nations.

1 WE ARE SOCIAL. *Digital 2023.* Available at: https://wearesocial.com/uk/blog/2023/01/the-changing-world-of-digital-in-2023/. Accessed on: December 15, 2023.

2 STATISTA. *Biggest Companies in the World by Market Cap 2023*. Available at: https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/. Accessed on: March 15, 2024.

The advent of digital transformation has profoundly redefined the realization and perception of human rights, extending beyond traditional state sovereignty with the emergence of potent IT firms. Human rights in digital space faces "systemic dependence on the capabilities of online stakeholders" for its' protection.[3] IT Giants, wielding substantial digital authority, increasingly mimic digital sovereignties. The question arises: can they be equated to states, especially concerning their role in human rights regulation within the digital milieu? To explore this query, it is essential to analyze the regulation of specific human rights within the digital space by IT Giants in comparison to states.

This article embarks on comparing the European Union and France, along with Russia, motivated by their distinctive approaches towards regulating IT Giants. The EU, recognized as a pioneer in protection of human rights in the digital space, along with France's absence of native IT Giants and Russia's successful competition with global IT conglomerates within its market, presents a rich tapestry for analysis. The comparison seeks to illuminate the strategies employed by non-EU states in navigating digital human rights.

Through a precise examination of open quantitative data on user engagement across various internet platforms, alongside a qualitative-linguistic analysis of legal texts and IT Giants' policies, this article endeavors to discern the nuances in human rights regulation. By juxtaposing IT Giants with states, the article aims to ascertain the legitimacy of comparing these digital behemoths to traditional state entities in the context of human rights governance in the digital sphere. This inquiry, while not delving into the theoretical depths of human rights, focuses on a comparative analysis between selected IT Giants and states, probing the extent of IT Giants' commitment to human rights regulation and their resemblance to states in digital governance.

2 Human rights in the digital space. Selection of rights for analysis

Human rights, as outlined in the Universal Declaration of Human Rights (UDHR) by the United Nations in 1948,[4] set the foundation for the fundamental rights every individual should have. However, with the advent of digital technology and its impact

[3] SUSI, Mart. The image of human rights in e-state. *Journal of the Belarusian State University. International Relations*, [s.l.], vol. 20, n. 1, p. 62-68, jan./jun. 2020, p. 64.

[4] UNITED NATIONS. *Universal Declaration of Human Rights*. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed on: March 15, 2024.

on society, the interpretation and application of these rights in the digital realm have become imperative.[5]

Human rights are usually divided into three generations.[6] Currently, there is a talk about the formation of the fourth generation of human rights, which is associated with technological progress.[7] It appears that digitalization, by altering the specifics and conditions of the realization of fundamental rights, also impacts their content.

Part of the common and generally accepted human rights expansion in digital space is taking a new meaning. For example, the right to access information on the Internet is transforming into the right to true and accurate information, since digital space consists of various information streams, including a significant number of fakes. Modern technologies allow the creation of a great variety of cleverly crafted and believable fakes, which leads to misinformation for users, this perception building the formation of erroneous opinions and the adoption of unreasonable decisions. Any Internet user can become a newsmaker and influencer by spreading various types of data. Therefore, the task of the legislator is to provide users with access to reliable and truthful information. This is accomplished by instituting legal frameworks dedicated to the reduction and control of spurious content distribution.

Freedom of expression, for example, is also a cornerstone of the understanding of "freedom" and also apparently requires a more careful legal approach. Freedom of speech in digital space cannot be absolute, especially because of the anonymity of users, which gives them a sense of impunity leading to hate speech and bullying.[8] Such freedom of speech can provoke suffering for other users and even drive them to commit suicide. Therefore, it is crucial to find the right forms of control so as not to establish total control and thereby violate the right of freedom of speech, but at the same time protect everyone from the harmful results of such a right implementation. Regulation of web content and digital communications should be

5 FLORIDI, Luciano. *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality.* Oxford: Oxford University Press, 2014.

6 The initial generation encompasses civil and political liberties (liberty); the subsequent generation includes economic, social, and cultural entitlements (equality); and the final generation pertains to collective or solidarity rights (fraternity). This division was proposed in the 70s by Karel Vasak. *See* VASAK, Karel. A 30-Year Struggle: The Sustained Efforts to Give Force of Law to the Universal Declaration of Human Rights. *The UNESCO Courier*, vol.77, n. 11, p. 28-29, nov.1977, p. 29.

7 BUSTAMANTE DONAS, Javier. Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica. *Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación,* [s.l.], n.1, jan./mar. 2001.

8 PÉREZ DE LA FUENTE, Oscar. How can the internet change human rights on online hate speech regulations? *In*: SUNGUROV, Alexander (coord.); FERNÁNDEZ LIESA, Carlos Ramón (Coord.); BARRANCO AVILÉS, María del Carmen (coord.); LLAMAZARES CALZADILLA, María Cruz (coord.); PÉREZ DE LA FUENTE, Óscar (coord.). *Current Issues on Human Rights.* Madrid: Dykinson, 2020. p. 93-104.

carefully designed with the participation of all stakeholders and in accordance with international human rights law.[9]

Within the digital domain, the foremost right demanding safeguarding is the confidentiality of personal information. The imperative to protect online personal data emerges as a legislative priority, given that personal data constitutes the quintessential asset in the contemporary digital landscape. The potential for misuse of individuals' personal information spans a spectrum from engaging in various fraudulent activities to acts of bullying and inducing suicidal behavior. It is essential that individuals are empowered with knowledge regarding the collection, processing, and storage of their personal data, alongside the capabilities to amend and expunge such data. This encompasses the rights to personal data protection, access to one's personal data, data rectification, and the right to be forgotten.[10]

Digitalization has not only led to new approaches to traditional human rights, but has also given rise to new rights and freedoms.[11] It is notable that new "digital rights" are emerging, that is, rights that would not exist if there were no digital space. A striking example of such a new digital right is the right to Internet access. If earlier there were disputes about whether access to the Internet is a human right, and as such, in particular, "one of the fathers of the Internet" Vinton Cerf did not recognize such a right,[12] then at present, the right to access information technologies and, in particular, to access the Internet is already recognized as a human right. The UN has recognized Internet access as an inalienable human right that must be ensured at all levels. The European Declaration on Digital Rights and Principles for the Digital Decade says that "everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity". The right to access the Internet has a special nature because it is essentially an instrumental right, that is, a right that facilitates the realization of a number of other rights. Failure to realize the right to access the Internet leads to restrictions on other rights – to education, access to information, freedom of expression and a range of others. Lack of access to the Internet creates a digital divide.[13]

---

9 BELLOCCHIO, Lucía; SANTIAGO, Alfonso. Estado digital de Derecho. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 20, n. 80, p. 87-102, abr./jun. 2020, p. 100.

10 Art. 8, EUROPEAN UNION. EU Charter of Fundamental Rights. Available at: https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data#:~:text=Article%2010%20(3)%20Everyone%20has,misuse%20of%20her%20personal%20data. Accessed on: March 15, 2024.

11 COCCOLI, Jacopo. The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era. *Peace Human Rights Governance*, Padova, vol. 1, n. 2, p. 223-250, 2017. DOI: 10.14658/PUPJ-PHRG-2017-2-4.

12 CERF, Vinton G. Internet access is not a human right. *The New York Times*, jan./2012. Available at: https://nyti.ms/3FWWArK. Accessed on: March 15, 2024.

13 ÁLVAREZ ROBLES, Tamara. Las garantías de los derechos fundamentales en y desde la red: el contexto español. *Revista Chilena De Derecho Y Tecnología*, [s.l.], vol.11, n.1, p. 5-40. jan./mar. 2022, p.28.

Hence, the core human rights warranting defense in the digital realm include privacy of personal data, freedom of expression, the right to access personal data, the right to personal data rectification, the right to erasure (be forgotten), the right to access authentic and factual information, the principle of non-discrimination, and the right to Internet access. This encapsulation is particularly pertinent when considering services offered by IT Giants. The exploration of how states and IT Giants regulate these rights presents a compelling field of inquiry.

3 IT Giants: Digital States?

Once in the digital space, a person becomes a kind of "digital citizen" of IT platforms. IT giants are increasingly being compared to real states.[14] It is obvious that the policies and rules for using the services of IT platforms are similar to the laws of the state, users to citizens, moderators to courts and law enforcement agencies; blocking is essentially a form of coercion. The relationship between users and IT platforms is not between equal subjects, IT giants have independent "foreign policy", introduce "currency"[15] and have stronger cyber-military capabilities than most governments.[16] For example, prominent American political scientist Ian Bremmer openly states that "no government today has the toolkit to mess around with big tech, so it's time to start thinking of the biggest tech companies as true 'digital nation-states' with their own international relations. Never before has a small group of companies had such a vast impact on humanity".[17]

A state is often defined by three components, including the exercise of sovereignty upon a single territory and a single population.[18] It is the main subject

[14] DMITRIK, Nikolay. Digital State, Digital Citizen: Making Fair and Effective Rules for a Digital World. *Legal Issues in the Digital Age*, vol. 1, n. 1, p 54-78, jan./mar. 2020; APOSTOLICAS, Paul. Silicon States: How Tech Titans are Acquiring State-like Powers. *Harvard international review*, aug./2018. Available at: https://hir.harvard.edu/silicon-states-big-tech/ – Accessed on: March 15, 2024; BREMMER, Ian. Why Big Tech companies are like "digital nation states". *Gzero*, oct./2021. Available at: https://www.gzeromedia.com/gzero-world-clips/why-big-tech-companies-are-like-digital-nation-states. Accessed on: March 15, 2024.

[15] This is, for example, about the Libra project (later changed its name to Diem) to create a global digital cryptocurrency, initiated in 2019 by Facebook* (now Meta Platforms). The project faced serious challenges from governments and financial institutions around the world and was discontinued in early 2022. Facebook launched its own cryptocurrency Libra. *See*: Facebook unveils global digital coin called Libra. *Financial Times*, jun. 2019. Available at: https://www.ft.com/content/af6b1d48-90cc-11e9-aea1-2b1d33ac3271. Accessed on: March 15, 2024.

[16] APOSTOLICAS, Paul. Silicon States: How Tech Titans are Acquiring State-like Powers. *Harvard international review*, aug./2018. Available at: https://hir.harvard.edu/silicon-states-big-tech/. Accessed on: March 15, 2024.

[17] BREMMER, Ian. Why Big Tech companies are like "digital nation states". *Gzero*, oct./2021. Available at: https://www.gzeromedia.com/gzero-world-clips/why-big-tech-companies-are-like-digital-nation-states. Accessed on: March 15, 2024.

[18] CARREAU, Dominique. *État*. Répertoire de Droit International. Paris: Dalloz, 2010, §6-30.

of international law[19] and, as a sovereign power, it is the entity which naturally is responsible for the protection of human rights. Therefore, it is not surprising to encounter dispositions regarding such protection in constitutional norms. In France, this is especially the case with the DCHR, which has constitutional value, and in some provisions of the Constitution like in article 1. Whereas in Russia, human rights and freedoms are enshrined in Chapter 2 of the Russian Constitution entitled "Rights and Freedoms of Man and Citizen". However, protection of human rights can also be found at the international level. For instance, multiple human rights are enshrined in the ECHR and in EU law, for example, in the CFR, TFUE or the Treaty on the European Union (TEU). Nevertheless, international law is always based on states' consent, which make them the primary source of human rights.

The question raised by this article comes from the observation that IT Giants are today often compared to "Digital States". Some scholars have drawn the comparison of IT Giants directly to the definition of a state. First, it is emphasized that they have the power to create quasi-laws. Then, their users are identified as their population.[20] But the criteria of their territory as not having been explored can be explained in two ways. First, IT Giants provide their services almost world-wide, and secondly, because the relationship between the state and its territory is nowadays very stretched. Indeed, a number of laws and regulations have extraterritorial application,[21] for example, as is the case for the GDPR, which can apply to companies located in third countries. Therefore, the extraterritoriality automatically weakens the criteria of the territory. The state can now outline its territory and exercise its authority abroad.

However, two objections can be raised against the qualification of IT Giants as Digital States, both of which refute the authors' hypothesis. The first objection is that the criteria of the territory might be weakened by extraterritoriality, but it still exists, nevertheless. The state is still defined by the exercise of public authority over a territory and a population which requires the definition and limitation of a specific territory. Therefore, IT Giants lack a major defining element to be qualified as such. The second objection is that they might enact regulations applying to their users, but it is limited to very specific topics in relation to their services. For example, one cannot imagine Google locking up criminals (though it may contribute to it). The company clearly has no power to do so, even for digital crimes. Also, they do not

19 DUPUY, Pierre-Marie; KERBRAT, Yann. *Droit International Public*. 15. ed. Paris: Dalloz, 2020, p. 31.

20 DMITRIK, Nikolay. Digital State, Digital Citizen: Making Fair and Effective Rules for a Digital World. *Legal Issues in the Digital Age*, vol.1, n.1, p 54-78, jan./mar 2020, p.70.

21 DMITRIK, Nikolay. Digital State, Digital Citizen: Making Fair and Effective Rules for a Digital World. *Legal Issues in the Digital Age*, vol.1, n.1, p 54-78, jan./mar 2020, p. 65, 66.

have a general public power equivalent to the one states have. States can even oblige IT Giants to protect some liberties as is the case, for instance, in the GDPR for data protection. This being said, there are still some good arguments in favor of the qualification of "Digital States" in analyzing relevant laws and regulations.

Thus, IT Giants present only some elements of traditional states. This is why, when referring to "Digital States", one has to understand the limits of the expression compared to a regular or traditional state. Digital States do not have a territory, this is even one of their main features: they are by nature nonterritorial. Also, their power is limited to what is necessary to regulate their activity. Therefore, they partially assume the functions of a real state but are not its exact equivalent. The term "Digital States" should be understood within this specific context.

4 Review of the regulation of human rights in states and Digital States

4.1 Legislative comparison of states' regulations

In an era where the digital domain profoundly influences societal dynamics, the discourse surrounding human rights within this virtual space takes on paramount importance. The protection and assertion of these rights within the European Union, exemplified by France, and Russia, present an intriguing juxtaposition of legal frameworks and regulatory approaches. The European Union, with France as a member, predicates its data protection protocols on the GDPR, a comprehensive legislative act that safeguards personal data and facilitates its free movement. This regulation epitomizes the EU's commitment to upholding individuals' rights to data privacy, access, rectification, and erasure, embodying a uniform standard across member states.

Conversely, Russia's approach, encapsulated in the Federal Law "On Personal Data", underscores a more localized perspective, emphasizing the constitutional rights and freedoms of its citizens. This legislation delineates the parameters for personal data processing, rights to access, correction, and deletion of data, reflecting a nuanced balance between personal privacy and the state's regulatory interests. Additionally, Russia's Law on the Right to Oblivion introduces an interesting dimension to the discourse on human rights in the digital space, allowing individuals to request the removal of personal information from search engines without proving its illegality.

Both jurisdictions articulate mechanisms for the cross-border transfer of personal data, albeit with differing emphases on adequacy levels and safeguard provisions. The

European Union's Digital Services Act (DSA) and Russia's proactive stance against internet censorship and misinformation further illustrate the divergent pathways adopted by these entities in navigating the complexities of digital governance.

The examination of these legal frameworks below reveals a fundamental endeavor to reconcile the free flow of information with the imperative of protecting personal data and ensuring a safe digital environment. While the EU and Russia adopt distinct approaches reflective of their unique legal and cultural milieus, the underlying pursuit of human rights in digital space protection remains a common thread. This exploration not only underscores the challenges inherent in human rights in the digital space governance but also highlights the dynamic interplay between legal norms, technological advancements, and human rights imperatives in shaping the contours of our digital existence.

So, France is a member of the European Union, and in the field of data rights, most rules come from European documents. This is why one has to explore EU legislation in order to understand how data is protected in France.

Personal data protection in the EU is mainly regulated by Regulation No. 2016/679 dated April 27, 2016 regarding the protection of individuals with regard to the processing of personal data and on the free movement of such data (referred to as the General Data Protection Regulation, GDPR). The purpose of this document is to "establish rules concerning the protection of natural persons with regard to the processing of personal data and rules concerning the free movement of personal data".[22] It should be noted that this regulation is binding in its entirety and directly applicable to and in all Member States.[23] As a result, all of the rules are in force in the national legislation of all Member States.

With respect to the rights of data subjects (users) under the GDPR, users must have access to transparent and clear information; be informed as to where personal data is collected; have access to the personal data collected; and obtain rectification without undue delay of inaccurate personal data. They may also obtain the deletion of personal data without undue delay where the data is no longer needed in connection with the purposes for which it was initially collected; or if the user has subsequently withdrawn their consent; or the data has been unlawfully processed; the data must be erased to comply with a legal obligation under Union law or the

[22] Article 1(1), EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[23] Article 288, Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal* C 326, 26/10/2012 P. 0001-0390.

law of the Member State to which the controller is subject. Users also have the right to object to the processing of personal data at any time.[24]

In addition, individuals have the right to be forgotten, that is, to be removed from the search engine list. Indeed, in 2014, the European Court ruled that "the search engine operator is obliged to remove from the list of results displayed after a search on a person's name links to web pages published by third parties and containing information relating to that person, also in cases where that name or information is not previously or simultaneously removed from those web pages, and even, as the case may be, where their publication on those pages is itself lawful".[25] Shortly after this decision, a case was brought in France in which the authority ordered Google to remove links relating to one person worldwide. However, the company only removed them from its European domain, resulting in a fine of €100,000. A preliminary ruling was then referred to the European Court of Justice to ascertain the territorial scope of such removal. The ECJ clarified that the deletion could only apply to a version of the search engine available within the EU. This decision ultimately led to the annulment of the fine by the French Council of State.

Curiously, a year later, in 2015, Russia adopted the so-called Law on the Right to Oblivion. Under the provisions of the Law, every citizen may request that the search engine operator remove information about him/her and, most importantly, there is no need to prove the unlawfulness of the use of personal data. The applicant may request the deletion of the following information: disseminated in violation of Russian law, unreliable, irrelevant, or no longer relevant to the applicant due to subsequent events or actions of the applicant. An exception is information regarding events that contain indications of criminal offences for which the time limit for criminal prosecution has not expired, as well as information about the commission of a crime by a citizen for which the criminal record has not been expunged or cancelled.

As regards the transfer of personal data to third countries or international organizations, this is possible only if the European Commission has declared that those countries or organizations provide an adequate level of protection.[26] However, in the absence of such a decision, personal data can still be transferred to third

[24] Articles 12, 13, 15, 16, 17 (1), 21, EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[25] EUROPEAN UNION. Tribunal de Justicia de la Unión Europea. Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos y Mario Costeja González, C-131/12, 2014.

[26] Article 45(1), EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

countries if appropriate safeguards have been given to ensure that data subjects have rights and effective remedies.[27]

On the other hand, in Russia, where national and transnational IT Giants have been established, Federal Law No. 152-FZ dated July 27, 2006, entitled "On Personal Data",[28] takes center stage in the legal regulation of personal data protection. This law is aimed at implementing the provisions of the Constitution of the Russian Federation that enshrine the rights and freedoms of citizens: the prohibition of collecting, storing, using and disseminating information about the private life of individuals without their consent; and the obligation of public and local authorities and their officials of providing everyone with access to the documents and materials directly affecting their rights and freedoms.[29] Under Article 2 of the Act, the aim is to protect human and civil rights and freedoms in the processing of personal data, including the protection of the rights to privacy and to personal and family secrets. With regard to the rights of the data subject, he or she has the right to access his or her personal data, to have them corrected, blocked, or destroyed if the personal data is incomplete, outdated, inaccurate, has been illegally obtained or is no longer necessary for the stated purpose of processing. The Law also sets out the conditions for processing. The Law sets out certain requirements for consent to the processing of personal data. The subject of personal data decides whether to provide his or her personal data and consents to the processing freely, of his or her own free will, and in his or her own interests.[30]

Like the GDPR, the Federal Law on Personal Data defines the procedure for cross-border transfer of personal data, which means the transfer of personal data to a foreign authority, a foreign person, or a foreign legal entity. At the same time, the burden of responsibility for the protection of the user's personal data rests with the foreign country to which such data has been transferred.

On the 15th of December 2020, the European Commission also published a proposal for a Regulation of the European Parliament and of the Council on the Single Market for Digital Services (Digital Services Act, DSA) amending Directive 2000/31/EC. The main reason for this proposal was that, since the adoption of the

27 Article 46(1), EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

28 RUSSIA. Federal Law No. 152-FZ dated July 27, 2006. On Personal Data. Available at: http://www.kremlin.ru/acts/bank/24154. Accessed on: March 15, 2024.

29 Article 24, RUSSIA. Constitution of the Russian Federation, 1993. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102027595. Accessed on: March 15, 2024.

30 Articles 2, 14, 6, 9, RUSSIA. Federal Law No. 152-FZ dated July 27, 2006. On Personal Data. Available at: http://www.kremlin.ru/acts/bank/24154. Accessed on: March 15, 2024.

E-Commerce Directive in 2000, digital services have changed profoundly and taken a more important place in society, creating new risks for individuals.

Nowadays the DSA seeks to establish a safer online environment within the EU by introducing regulations to enhance consumer protection and fundamental rights, specify online platforms and social media responsibilities, address illegal content, hate speech, and disinformation, and promote transparency through improved reporting and oversight mechanisms. Additionally, the DSA aims to foster innovation, growth, and competitiveness within the EU's internal market. Hence the DSA "seeks to create a legislative infrastructure that facilitates the co-existence of fundamental rights and digital services".[31] And the document is an EU legal text of general application, binding in its entirety and directly applicable to and in all Member States.[32]

In the Russian Federation, legislation expressly forbids any propaganda or agitation that instigates social, racial, national, or religious hatred and enmity, alongside the promotion of superiority based on social, racial, national, religious, or linguistic grounds. According to the law referred to as "On the prohibition of censorship on Internet portals",[33] the regulatory authority (Roskomnadzor) possesses the power to partially or fully restrict access to internet resources that hinder the dissemination of vital information across the Russian territory based on nationality, language, origin, property and official status, occupation, location of residence and work, religious views, or in response to the implementation of political or economic sanctions by foreign nations against the Russian Federation or its citizens. This law also encompasses measures against the discriminatory treatment of Russian media materials.

Internet resources found contravening this legislation are added to a specific registry identifying websites that infringe upon "fundamental human rights and freedoms, as well as the rights and freedoms of citizens of the Russian Federation".[34] Consequently, numerous resources have faced blocks within Russia for violating this

[31] TURILLAZZI, Aina; TADDEO, Mariarosaria; FLORIDI, Luciano; CASOLARI, Federico. The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, [s.l.], vol. 15, n. 1, p. 83-106, jan./jun. 2023, p. 100. DOI: 10.1080/17579961.2023.2184136.

[32] Article 288, Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal* C 326, 26/10/2012, P. 0001-0390.

[33] RUSSIA. Federal Law No. 482-FZ dated December 30, 2020. Concerning the Introduction of Amendments to the Federal Law 'On Measures to Exert Influence on Persons Involved in Violations of Fundamental Human Rights and Freedoms, Rights and Freedoms of Citizens of the Russian Federation. Available at: http://publication.pravo.gov.ru/Document/View/0001202012300002?index=1. Accessed on: March 15, 2024.

[34] ROSKOMNADZOR. List of owners of resources on the Internet that violate the rights of citizens of the Russian Federation. Available at: https://new.rkn.gov.ru/activity/electronic-communications/rights-violation/. Accessed on: March 15, 2024.

regulation, especially in the context of discrimination. Notably, since the escalation of conflict in Ukraine, the number of blocked resources has surged, leading to the prohibition of platforms such as Facebook and Instagram, with Twitter and YouTube receiving notifications regarding impending restrictions.

As regards freedom of expression, it may be restricted in the case of illegal content, which is any information that does not comply with the legislation of the EU or a Member State. Intermediary service providers must remove such content when ordered to do so by either a national judicial or administrative body.[35] This encompasses decisions related to the removal or restriction of access to information, suspension or termination of services, and the suspension or closure of user accounts. Online platforms are obligated to temporarily suspend users who frequently disseminate overtly illegal content after issuing a prior warning. The same regulation applies to users who habitually lodge baseless complaints.[36] In 2019, Russia enacted laws to combat the creation and dissemination of misinformation, specifically forbidding the circulation of information online that could threaten public health or safety, disrupt public order, or endanger critical infrastructure and communication systems.[37] The COVID-19 pandemic highlighted the urgency of regulating false information, leading to the introduction of the additional articles to the Criminal Code of the Russian Federation targeting the spread of knowingly false information that endangers public safety or causes severe consequences.[38]

In Russia, social media regulation forms a crucial part of safeguarding freedom of speech. The regulation is based on the Information Law,[39] which imposes specific

---

35 Article 8(1), EUROPEAN UNION. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj. Accessed on: March 15, 2024.

36 Article 20 (1,2), EUROPEAN UNION. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj. Accessed on: March 15, 2024.

37 RUSSIA. Federal Law No. 31-FZ dated March 18, 2019. On Amendments to Article 15-3 of the Federal Law "On Information, Information Technologies and Information Protection". Available at: http://publication.pravo.gov.ru/Document/View/0001201903180031?index=1. Accessed on: March 15, 2024; RUSSIA. Federal Law No. 27-FZ dated March 18, 2019. On Amendments to the Code of Administrative Offences of the Russian Federation. Available at: http://publication.pravo.gov.ru/Document/View/0001201903180021. Accessed on: March 15, 2024.

38 Article 207.1 ("Public dissemination of knowingly false information about circumstances endangering the life and security of citizens") and Article 207.2 ("Public dissemination of knowingly false information of public significance resulting in grave consequences"), RUSSIA. Criminal Code of the Russian Federation dated June 13, 1996. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891&ysclid=luf wxu4tyg475564034. Accessed on: March 15, 2024.

39 RUSSIA. Federal Law No. 149- FZ dated July 27, 2006. On Information, Information Technologies, and Information Protection. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264. Accessed on: March 15, 2024.

duties on social network owners to identify and block prohibited content. Notably, Google and Meta Platforms were fined for failing to remove banned content, marking the first instances of turnover fines for non-compliance with content removal laws.[40] These fines reflect Russia's commitment to creating a safe online environment for its users, emphasizing government priorities.

The right to nondiscrimination mandates that data revealing racial origin, political views, religious or philosophical beliefs must not be processed as stated in GDPR.[41] In Russia, nondiscrimination is governed by the Constitution[42] and the "Law on the Prohibition of Censorship on Internet Portals",[43] allowing relevant authority (Roskomnadzor) to restrict internet portals.

Additionally, the right to internet access is recognized as crucial for participating in democratic processes and expressing ideas, with the Constitutional Council affirming this right in 2009.[44]

In the EU, and by extension in France, the Internet is deemed a universal service under Directive (EU) 2018/1972,[45] ensuring accessibility across Member Sstates at an affordable price. This directive aims to facilitate internet access. Meanwhile, in Russia, the right to internet access is defined by the Federal Law "On Communications",[46] which serves as the primary legal framework for internet access on the sustainable, secure, and comprehensive operation of the Internet in the Russian Federation.

---

40 Russia fines Google £73m over failure to delete 'illegal' content. *The Guardian,* dec./2021. Available at: https://www.theguardian.com/world/2021/dec/24/russia-fines-google-failure-delete-content. Accessed on: March 15, 2024.

41 Article 9, EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

42 Article 29 (2), RUSSIA. Constitution of the Russian Federation, 1993. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102027595. Accessed on: March 15, 2024.

43 RUSSIA. Federal Law No. 482-FZ dated December 30, 2020. Concerning the Introduction of Amendments to the Federal Law 'On Measures to Exert Influence on Persons Involved in Violations of Fundamental Human Rights and Freedoms, Rights and Freedoms of Citizens of the Russian Federation. Available at: http://publication.pravo.gov.ru/Document/View/0001202012300002?index=1. Accessed on: March 15, 2024.

44 FRANCE. The Constitutional Council. Decision no. 2009-580 DC of 10 June 2009. Available at: https://www.conseil-constitutionnel.fr/en/decision/2009/2009580DC.htm. Accessed on: March 15, 2024; Internet access is a fundamental human right, rules French court. *Mail Online*, jun./2009. Available at: https://www.dailymail.co.uk/news/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html. Accessed on: March 15, 2024.

45 Preambula (212), Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

46 Chapter 7.1 ("Ensuring Sustainable, Secure and Comprehensive Functioning of the Information and Telecommunications Network "Internet" in the Russian Federation"). RUSSIA. Federal Law No. 27-FZ dated July 7, 2003. On communications. Available at: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102082548. Accessed on: March 15, 2024.

According to the abovementioned, digital space is an environment created by IT companies and users, which is loosely regulated by law. Public content is created by users at their own discretion, so in order to ensure the safety of users and preserve generally recognized human values lawmakers are moving towards imposing various restrictions.

It follows from these provisions that IT Giants (especially the social network ones) should, at the same time, ensure, for example, freedom of expression, but should also be responsible for eliminating excesses in its use.

Comparing how human rights in digital space are ensured by states reveals that they face similar questions even if they do not necessarily find the same answers to them. Different degrees of control can be found, but in general, the same rights are protected in a similar way. However, as we stated earlier, IT Giants can also intervene in matters related to their services, and are, therefore, qualified as "Digital States". The question that arises is how they deal with human rights. It is interesting to explore whether they have the same pattern as regular states and protect the same rights or, on the contrary, whether they perhaps have a totally different way to regulate human rights of their users. Comparing the IT Giants is the key to answering this question.

4.2 Legislative comparison of Digital States' regulation

Digital States have their own rules which can be drawn from their terms and policies. These documents aim at regulating the use of their services. For this purpose, they afford protection for some rights in the same manner as states' regulations. To access their services, one must agree with their terms, conditions, and policies, and abide by them. A comparison between these documents reveals the differences between the ways that these Digital States envision fundamental rights and enforce them. One can see that every one of these companies took a position on this question which underlines the importance of the protection of fundamental rights. It also shows that states are not the only entities that pursue their effectiveness. As such, Digital States seem to bear the same task as regular states. It is a solid argument in favor of the relevance of their comparison. But first, the comparison between the policies of Digital States must be undertaken. Moreover, due to differences in territorial coverage, it is also interesting to compare the regulation of human rights by US IT companies as global IT Giants and by their counterparts, which are large and powerful, but operate mainly within the territory of one country. That is why it was chosen here to compare the main US IT Giants present in the European market and their equivalents operating mainly in Russia, in pairs.

4.2.1 Google vs. Yandex

Google and Yandex are technology companies that specialize in Internet-related services and products, which include a search engine, online advertising technologies, cloud computing, software, and hardware. Both companies have an enormous turnover of customer personal data. And the IT Giants ensure that shared personal data is protected.

Regarding the privacy of personal data, Google provides an explicit provision on the information that can be collected, such as search terms, watched videos, views and interaction with content and ads, voice and audio information, purchase activity, people communicated with or shared content with, and many others. Also, which technologies are used for personal data collection is emphasized (for example, cookies, pixel tags, local storage, databases, and server logs).[47] In comparison, Yandex privacy policies set out mainly procedural provisions such as informing users regarding implementing sufficient technical and organizational measures to protect Personal Information from unauthorized, accidental, or illegal destruction, loss, alteration, unfair use, disclosure or access, as well as other illegal forms of processing.[48]

As for the freedom of speech, Google refers to the laws in force and protects any violation such as abuse or harm to others or oneself, and interfering with or disrupting the service.[49] In turn, Yandex also refers to applicable laws and regulations, but specifies that the user shall be solely responsible as to the content posted by the user for compliance with the requirements of applicable law, including liability to third parties in cases where the user's posting of particular content violates the rights and legitimate interests of third parties, including personal non-property rights of authors, other intellectual rights of third parties, and/or infringes on their own intangible benefits.[50]

In reference to the right to access one's personal information, the right to rectification of personal data, and the right to be forgotten, Google establishes provisions applicable to US laws and regulations as well as special provisions for

47 Section "Information Google collects", GOOGLE. Privacy Policy. Available at: https://policies.google.com/privacy?hl=en-US. Accessed on: March 26, 2024.

48 Clause 6, YANDEX. Privacy Policy. Available at: https://yandex.com/legal/confidential/. Accessed on: March 26, 2024.

49 Section "What we expect from you". GOOGLE. Terms of Service. Available at: https://policies.google.com/terms?hl=en-US. Accessed on: March 26, 2024.

50 Clause 4.1, YANDEX. User Agreement. Available at: https://yandex.ru/legal/rules/. Accessed on: March 26, 2024.

the EU Member States.[51] This might be due to the fact that strict EU regulations in the General Data Protection Regulation (GDPR) are more limiting in terms of the ways personal data can be used in Europe when compared with the US. Yandex also explicitly contains provisions for protecting user's rights from violation and restricts violation in accordance with national laws and regulations.[52]

Referring to the access to true and accurate information, Google is not considering any such provision in their privacy policies, whereas Yandex has enshrined in its policies an indemnity clause that Yandex services may contain links to other sites on the Internet (sites of third parties). Such third parties and their content are not checked or verified by Yandex for compliance with any requirements (reliability, completeness, legality, etc.).[53] This provision eliminates liability for incorrect information in third-party sources and protects the company more than the user.

As for the right to access the service (equivalent to the right to Internet access protected by real states), both of these IT Giants provide a clause that the company can suspend or terminate access to its services if the user materially and repeatedly breaches the terms and conditions of its services and policies.[54]

A nondiscrimination provision is not enshrined in either Google or in Yandex policies.

4.2.2 WhatsApp vs. Telegram

WhatsApp and Telegram are both messenger applications. The former is one belonging to the Meta companies, while the latter is an independent IT company created by the Durov brothers for safe and secure communication. Despite the fact that the company is officially registered in the British Virgin Islands, and the company's headquarters is located in Dubai, this giant is considered Russian.

As for the privacy of personal data, it should be mentioned that in 2021, WhatsApp announced changes to its privacy policies that led to a significant drop

51 GOOGLE. Privacy Policy. Available at: https://policies.google.com/privacy?hl=en-US. Accessed on: March 26, 2024; Google.

52 Clause 10. YANDEX. Privacy Policy. Available at: https://yandex.ru/legal/confidential/index.html. Accessed on: March 26, 2024.

53 Clause 7.1. YANDEX. User Agreement. Available at: https://yandex.ru/legal/rules/. Accessed on: March 26, 2024.

54 Section "Your relationship with Google", GOOGLE. Terms of Service. Available at: https://policies.google.com/terms?hl=en-US. Last accessed on: March 26, 2024;

Clause 3.1, YANDEX. User Agreement. Available at: https://yandex.ru/legal/rules/. Accessed on: March 26, 2024.

in the number of its users.[55] The main reason therefore was that they began sharing user information with all companies of the Meta family. Such information includes, but is not limited to, language, time zone, IP address, battery and signal strength information, as well as browser data and other information. The information collected depends on the users' settings. Also, within the framework of international activities, the user's personal data may be transferred to and stored on the territory of completely different countries, where the provisions regarding its confidentiality may differ dramatically.

In general, it should be noted that the policies of Telegram are quite capacious and make it clear that the primary strong point of this platform is the privacy of user data, and it is for good reason then that it has been repeatedly blocked for being closed and unwilling to share its user data with anyone, and also for refusing to transfer encryption keys to state authorities.[56]

Unlike WhatsApp, Telegram doesn't use personal data for ad targeting or other commercial purposes.[57]

In regard to the freedom of speech of their users, both WhatsApp and Telegram regulate it by establishing some restrictions in their Policies and Terms of Services. So, WhatsApp policy contains provisions according to which its services can be used only for legal, authorized, and acceptable purposes. The user is prohibited from using (or assisting others in using) the services in ways that: violate, misappropriate, or infringe the rights of WhatsApp users or others, including privacy, publicity, intellectual property, or other proprietary rights; are illegal, obscene, defamatory, threatening, intimidating, harassing, hateful, racially or ethnically offensive, or instigate or encourage conduct that would be illegal or otherwise inappropriate, such as promoting violent crimes, endangering or exploiting children or others, or coordinating harm to others; involve publishing falsehoods, misrepresentations, or misleading statements; impersonate someone; involve sending illegal or impermissible communications, such as bulk messaging, auto-messaging, auto-dialing, and the like.[58] As for Telegram, it has established in the provisions of its Terms of Services that, by signing up for Telegram, the user accepts its Privacy Policy and agrees not to: use Telegram services to send spam or scam users; promote violence on

[55] WhatsApp to try again to change privacy policy in mid-May. *Guardian*, Feb. 2021. Available at: https://www.theguardian.com/technology/2021/feb/22/whatsapp-to-try-again-to-change-privacy-policy-in-mid-may. Accessed on: March 26, 2024.

[56] Clause 4. "Keeping your personal data safe", TELEGRAM. Privacy Policy. Available at: https://telegramapp.github.io/privacy.html. Accessed on: March 26, 2024.

[57] Clause 5.6. "No Ads Based on User Data", TELEGRAM. Privacy Policy. Available at: https://telegramapp.github.io/privacy.html. Accessed on: March 26, 2024.

[58] Section "Acceptance use of our services". WHATSAPP. Terms of Service. Available at: https://www.whatsapp.com/legal/terms-of-service-eea/preview. Accessed on: March 26, 2024.

publicly viewable Telegram channels, bots, etc.; post illegal pornographic content on publicly viewable Telegram channels, bots, etc.[59]

As for the right to access one's personal data, it is enshrined in the policies of both of these messengers. WhatsApp users can access information about themselves using its in-app Request Account Info feature.[60] Telegram users have the right to: request a copy of all personal data held by Telegram and to give that copy to another data controller.[61]

Regarding the right to rectification of personal data, WhatsApp gives its users the ability to change their mobile phone number, profile name and picture, and "About" Information. Telegram also allows its users to "correct any inaccurate or incomplete personal data that Telegram has about them".

Both messengers provide their users with the option of deleting their accounts. That is how the right to be forgotten is implemented. However, it is important to note that only in Telegram can users completely delete all sent and received messages from chats for both participants,[62] which, of course, provides the possibility of exercising the right to be forgotten on a wider scale.

Referring to the access to true and accurate information, only WhatsApp policies contain provisions on not being responsible for the accuracy of the information, while that issue is not addressed at all in Telegram's provisions.

As for the right to access the service, both WhatsApp and Telegram provide for the possibility of partial access restriction or even complete blocking of users' accounts. WhatsApp can disable or suspend one's account in the case of violation of its terms and policies.[63] Telegram can temporarily or permanently block the accounts of its users to prevent phishing, spamming, and other kinds of abuse, as well as violations of Telegram's Terms of Service.[64]

Nondiscrimination provisions are directly provided for only in WhatsApp Policy: WhatsApp users cannot use (or assist others in using) the services in ways that are racially or ethnically offensive.[65]

---

59 Telegram. Terms of Service. Available at: https://telegramapp.github.io/tos.html. Accessed on: March 26, 2024.

60 Section "Managing And Retaining Your Information". WHATSAPP. Privacy Policy. Available at: https://www.whatsapp.com/legal/privacy-policy-eea. Accessed on: March 26, 2024.

61 Clause 9. "Your Rights Regarding the Personal Data You Provide to Us", TELEGRAM. Privacy Policy. Available at: https://telegramapp.github.io/privacy.html. Accessed on: March 26, 2024.

62 Clause 10. "Deleting data", TELEGRAM. Privacy Policy. Available at: https://telegramapp.github.io/privacy.html. Accessed on: March 26, 2024.

63 Section "Acceptance use of our services". WHATSAPP. Terms of Service. Available at: https://www.whatsapp.com/legal/terms-of-service-eea/preview. Accessed on: March 26, 2024.

64 Clause 5.3. "Spam and Abuse" TELEGRAM. Privacy Policy. Available at: https://telegramapp.github.io/privacy.html. Accessed on: March 26, 2024.

65 Section "Acceptance use of our services". WHATSAPP. Terms of Service. Available at: https://www.whatsapp.com/legal/terms-of-service-eea/preview. Accessed on: March 26, 2024.

4.2.3 Facebook vs. VK

Facebook and VK are both social networks which allow their users to publish written posts and pictures of themselves or themselves with others.

Regarding the protection and privacy of personal data, Facebook's terms and policies are much more developed. Unlike VK, they disclose the purpose for which data is collected. The data is processed in order to provide personalized and improved products; to give feedback to partner websites about the effectiveness and efficiency of their advertisements; to enhance safety, integrity, and security; to communicate with users; and to conduct scientific research and innovation for the common good. They also vaguely indicate where the data is stored: in the United States or other countries.[66] This is not specified in VK's terms and policies, but since the company is Russian, one can suppose that the data is stored in Russia. Both companies indicate that data about one user can be disclosed by other users on the network, and that users can determine which level of protection they want. They collect data disclosed by the users themselves. In the case of Facebook, Meta company also collects information shared by partner websites using Meta Business Tools. VK specifies that data is processed using automated systems unless legal requirements prohibit it from doing so.[67] That is all for VK, whereas Facebook adds that data is not sold, and that no data identifying people is shared unless explicit consent is given. Also, data is stored until it is no longer necessary to provide services or until suppression of users' accounts.[68] Thus, it seems that Facebook possesses more requirements for the protection and privacy of personal data. It must be noted that this is the result of European law, which requires such companies to indicate the purpose of data collection, and the duration of their storage and use. This explains the difference with VK, whose requirements are much shorter.

Regarding freedom of speech, Facebook explicitly declares its protection. However, it also enumerates its limitations: forbidden are violence and inciting to violence; dangerous people and organizations; coordination of dangerous actions and promotion of criminal acts; fraud and deceit; commerce of psychoactive non-medical substances and of firearms; suicide and automatization; mistreatment, nudity, and sexual exploitation of children; violation of private life; hate speech; violent and explicit content; nudity and sexual activity for adults; sexual solicitation and discriminatory

[66] FACEBOOK. Privacy Policy. Available at: https://www.facebook.com/about/privacy. Accessed on: March 26, 2024.

[67] Clause 5.1.3, VK. Privacy Policy. Available at: https://vk.com/privacy. Accessed on: March 26, 2024.

[68] Section "How long do we store your information?" FACEBOOK. Privacy Policy. Available at: https://www.facebook.com/about/privacy. Accessed on: March 26, 2024.

content. Any violation of these standards can be suppressed or blocked, and users can report unauthorized content. In such cases, the author can ask for a second inquiry.[69] Regarding VK, if the company does not declare protection of freedom of speech, it indicates that it does not operate pre-moderation or censorship, although it might be seen as a close equivalent. However, regarding unauthorized content, VK's terms and policies are much vaguer. They only state that VK will take action to protect the rights and interests of individuals and ensure compliance with the laws of the Russian Federation only after the interested party has applied to the site's administration in the prescribed manner. Also, it prevents and suppresses violations of third-party rights to the results of intellectual activity.[70] Consequently, it is not clear which content is authorized or not unlike the case of Facebook. This can, at the same time, lead to either a stricter or more lenient regulation of speech. It is hard to compare the reality of the protection of freedom of speech between the two companies. One can only say that Facebook is more precise in defining unauthorized content whereas VK lacks transparency on this topic.

Regarding the right of access to personal data and the right to rectification of personal data, both VK and Facebook provide protections. On this topic, Facebook follows the GDPR rules. For the rectification of data, VK specifies that the data must be incomplete, outdated, unreliable, illegally obtained, or is not necessary for the stated purpose of processing.[71] It is thus stricter than Facebook, even if these characteristics of the data are implied when talking about "rectification". Only Facebook completely protects the right to be forgotten conferring upon users the right to suppress their data in any case. However, data shared by other users cannot be suppressed.[72] This is a result of the requirements of the GDPR. Facebook is thus a little bit more protective but, on these points, it is still very similar to VK's terms and policies. Both companies ensure a right to access the data and to rectify it. VK does not ensure entirely the right to be forgotten, but a user can still request that the company destroy his or her data per the same conditions as rectification.

Interestingly enough, only Facebook has provisions about the dissemination of fake news. Indeed, its terms and policies state that the company aims at limiting its

69 Section "Allowed content and allowed actions in Meta Products". FACEBOOK. User's Agreement. Available at: https://www.facebook.com/legal/terms. Accessed on: March 26, 2024.

70 Clause 7. "Terms and conditions on intellectual property rights". VK. User's Agreement. Available at: https://vk.com/terms. Accessed on: March 26, 2024.

71 Clause 6. "Rights and obligations of users". VK. Privacy Policy. Available at: https://vk.com/privacy. Accessed on: March 26, 2024.

72 Section "How can you manage or delete your information and exercise your rights?" FACEBOOK. Privacy Policy. Available at: https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 Accessed on: March 26, 2024.

dissemination in order to ensure the right to access true and accurate information. This also comes in a limitation to freedom of speech. VK has no provision about such things. In that sense, freedom of speech seems broader from its point of view.

Regarding the right to access the service, both Facebook and VK are very similar. Indeed, they have the right to suspend or suppress users' accounts. To justify such sanctions, Facebook invokes the violation of its terms and policies,[73] whereas VK talks about the case where the opinions of a user would present a threat to the site or other users.[74] The formulation is not the same, but looking at unauthorized content at Facebook, it is more or less the same result. Here again, VK is vaguer and broader, which can, at the same time, provide more protection for users or be more restrictive for freedom of speech depending on how the company enforces its policy. VK also specifies that in the case of deleting an account, there is a deletion of all of the user's information.[75]

Regarding nondiscrimination, interestingly, VK has no provision covering it. Only Facebook expressly mentions that discriminating content is forbidden, and accordingly, they can restrict freedom of speech. This is another sign of the broader approach of VK's terms and policies which relies on more general requirements than Facebook. This is also due to the application of the GDPR and DSA, which are quite precise in terms of obligations applying to operators such as Facebook. However, the difference between Facebook and VK is not broad and one can thus see that they generally protect the same rights for their users.

With the exception of a few features, one can see that the regulation of human rights by the IT Giants with worldwide user coverage, and by the IT Giants with mainly single country user coverage, is in many ways similar. Human rights are important and of particular interest, as evidenced by the presence of relevant provisions. However, it is important to note that policies and terms of use also contain a reference to the relevant jurisdiction regulation, for example, the EU, the USA, and Russia, respectively. And the provisions are quite general, although the provisions of the IT Giants with worldwide user coverage are still more detailed. It is likely that some of the differences that do exist in the regulation of human rights are due to differences in the national laws and legislation, and their greater or lesser severity in regulating a particular issue. It is also important to note that IT

[73] Section 4. "Additional provisions", FACEBOOK. User's Agreement. Available at: https://www.facebook.com/legal/terms. Accessed on: March 26, 2024.

[74] Clause 8. "Functioning of the VK Website and responsibility for its use", VK. User's Agreement. Available at: https://vk.com/terms. Accessed on: March 26, 2024.

[75] Clause 8.7 "Functioning of the VK Website and responsibility for its use", VK. User's Agreement. Available at: https://vk.com/terms. Accessed on: March 26, 2024

Giants with worldwide user coverage collect more data about their users, explaining this by citing user convenience, but in reality, it is for purposes of ad targeting. The most striking example is considered that of Meta Companies, that is, Facebook and WhatsApp. The regulation of freedom of speech and the right of access to true information is carried out not in the format of declaring and securing rights, which is typical for the constitutions of real states, but in the opposite format, by defining "what is prohibited" and which content is forbidden. By doing so IT Giants endorse the role of protector of rights and liberties as states would do. In fact, from this perspective, they act as Digital States defining which rights they will protect and to which extent this protection can be applied. However, the real states are never far since they can orchestrate the interventions of IT Giants by requiring them to protect some specific rights and liberties. As such, IT Giants are in fact semi-autonomous in this protective role highlighting the particular nature of digital states.

5 Conclusion

Throughout the rapid evolution of the World Wide Web, key entities have attained a level of influence comparable to that of sovereign states. The digital realm has evolved into a parallel dimension for a vast majority of the global population, with significant portions of individuals' lives being spent online. Initially, the pioneers of the internet focused on creating a technological marvel to enhance communication and data exchange, often overlooking the implications for security and the safeguarding of user rights. To ensure comprehensive protection for individuals in this digital environment, it is imperative to regulate human rights and freedoms appropriately.

The expansion of universally recognized human rights into the digital domain has introduced new interpretations and challenges. Fundamental rights requiring protection online include the privacy of personal data, freedom of speech, the right to access and rectify personal data, the right to be forgotten, access to accurate information, non-discrimination, and the right to internet access. These rights necessitate governance through the enactment of legal statutes, soft law norms, and local policy measures. The internet's history underscores the limitations of self-regulation, primarily because personal data – viewed as a valuable commodity by corporations – becomes a battleground for commercial interests, with IT companies deploying complex algorithms for data mining and targeted advertising, showing little inclination towards self-imposed restraint.

Legal frameworks and policy stipulations governing user rights, as analyzed in this context, emerge from state and international regulatory efforts aimed at curbing

the latitude of IT giants through legislative actions, ethic policies, and guidelines. The oversight of human rights by both global and local IT entities shows substantial uniformity with slight variations attributed to specific legal landscapes and their relative rigor in addressing certain issues. However, these regulatory provisions remain broadly defined, lacking in specificity and clarity regarding offenses, accountability mechanisms, and human rights protection measures.

Users find themselves at the discretion of IT Giants, which unilaterally determine restrictions on user rights, including partial or complete blocking, effectively isolating individuals digitally to an extent akin to imprisonment or "digital death". In contrast, democratic legal systems detail the prerequisites for such punitive measures, emphasizing judicial intervention and due process – elements conspicuously absent in the digital governance by IT Giants.

Thus, while IT Giants, or "Digital States", operate as transnational corporations devoid of physical territories, embodying some state-like characteristics, their capacity to govern is inherently limited to their operational needs. They undertake some state-like functions but cannot be considered full equivalents, particularly in safeguarding human rights within the digital sphere. The term "Digital States" thus requires a nuanced understanding of its limitations and the provisional nature of its applicability. In addition, it should be mentioned that the EU is advanced in protecting human rights. France, as a member of the European Union, has been and is very active in addressing issues related to the protection of human rights in digital space and participating in the discussion of a number of issues at the sites of various organizations. Its approach to regulating the activities of global IT Giants within its territory with the use of tax measures is also highlighted. Comparing how human rights in digital space are ensured by the European Union, and in particular by France, and by a non-EU state that has its own IT Giants, in particular, by the Russian Federation, we can draw the conclusion that different degrees of control can be found, but in general, the same rights are protected in a similar legal manner.

It is quite obvious that, in view of the impossibility of self-regulation of digital space already indicated above, the key role should be played by regulations implemented by real states and international organizations. While IT Giants may operate globally, they are bound by local laws that protect personal data. This presents a dual challenge to such entities: to adjust their global data practices to local legal realities and to engage with national regulatory authorities that are increasingly empowered to enforce data protection laws. This legal evolution reflects a growing international trend towards asserting national sovereignty over personal data and curbing the unfettered influence of IT Giants in the digital ecosystem.

In this case, one could take as a basis, for example, the model of the European Union, where normative acts, obligatory for all members, are adopted centrally and national legislation is then brought into line with them. A unified global regulation of digital space could solve the problem of the extraterritoriality of the Digital States. But if one can argue about the expediency and possibility of a single all-Internet code, then there is definitely no doubt about the very need to regulate the protection of human rights in digital space.

References

ÁLVAREZ ROBLES, Tamara. Las garantías de los derechos fundamentales en y desde la red: el contexto español. *Revista Chilena de Derecho Y Tecnología*, [s.l.] vol. 11, n. 1, p. 5-40, jan./mar 2022.

APOSTOLICAS, Paul. Silicon States: How Tech Titans are Acquiring State-like Powers. *Harvard international review*, aug. 2018. Available at: https://hir.harvard.edu/silicon-states-big-tech/ – Accessed on: March 15, 2024.

BELLOCCHIO, Lucía; SANTIAGO, Alfonso. Estado digital de Derecho. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 20, n. 80, p. 87-102, abr./jun. 2020.

BREMMER, Ian. Why Big Tech companies are like "digital nation states". *Gzero*, oct. 2021. Available at: https://www.gzeromedia.com/gzero-world-clips/why-big-tech-companies-are-like-digital-nation-states. Accessed on: March 15, 2024.

BUSTAMANTE DONAS, Javier. Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica. *Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación,* [s.l.], n.1, jan./mar. 2001.

CARREAU, Dominique. *État*. Répertoire de Droit International. Paris: Dalloz, 2010.

CERF, Vinton G. Internet access is not a human right. *The New York Times*, jan. 2012. Available at: https://nyti.ms/3FWWArK. Accessed on: March 15, 2024.

COCCOLI, Jacopo. The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era. *Peace Human Rights Governance*, Padova, vol. 1, n. 2, p. 223-250, 2017. DOI: 10.14658/PUPJ-PHRG-2017-2-4.

CONSOLIDATED version of the Treaty on the Functioning of the European Union. Official Journal C 326, 26/10/2012. P. 0001-0390.

DIRECTIVE (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

DMITRIK, Nikolay. Digital State, Digital Citizen: Making Fair and Effective Rules for a Digital World. *Legal Issues in the Digital Age*, vol.1, n.1, p 54-78, jan./mar. 2020.

DUPUY, Pierre-Marie; KERBRAT, Yann. *Droit International Public*. 15. ed. Paris: Dalloz, 2020.

EUROPEAN UNION. *EU Charter of Fundamental Rights*. Available at: https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data#:~:text=Article%2010%20(3)%20Everyone%20has,misuse%20of%20her%20personal%20data. Accessed on: March 15, 2024.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

EUROPEAN UNION. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj. Accessed on: March 15, 2024.

EUROPEAN UNION. Tribunal de Justicia de la Unión Europea. Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos y Mario Costeja González, C-131/12, 2014.

FACEBOOK unveils global digital coin called Libra. *Financial Times*, jun. 2019. Available at: https://www.ft.com/content/af6b1d48-90cc-11e9-aea1-2b1d33ac3271. Accessed on: March 15, 2024.

FACEBOOK. *Privacy Policy*. Available at: https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 Accessed on: March 26, 2024.

FACEBOOK. *User's Agreement.* Available at: https://www.facebook.com/legal/terms. Accessed on: March 26, 2024.

FLORIDI, Luciano. The Fourth Revolution: How the Infosphere Is Reshaping Human Reality. Oxford: Oxford University Press, 2014.

FRANCE. The Constitutional Council. *Decision no. 2009-580 DC of 10 June 2009*. Available at: https://www.conseil-constitutionnel.fr/en/decision/2009/2009580DC.htm. Accessed on: March 15, 2024.

GOOGLE. *Terms of Service.* Available at: https://policies.google.com/terms?hl=en-US. Last accessed on: March 26, 2024.

GOOGLE. *Privacy Policy.* Available at: https://policies.google.com/privacy?hl=en-US. Accessed on: March 26, 2024.

INTERNET access is a fundamental human right, rules French court. *Mail Online*, jun./2009. Available at: https://www.dailymail.co.uk/news/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html Accessed on: March 15, 2024.

PÉREZ DE LA FUENTE, Oscar. How can the internet change human rights on online hate speech regulations? In: SUNGUROV, Alexander (coord.); FERNÁNDEZ LIESA, Carlos Ramón (coord.); BARRANCO AVILÉS, María del Carmen (coord.); LLAMAZARES CALZADILLA, María Cruz (coord.); PÉREZ DE LA FUENTE, Óscar (coord.). *Current Issues on Human Rights*. Madrid: Dykinson, 2020. p. 93-104.

ROSKOMNADZOR. *List of owners of resources on the Internet that violate the rights of citizens of the Russian Federation*. Available at: https://new.rkn.gov.ru/activity/electronic-communications/rights-violation/. Accessed on: March 15, 2024.

RUSSIA fines Google £73m over failure to delete 'illegal' content. *The Guardian,* dec. 2021. Available at: https://www.theguardian.com/world/2021/dec/24/russia-fines-google-failure-delete-content. Accessed on: March 15, 2024.

RUSSIA. *Constitution of the Russian Federation*, 1993. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102027595. Accessed on: March 15, 2024.

RUSSIA. *Federal Law No. 149- FZ dated July 27, 2006.* On Information, Information Technologies, and Information Protection. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264. Accessed on: March 15, 2024.

RUSSIA. *Federal Law No. 152-FZ dated July 27, 2006.* On Personal Data. Available at: http://www.kremlin.ru/acts/bank/24154. Accessed on: March 15, 2024.

RUSSIA. *Federal Law No. 27-FZ dated July 7, 2003.* On communications. Available at: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102082548. Accessed on: March 15, 2024.

RUSSIA. *Federal Law No. 27-FZ dated March 18, 2019*. On Amendments to the Code of Administrative Offences of the Russian Federation. Available at: http://publication.pravo.gov.ru/Document/View/0001201903180021. Accessed on: March 15, 2024.

RUSSIA. *Federal Law No. 31-FZ dated March 18, 2019*. On Amendments to Article 15-3 of the Federal Law "On Information, Information Technologies and Information Protection". Available at: http://publication.pravo.gov.ru/Document/View/0001201903180031?index=1. Accessed on: March 15, 2024.

RUSSIA. *Federal Law No. 482-FZ dated December 30, 2020*. Concerning the Introduction of Amendments to the Federal Law 'On Measures to Exert Influence on Persons Involved in Violations of Fundamental Human Rights and Freedoms, Rights and Freedoms of Citizens of the Russian Federation. Available at: http://publication.pravo.gov.ru/Document/View/0001202012300002?index=1 Accessed on: March 15, 2024.

RUSSIA. *Criminal Code of the Russian Federation dated June 13, 1996*. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891&ysclid=lufwxu4tyg475564034. Accessed on: March 15, 2024.

STATISTA. *Biggest Companies in the World by Market Cap 2023*. Available at: https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/. Accessed on: March 15, 2024.

SUSI, Mart. The image of human rights in e-state. *Journal of the Belarusian State University. International Relations*, [s.l.], vol.20, n. 1, p. 62-68, jan./jun. 2020.

TELEGRAM. *Privacy Policy.* Available at: https://telegramapp.github.io/privacy.html. Accessed on: March 26, 2024.

TELEGRAM. *Terms of Service.* Available at: https://telegramapp.github.io/tos.html. Accessed on: March 26, 2024.

TURILLAZZI, Aina; TADDEO, Mariarosaria; FLORIDI, Luciano; CASOLARI, Federico. The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, [s.l.], vol. 15, n. 1, p. 83-106, jan./jun. 2023. DOI: 10.1080/17579961.2023.2184136.

UNITED NATIONS. *Universal Declaration of Human Rights*. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed on: March 15, 2024.

VASAK, Karel. A 30-Year Struggle: The Sustained Efforts to Give Force of Law to the Universal Declaration of Human Rights. *The UNESCO Courier*, vol.77, n. 11, p. 28-29, nov.1977, p.29.

VK. *Privacy Policy.* Available at: https://vk.com/privacy. Accessed on: March 26, 2024.

VK. *User's Agreement.* Available at: https://vk.com/terms. Accessed on: March 26, 2024.

WE ARE SOCIAL. *Digital 2023*. Available at: https://wearesocial.com/uk/blog/2023/01/the-changing-world-of-digital-in-2023/. Accessed on: December 15, 2023.

WHATSAPP to try again to change privacy policy in mid-May. *Guardian*, feb./ 2021. Available at: https://www.theguardian.com/technology/2021/feb/22/whatsapp-to-try-again-to-change-privacy-policy-in-mid-may. Accessed on: March 26, 2024.

WHATSAPP. *Privacy Policy.* Available at: https://www.whatsapp.com/legal/privacy-policy-eea. Accessed on: March 26, 2024.

WHATSAPP. *Terms of Service.* Available at: https://www.whatsapp.com/legal/terms-of-service-eea/preview. Accessed on: March 26, 2024.

YANDEX. *Privacy Policy.* Available at: https://yandex.com/legal/confidential/. Accessed on: March 26, 2024.

YANDEX. *User Agreement.* Available at: https://yandex.ru/legal/rules/. Accessed on: March 26, 2024.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

VINOGRADOV, Vadim; CHAMBAS, Estelle. IT Giants vs. states in human rights regulation in digital space: a comparative review. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 98, p. 11-38, out./ dez. 2024. DOI: 10.21056/aec.v24i98.1931.