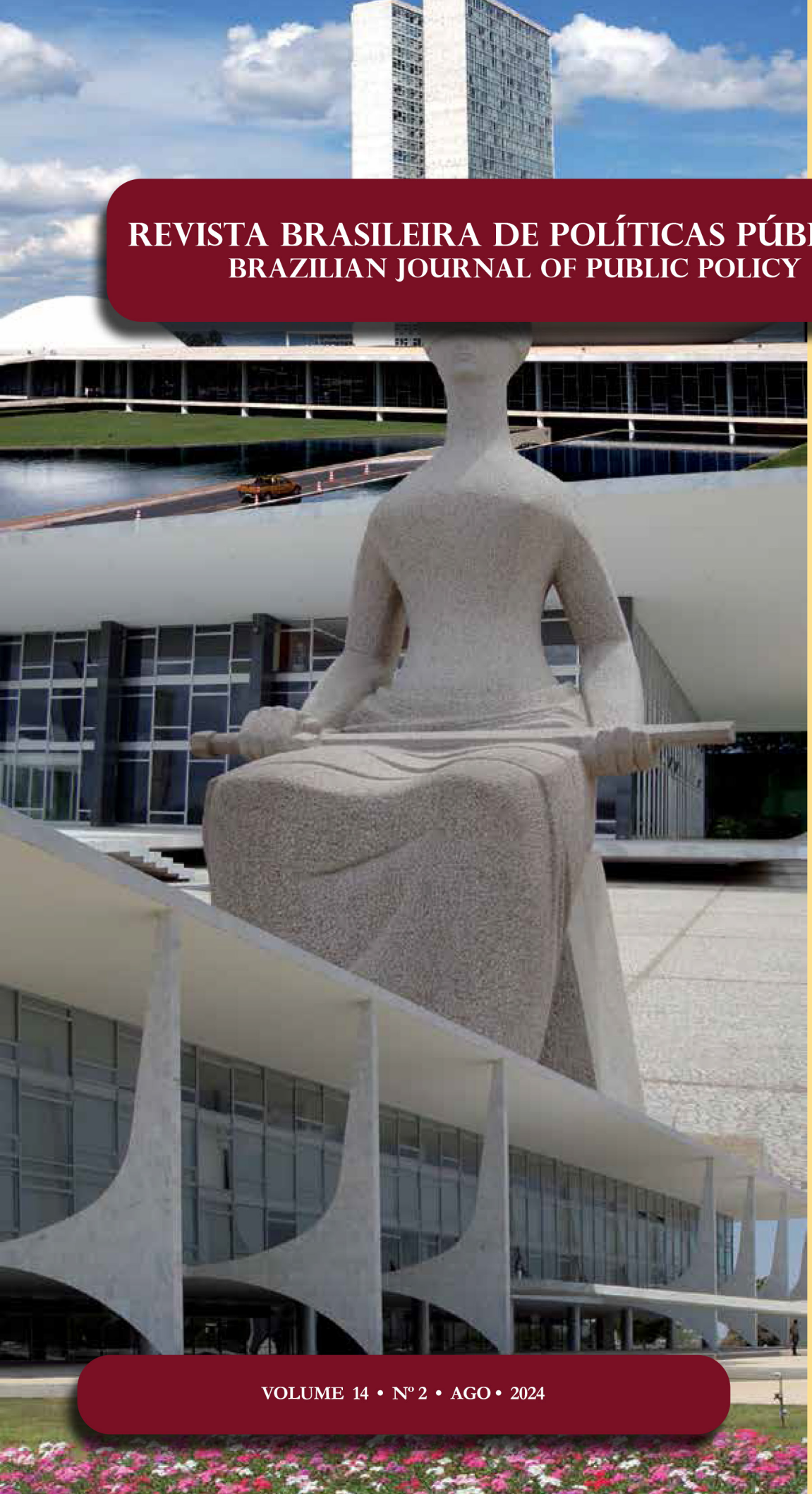

CEUB
EDUCAÇÃO SUPERIOR
ISSN 2236-1677

REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS
BRAZILIAN JOURNAL OF PUBLIC POLICY

Introspecting the digital dynamics: reconnecting the interplay between privacy, surveillance, and governance in the global landscape, with a special focus on India

Introspecção da dinâmica digital: reconhecendo a interação entre privacidade, vigilância e governança no cenário global, com foco especial na Índia

Neha Agashe

Anuttama Ghose

VOLUME 14 • Nº 2 • AGO • 2024

Sumário

doi: 10.5102/rbpp.v14i2.9408

Introspecting the digital dynamics: reconnecting the interplay between privacy, surveillance, and governance in the global landscape, with a special focus on India*

Introspecção da dinâmica digital: reconhecendo a interação entre privacidade, vigilância e governança no cenário global, com foco especial na Índia

Neha Agashe**

Anuttama Ghose***

Abstract

The interconnectedness of our modern society is deeply entangled, and technological pry has given rise to an intricate web that shapes our everyday lives. This paper analyses the intricate dynamics of the present Digital Age, primarily focusing on the ramifications of ubiquitous social media platforms and their consequential impact on democratic norms. Against the backdrop of industrial growth and development, thisresearch probes the profound significance of data as a pivotal driver of the contemporary economy and its multifaced repercussions on individual privacy, human rights, and power structures that operate within and beyond national boundaries. The research methodology employed in this study follows a doctrinal approach, focusing on a thorough examination and analysis of existing legal doctrines, constitutional provisions, legislation, and pertinent judicial precedents. This approach involves a systematic and structured exploration of legal materials to derive insights and conclusions. This exploration sheds light on how political thought evolves in response to the digital age and investigates how these theories influence legislative initiatives and policy formulations. This paper aims to outline a comprehensive analysis of the dichotomy that persists within digitally open and closed societies, accentuating the strategic role of data within the national security framework. The paper further accentuates the varied approaches adopted by governments to address digital vulnerabilities and ensure privacy rights, with a particular emphasis on the unique contours of the Indian landscape. Moreover, the study examines particular aspects of the Indian context, such as the development of privacy paradigms, a thorough examination of the Digital Personal Data Protection Act 2023, and a discerning assessment of privacy issues in light of the changing telecommunications laws, thereby highlighting the way in which the country has progressed in managing the intricate convergence of technological advancements, legislative changes, and societal demands.

Keywords: data protection; democracy; digital governance; national security and right to privacy.

* Recebido em: 29/01/2024
Aprovado em: 29/07/2024

** Dr. NehaAgashe is currently associated with Dr.Vishwanath Karad MIT World Peace University as Assistant Professor and as B.A LL.B Program Coordinator. She has pursued her PhD., M.Phil. and M.A from the University of Pune (SPPU), She has 16 years of teaching experience and has taught subjects related to political science in several reputed institutions in Pune, India.
E-mail: agashenehav@gmail.com.

*** Dr. Anuttama Ghose is an Assistant Professor of Law and Program Co-ordinator of PhD and LLB Program at the School of Law, Dr. Vishwanath Karad MIT World Peace University, Pune, India. She has completed her B.A LL.B (IPR Hons.) from the School of Law, KIIT University, Bhubaneshwar and LL.M with specialisation in the field of Intellectual Property Laws from Symbiosis Law School, Pune, India. She has completed her PhD from School of Law and Justice, Adamas University, Kolkata. She has previously worked as Vice-Principal and Assistant Professor of Law at Indian Institute of Legal Studies, Darjeeling, India.
E-mail: anuttamaghose@gmail.com.

Resumo

A interligação da nossa sociedade moderna está profundamente emaranhada e o progresso da tecnologia deu origem a uma intrincada rede que molda a nossa vida quotidiana. Este artigo procura analisar a intrincada dinâmica da atual Era Digital, com foco principal nas ramificações das onipresentes plataformas de mídia social e no seu consequente impacto nas normas democráticas. Tendo como pano de fundo o crescimento e o desenvolvimento industrial, esta investigação investiga o profundo significado dos dados como um motor central da economia contemporânea e as suas repercussões multifacetadas na privacidade individual, nos direitos humanos e nas estruturas de poder que operam dentro e fora das fronteiras nacionais. Neste estudo segue uma abordagem doutrinária, com foco em um exame e análise minuciosos das doutrinas jurídicas existentes, disposições constitucionais, legislação e precedentes judiciais pertinentes. Esta abordagem envolve uma exploração sistemática e estruturada de materiais jurídicos para obter insights e conclusões. Esta exploração esclarece como o pensamento político evolui em resposta à era digital e investiga como estas teorias influenciam as iniciativas legislativas e as formulações de políticas. Este artigo pretende delinear um a análise abrangente da dicotomia que persiste nas sociedades digitalmente abertas e fechadas, acentuando o papel estratégico dos dados no quadro da segurança nacional. O documento acentua ainda as diversas abordagens adotadas pelos governos para abordar as vulnerabilidades digitais, garantindo os direitos de privacidade, com especial ênfase nos contornos únicos da paisagem indiana. Além disso, o estudo examina aspectos específicos do contexto indiano, como o desenvolvimento de paradigmas de privacidade, um exame aprofundado da Lei de Proteção de Dados Pessoais Digitais de 2023 e uma avaliação criteriosa das questões de privacidade à luz das mudanças nas leis de telecomunicações, destacando assim a a forma como o país progrediu na gestão da intrincada convergência de avanços tecnológicos, mudanças legislativas e exigências sociais.

Palavras-chave: proteção de dados; democracia; governança digital; segurança nacional e direito à privacidade.

1 Introduction

The globalized nature of our society is intricately intertwined, and advancements in technology have created a complex network that governs our daily existence. As of January 2023, the global number of internet users exceeds 64%, which amounts to 5.16 billion individuals.[1] In addition to facilitating the organization of sociopolitical movements, the circulation of news, and the participation in political activities, the internet and social media platforms such as Facebook, Instagram, and Twitter, in particular, have evolved into arenas for these purposes. The decentralized nature of the platform often encourages the notion that democratic norms could be anticipated through robust debate and discussion.[2]

The advent of a digital society has resulted in a significant influx of information, which is the foundation of the Fourth Industrial Revolution (Industry 4.0). The commonly used phrase 'Data is the new oil' symbolizes the idea that human information drives the economy that relies on information. In this scenario, various concerns arise over the extensive databases amassed by social media platforms with the purpose of contributing to Artificial Intelligence.[3] Data harvesting can facilitate comprehension of many phenomena,

[1] KEMP, Simon. Digital 2023: global overview report. *Datareportal*, 26 jan. 2023. Available at: https://datareportal.com/reports/digital-2023-global-overview-report. Access on: 27 dec. 2023.

[2] ÜNVER, H. Akın. *Politics of digital surveillance, national security and privacy*. Istanbul: Centre for Economics and Foreign Policy Studies, 2018. Available at: https://www.jstor.org/stable/resrep17009. Access on: 27 dec. 2023.

[3] GLOBAL COMMISSION ON INTERNET GOVERNANCE. Toward a social compact for digital privacy and security. *In*: GLOBAL COMMISSION ON INTERNET GOVERNANCE. *Cyber security in a volatile world*. Waterloo: Centre for International Governance Innovation, 2017. p. 121-131. Available at: http://www.jstor.org/stable/resrep05239.14. Access on: 27 dec. 2023.

such as traffic patterns and the presence of undocumented migrants, as well as assessing potential voters' personality traits, among other applications. This profoundly affects the freedom and privacy of an individual at the most fundamental level. Furthermore, it strengthens the influence of non-state players who possess this data, as well as that of governments that may employ it for widespread monitoring, resulting in an imbalance of power. The right to privacy is universally recognized worldwide as an essential and inherent human right. Currently, most countries ensure the provision of certain rights to their inhabitants, but the extent of these rights may differ.[4] Freedom is a basic right that is universally guaranteed, yet it is restricted and has many different aspects. The concept of privacy is essentially a right bestowed upon individuals to safeguard their acts, decisions, and personal ideas conveyed inside a certain domain, preventing them from being revealed or examined by the general public.[5] This right is seen to be of utmost significance, particularly in contemporary society. Samuel Warren and Louis Brandeis pioneered establishing a legal entitlement to privacy.[6] They defined privacy as the protection of one's personal identity from intrusion or unwarranted disclosure. Essentially, they advocated for a "right to be left alone." Brandeis' understanding of privacy, particularly in relation to government interference, influenced the development of the US constitutional law.[7] This understanding is based on the specific provisions in the Bill of Rights that safeguard individuals against government intrusion into their homes and personal belongings. It also recognizes the importance of protecting personal autonomy and freedom of choice.

The boundaries of privacy have undergone significant shifts, particularly in the era of the data-driven online environment.[8] Many governments worldwide now prioritize the implementation of CCTV systems, utilization of image recognition technology, automatic interception and storage of internet and telecommunication data, and the application of AI for comprehensive analysis of the gathered information. Governments worldwide are actively promoting the use of these technologies, recognizing their practicality and cost-effectiveness. Some critics have raised concerns about the far-reaching effects of surveillance on individuals' privacy rights, suggesting that it may contribute to a growing sense of mistrust.[9] This research aims to evaluate a comparative analysis of governments categorized as digitally open or closed societies, focusing on data utilisation for surveillance purposes justified by national security concerns. This study assesses the issue of digital vulnerability and the diverse approaches governments take to enhance digital security and protect privacy rights, with a specific focus on India. Furthermore, the research investigates specific facets of the Indian milieu, including the evolution of privacy paradigms, a comprehensive analysis of the Digital Personal Data Protection Act, 2023 and a perceptive evaluation of privacy concerns in response to the evolving telecommunications legislation.

2 Unveiling the impact of communication technology and internetplatforms on privacy rights

In the era of rapid technological advancement and the pervasive integration of internet platforms, the profound impact on privacy rights has emerged as a paramount issue warranting rigorous scholarly exami-

[4] KAMPMARK, Binoy. Restraining the surveillance state: a global right to privacy. *Journal of Global Faultlines,* v. 2, n. 1, p. 1-16, 2014. Available at: https://doi.org/10.13169/jglobfaul.2.1.0001. Access on: 4 jul. 2024.

[5] SPEED, John Gilmer. The right of privacy. *The North American Review,* v. 163, n. 476, p. 64-74, 1896. Available at: http://www.jstor.org/stable/25118676. Access on: 4 jul. 2024.

[6] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890. Available at: https://doi.org/10.2307/1321160. Access on: 24 jan. 2024.

[7] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890. Available at: https://doi.org/10.2307/1321160. Access on: 24 jan. 2024.

[8] KAMPMARK, Binoy. Restraining the surveillance state: a global right to privacy. *Journal of Global Faultlines,* v. 2, n. 1, p. 1-16, 2014. Available at: https://doi.org/10.13169/jglobfaul.2.1.0001. Access on: 4 jul. 2024.

[9] KAMPMARK, Binoy. Restraining the surveillance state: a global right to privacy. *Journal of Global Faultlines,* v. 2, n. 1, p. 1-16, 2014. Available at: https://doi.org/10.13169/jglobfaul.2.1.0001. Access on: 4 jul. 2024.

nation.In the 1990s, Mark Weiser wrote an article, "The Computer for the 21st Century", and introduced the concept of ubiquitous computing, which meant those technologies that become an indistinguishable part of life disappear in the background.[10] Weiser sensed the creation of an unprecedented power that could reshape society in untold ways. Today, internet technology has become a ubiquitous part of our lives. Big data indicates data generated by many devices used by people and helps in understanding the way we interact.[11] Patterns of social trends can be discerned with a meso level of analysis over a prolonged period. The data or big data collected due to Information and Communication Technology (ICT) use has created a transformation in business, public administration, education, security and other such areas. Big data generated by smartphones, Internet of Things (IoT) devices, and social media networks is extremely resourceful. The data gathered creates possibilities for addressing socio-economic problems and providing solutions and effective measures. Data analysis and data mining have been used, from creating anti-terrorist systems, passenger profiling, money laundering, and fighting diseases to providing government services.[12]

However, few scholars ring a note of caution regarding such kind of data collection. Data Skeptics such as O'Neil who refer to big data being used as a WMD – Weapons of mass destruction where algorithms have a pervasive effect on our lives. The collection of data without our knowledge undermines equality and has the ability to influence people at critical junctures, such as going to college, borrowing money, and getting a job, among others.[13] The developments in the World Wide Web led to differentiation in privacy norms. Seemingly so, the early days of the internet or Web 1.0 allowed users to access data from sources and was 'read-only web'.[14] User anonymity and largely textual data ensured protection for the end user. The concept of privacy was seen as a right of the individual, something that internet service providers and the government had to accommodate and adhere to. In Web 2.0, in the era of data scraping, the concept of privacy has completely changed. First, we need to understand the concept of privacy in the digital age. Solove categorized privacy into four categories, which consist of information collection, information processing, information dissemination and invasion.[15] Richards also defines privacy as "information about humans that is used, accessed as known and is a matter of degree".[16] Anita Allen has attempted to state the meaning of information privacy being violated, which stands to be violated when data, conversation that an individual wishes to be anonymous, is nonetheless disclosed.[17]

The concept of privacy has flipped; where privacy is not mandated, it is referred to as 'dead' and has become an individual burden. The IoT eavesdrops on conversations, recording them- details of utterances being analyzed and slotted as per values, motives, and characteristics, which enables data harvesting. This situation can be aptly described as a society we value our innate desire to be free – we also like social media that does not cost us, tools that are free, free games. We may not pay for these but we do trade our privacy and our data. Social media giants thrive on the human capacity to share data which could be considered harmless, and yet by collecting data on parameters of age, race, sex, weight, height, educational level, politics, buying habits, and holidays, which are analyzed through algorithms. This passive but active listener with a dangerously long memory has led to many paying eulogies to privacy. By placing the end user responsibility on the user, those bodies providing services through internet, there is a vast amount of personal information disclosed to third parties. Within the digital ecosystem, the social currency becomes the identity of an

[10] WEISER, Mark. The computer for the 21st century. *Scientific American*, 1991. Available at: https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf. Access on: 28 dec. 2023.

[11] WEISER, Mark. The computer for the 21st century. *Scientific American*, 1991. Available at: https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf. Access on: 28 dec. 2023.

[12] GLOBAL COMMISSION ON INTERNET GOVERNANCE. Toward a social compact for digital privacy and security. *In*: GLOBAL COMMISSION ON INTERNET GOVERNANCE. *Cyber security in a volatile world*. Waterloo: Centre for International Governance Innovation, 2017. p. 121-131. Available at: http://www.jstor.org/stable/resrep05239.14. Access on: 27 dec. 2023.

[13] O'NEIL, Cathy. *Weapons of math destruction*: how big data increases inequality and threatens democracy. New York: Crown, 2016.

[14] O'NEIL, Cathy. *Weapons of math destruction*: how big data increases inequality and threatens democracy. New York: Crown, 2016.

[15] SOLOVE, Daniel J. *The digital person*: technology and privacy in the digital age. New York: NYU Press, 2004.

[16] RICHARDS, Neil. *Why privacy matters*. New York: Oxford University Press, 2022.

[17] ALLEN, Anita. *Unpopular privacy*: what must we hide? studies in feminist philosophy. New York: Oxford University Press, 2011.

individual and, thereby, analysis associated with data collection and algorithms. This shift regarding privacy and data brings back the question of who is responsible for data protection and privacy of users. We also must grapple with the consequences on the ethical plane of the reconceptualization of the idea of privacy.[18]

So, the question arises: at what point did the developments lead us to reassess the privacy of individuals using the internet? Edward Snowden, one of the USA's most controversial whistleblowers, exposed the secret surveillance operations that allowed them to spy on the internet history of citizens undertaken by the National Security Agency in the USA.[19] These revelations sparked off a debate on government violating right to privacy under the name of national security. The practice of greater surveillance on citizens can be traced back to post-September 11, 2001 attacks that have taken place in the USA. The war on terror narrative became a factor for communication surveillance especially with growth of internet and mobile phones. In the next section of this article, the author's objective is to comprehend and assess the discussions around privacy and surveillance. These arguments have resonated with those about freedom of expression and censorship, which have persisted for millennia. These discussions have emerged as key obstacles in the information age, as well.

3 Surveillance state or national security? a comparative study of digitally open and closed societies

Digital surveillance in the modern age can be likened to the concept of the 'Panopticon' – a mechanism of social control or a type of prison system described by 18th-century Utilitarian scholar Jeremy Bentham.[20] In today's day and age, the panopticon guards have been replaced by CCTVs. Digital surveillance goes with the metaphor of panopticon in an apt manner as there is an asymmetry of collection of information where people are subjected to being merely 'objects of information'. Barlett infers that data collection done on the internet is like a modern panopticon, which has serious ramifications for potential manipulation, lack of choice on the part of the user, autonomy, or privacy.[21]

3.1 Data: the new frontier of exploitation and empowerment

This brings us to the question of why privacy matters in this digital age. Mark Zuckerberg, the founder of Facebook believes that privacy is no longer a social norm.[22] Privacy being claimed dead indicates an alarming position of those in control of our digital society. Data is the new oil, is the adage oft repeated and the fact that the digital society is built upon the edifice of the flow of human information. However, the rules for the collection of data and the manner in which information is used haven't been settled yet. This disempowers citizens and our ability to have a say over out information is slipping away.[23]

The right to privacy isn't only about controlling our information and limiting access to our lives; it is also about 'power'.[24] Privacy is not just who knows about us, but what rules apply to what they know. Neil Richards has spoken about privacy values and their instrumentality in his book 'Why Privacy Matters'. Firs-

[18] GOODMAN, Matthew P.; GERSTEL, Dylan. Championing data governance. *In*: REINSCH, William; MILLER, Scott (ed.). *Sharpening America's innovative edge*. Washington, DC: Center for Strategic and International Studies (CSIS), 2020. p. 21-24.

[19] GREENWALD, Glenn. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*, 11 jun. 2013. Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Access on: 28 dec. 2023.

[20] BARLETT, Jamie. *The people vs tech*: how the internet is killing democracy (and how to save it). London: Ebury Press, 2018.

[21] BARLETT, Jamie. *The people vs tech*: how the internet is killing democracy (and how to save it). London: Ebury Press, 2018.

[22] RICHARDS, Neil. *Why privacy matters*. New York: Oxford University Press, 2022.

[23] RICHARDS, Neil. *Why privacy matters*. New York: Oxford University Press, 2022.

[24] RICHARDS, Neil. *Why privacy matters*. New York: Oxford University Press, 2022.

tly, intellectual privacy is important in any democracy as it helps shape our political beliefs without being judged or watched. It is vital to shape our identity and even have the autonomy to have multiple identities, which only makes us human. Secondly, it is a bulwark for democratic freedom. National security demands and, at times, overstates the need for surveillance. However, this comes at the cost of us being less free. Mass surveillance in societies that know everything about everyone can be misused for the personal ends of those having access to such data. For instance, in South Korea in 2012, the security service tried rigging their election in favour of a preferred candidate.[25]

Information becomes social power. The fourth industrial revolution, namely the digitalization of the economy, was built on one that exploits personal data, and hence privacy becomes a central contesting concept. It is the position chosen over privacy that will determine the allocation of power in the economy and society. Human data provides raw material for futuristic technology such as machine learning and artificial intelligence. Gathering information gives power to control people. Internet companies, ergo, with the voluminous data collected, become power behemoths.[26] The Cambridge Analytica case reflects how personal data was utilized to design political campaigns. Cambridge Analytica built up a database of around 5000 data points on 230 million Americans from the internet, Facebook, and telephonic surveys, among others.[27] By analyzing with the help of big data, Cambridge Analytica discovered that most people favouring cars made in the USA would be the target audience for Trump's presidential elections. Cambridge Analytica shows the possibilities where data gets used and applied. This marks a jump from politics being shaped instinctively through understanding the public pulse to data-driven, evidence-backed digital interference in winning the mandate of people by using their own data to understand them.[28]

Zuboff has dubbed the Web 2.0 era as surveillance capitalism and believes it is an anti-democratic force.[29] The prevalence of fake news and information corruption are part of the online experience. Targeted advertising has led to political polarization in societies, and the use of algorithms and eventual display of extremist posts and placing predictive information products has led to more consumer engagement and the feeling of online oneness that's not based on egalitarian motives but a dictated anti-democratic social force manipulated through data. Zuboff believes that surveillance capitalism is acclaimed as personalization, but in reality, it degrades an individual into a metric to be used for further data harvesting.[30] This era of technology dominance of few firms that have entered the domain of social media has been referred to as not a *coup d'état* but as *coup de gens*. To substantiate this point, it would be appropriate to view Zuckerberg's statement where he referred to Facebook as a new global church which could address problems that are civilizational in scale and scope. The power of the data drives this understanding.[31]

---

[25] MCCURRY, Justin. South Korea spy agency admits trying to rig 2012 presidential election. *The Guardian*, 4 aug. 2017. Available at: https://www.theguardian.com/world/2017/aug/04/south-koreas-spy-agency-admits-trying-rig-election-national-intelligence-service-2012. Access on: 29 dec. 2023.

[26] MAGRANI, Eduardo. Hacking the electorate: thoughts on misinformation and personal data protection. *Konrad Adenauer Stiftung*: Facts & Findings, n. 399, 2020. Available at: https://www.jstor.org/stable/resrep25290. Access on: 31 dec. 2023.

[27] CONFESSORE, Nicholas. Cambridge Analytica and Facebook: the scandal and the fallout so far. *The New York Times*, 4 apr. 2018. Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Access on: 5 jan. 2023.

[28] NOSTHOFF, Anna-Verena; MASCHEWSKI, Felix. The platform economy's infrastructural transformation of the public sphere: Facebook and Cambridge Analytica revisited. *Philosophy & Social Criticism*, v. 50, n. 1, p. 178-199, 2024. Available at: https://doi.org/10.1177/01914537231203536. Access on: 8 jan. 2024.

[29] ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. London: Profile Books, 2019.

[30] ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. London: Profile Books, 2019.

[31] ZEEBIZ WEBTEAM. Mark Zuckerberg talks of using Facebook to build a better global community. *Zee Business*, 17 feb. 2017. Available at: https://www.zeebiz.com/companies/news-mark-zuckerberg-talks-of-using-facebook-to-build-a-better-global-community-12573. Access on: 12 jan. 2024.

Solove believes that users' powerlessness is due to being at the mercy of the bureaucratic process, opacity of procedure, and indifference to them and their concerns.[32] Julie Cohen calls digital platforms informational capitalism, where human beings become raw materials and data procured through the process of surveillance and through human conditioning, inadvertently turning users into conduits of information.[33]

3.2 Global approaches to digital vulnerability: examining governmental responses

Today, a new set of rules is mandated to protect against this asymmetrical power and unchecked abuses. As a human right, the right to privacy is mentioned in the Universal Declaration of Human Rights (UDHR) under Article 12, which states, "No one shall be subjected to arbitrary interference which his privacy, family, home or correspondence […]".[34] Under International Covenant on Civil and Political Rights Article 17 similarly states "No one shall be subjected to arbitrary or unlawful interference with privacy […] correspondence".[35] Few more recent charters, such as the E.U Charter of Fundamental Rights- Article 7, speak of the protection of private, family life, home and communication. Article 8 has gone one step ahead and also included the right to personal data.[36]

Even if these international/ regional treaties promise privacy, the question arises at the level of nation--states: how does this operate? There is an absence of global digital governance values. National security, surveillance and data privacy become contentious issues in today's times. The ideological factor also determines the responses of the state to the idea of individuals' data privacy.[37]

Chinese government runs a social credit system, which is the core of the Chinese internet agenda.[38] By leveraging citizens' personal data, it is used for behaviour modification and improvement. This data is collected by both government and private businesses. The system aims to punishgood and bad behaviour with rewards and punishments, respectively, solely by compiling data on citizens from public and private sources available through biometric collection. The device networks in China are also controlled by the government, which can also attack other networks. The 800-million-dollar shield project, which binds all Chinese device networks by a firewall (also dubbed as the great Chinese firewall), seeks to prevent Chinese internet users from accessing data outside China. Thus, the firewall operates on an extensive surveillance systemthat is meant to control any kind of political dissent and thereby keep public opinion under control.[39] The Chinese Intelligence Law of 2017 also requires private companies to co-operate and share data as and when required by the state agencies. China thus could be referred to as a model of digital authoritarianism, where it does not believe in free internet norms supported by the west.[40]

---

32 SOLOVE, Daniel J. *The digital person*: technology and privacy in the digital age. New York: NYU Press, 2004.

33 RICHARDS, Neil. *Why privacy matters*. New York: Oxford University Press, 2022.

34 UNITED NATIONS. *Universal Declaration of Human Rights*. New York: United Nation, 1948. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks. Access on: 15 jan. 2024.

35 UNITED NATIONS. *International covenant on civil and political rights*. New York: United Nation, 1966. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Access on: 18 jan. 2024.

36 EUROPEAN COMISSION. *EU Charter of Fundamental Rights*. 2000. Available at: http://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life#:~:text=Everyone%20has%20the%20right%20to,family%20life%2C%20home%20and%20communications. Access on: 18 jan. 2024.

37 POZEN, David E. Privacy-privacy tradeoffs. *The University of Chicago Law Review*, v. 83, n. 1, p. 221-247, 2016. Available at: https://www.jstor.org/stable/43741598. Access on: 18 jan. 2024.

38 ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. London: Profile Books, 2019.

39 BLOOMBERG NEWS. The great firewall of China. *Bloomberg*, 12 out. 2017. Available at: https://www.bloomberg.com/view/quicktake/great-firewall-of-china. Access on: 19 jan. 2024.

40 WANG, Maya. China's dystopian push to revolutionize surveillance. *Human Rights Watch*, 18 aug. 2017. Available at: https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance. Access on: 19 jan. 2024.

In USA, during Bush and Obama administration, progress in information technology was seen as one of the most effective ways in which security threats could be tackled, until Snowden's revelations. The complicity between the state security agencies and tech companies exposed the instrumentarian power dynamics. In the backdrop of terror attacks in France, President Obama insisted that tech companies such as Google, Facebook remove radical content related to terrorism, which the companies did comply with. In 2016, in a policy statement to Congress, it was told that the intelligence services of the USA would use the data gathered on the basis of IoT for surveillance purposes.[41] This got further consolidated when USA passed the CLOUD Act (Clarifying Lawful Overseas Use of Data) which can be required to produce the data stored by tech companies regardless of the jurisdiction it operates in and at any given point of time.[42]

Closer to home, at a micro level in India, interception in the name of security is legal under specific grounds. However, hacking is a punishable offence under the IT (Amendment) Act of 2008. At the macro level, to track the actions of its citizens, India uses various digital surveillance tools like CCTVs and facial recognition cameras.[43] Recently, India ranked in the Forbes list of the most mass surveillance cities in the world, namely Delhi, and Chennai, among others. However, there was great furore in India over the Pegasus spyware being used as a surveillance tool in India. There is a claim that Israeli spyware has been used by the government to spy on civilians, journalists, ministers and parliamentarians. This led to a Supreme Court-appointed group to analyze the charges.[44] The report of the group proved inconclusive as the evidence to prove if spyware was indeed installed on devices was lacking. The case is still subjudice.[45] The Pegasus case raises concerns that under the name of security, will privacy be held hostage? The question arises here: how do we identify grave national threats to security and being overzealous regarding the same?

The European Union framework offers a via media between extreme stands pertaining to security. European Union took the lead in establishing a legal framework entitled General Data Protection Regulation (GDPR) in 2016, which specifies guidelines for collecting, processing information and localizing data within the European Union.[46] It questions the companies' collecting data of users and companies have to justify why they need to collect the data. This system has also given the right to erase data or the right to be forgotten. It has set prohibitive fines for violators along with permission for class action suits in case the rights of people get violated. The GDPR is intended at using digital resources wisely at the same time protecting democratic values and individual freedoms while engaging in regulatory leadership and partnership.[47]

When it comes to surveillance and technology, predictive data science is pointing out to individuals who may have the propensity to be a criminal. Under the name of security, this has created a heavier burden of proof on the party treated as suspect and thus increasing the 'innocence threshold' that ought to be overco-

41 ZITTRAIN, Jonathan L. *et al*. Don't panic: making progress on going dark debate. *Berkman Center Research Publication*, 1 feb. 2016. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552576. Access on: 20 jan. 2024.

42 ZITTRAIN, Jonathan L. *et al*. Don't panic: making progress on going dark debate. *Berkman Center Research Publication*, 1 feb. 2016. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552576. Access on: 20 jan. 2024.

43 DURAISWAMI, Dhiraj R. Privacy and data protection in India. *Journal of Law & Cyber Warfare*, v. 6, n. 1, p. 166-186, 2017. Available at: https://cybersecuritysummit.com/wp-content/uploads/2017/10/JLCW_6-1_Cyber-Enhanced-Sanction-Strategies_Do-Options-Exist.pdf. Access on: 20 jan. 2024.

44 DESOMBRE, Winnona *et al*. *Countering cyber proliferation*: zeroing in on access-as-a-service. Washington, DC: Atlantic Council, 2021. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf. Access on: 22 jan. 2024.

45 FELDSTEIN, Steven; KOT, Brian. Global context of commercial spyware and digital forensics. *In*: FELDSTEIN, Steven; KOT, Brian. *Why does the global spyware industry continue to thrive?*: trends, explanations, and responses. Washington, DC: Carnegie Endowment for International Peace, 2023. p. 8-11. Available at: https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf. Access on: 22 jan. 2024.

46 RYNGAERT, Cedric; TAYLOR, Mistale. The GDPR as global data protection regulation?. *AJIL Unbound*, v. 114, p. 5-9, 2020. Available at: https://doi.org/10.1017/aju.2019.80. Access on: 23 jan. 2024.

47 YOKOHAMA, Shinichi. Private sector and the regional level. *In*: SAALMAN, Lora (ed.). *Integrating cybersecurity and critical infrastructure*: national, regional and international approaches. Solna: Stockholm International Peace Research Institute, 2018. p. 23-28. Available at: https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity_0.pdf. Access on: 23 jan. 2024.

me.[48] A deeper implication here would be that somewhere it violates the trust of a citizen to the state along with the presumption of individual's innocence. In 1890 a seminal article was written by Samuel Warren and Louis Brandies in the Harvard Law review, on the invention of cameras and its impact on society. Warren and Brandies stated that camera invention would put citizens under the scanner of constant surveillance.[49] The shift of delicate social norms and rise of new technology necessitates new laws to evolve. It is through this article, that Warren and Brandies(1890) underlined the importance of privacy to the individual and believed that citizens needed a right to be alone.[50]

The United Nations have addressed the idea of the right to privacy in the digital age. In 2015, UN General Assembly adopted a resolution on the right to privacy in the digital age, even though there was opposition from the other states.[51] The Secretary-General called for a strategy on new technology and a road map for digital cooperation. In 2015, the U.N. Human Rights Council supported the creation of a Special Rapporteur on Right to Privacy, having the mandate on reporting of violations of member states.[52] The Rapporteur can review governmental policies on the interception of personal data and objects if they intrude on privacy. Examining the private sector's responsibilities with respect to human rights and privacy, working with other UN experts to broaden the idea of protection of privacy by including protecting freedom of expression, peaceful assembly, and identifying threats to rights in the context of indiscriminate mass surveillance are also part of the duties of the Rapporteur.[53]

The courts in countries like the United Statesand India have interpreted the Right to Privacy in various legislations, even in cases where privacy is not explicitly recognized in the Constitution. In the following segment, the authors will delve into India's perspective on privacy rights, the concerns surrounding mass surveillance programs, and the latest legislative advancements in this area.

4 **Striking a balance:** India's pursuit of harmony between digital security and privacy rights

In the Indian context, with reference to right to privacy, in the constituent assembly while drafting of Indian Constitution there was a discussion on this right. As part of the states and minorities reports, Dr. Ambedkar, K. M. Munshi and Harman Singh firmly supported the need to include privacy as a fundamental right.[54] However few constituent assembly members such as B.N Rau and Alladi Krishnaswamy Ayyar vehemently dissented as such as right would be an impediment in way of law enforcing agencies. The principal objection also lied in the fact that administration of a vast and diverse country like India would be inherently arduous.

[48] GALETTA, Antonella. The changing nature of presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?. *European Journal of Law and Technology*, v. 4, n. 2, 2013. Available at: https://ejlt.org/index.php/ejlt/article/view/221/377. Access on: 24 jan. 2024.

[49] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890. Available at: https://doi.org/10.2307/1321160. Access on: 24 jan. 2024.

[50] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890. Available at: https://doi.org/10.2307/1321160. Access on: 24 jan. 2024.

[51] UNITED NATIONS. General assembly backs right to privacy in digital age. *UN News*, 19 dec. 2013. Available at: https://news.un.org/en/story/2013/12/458232. Access on: 25 jan. 2024.

[52] UN Human Rights Council creates special rapporteur on right to privacy. *International Justice Resource Center*, 22 apr. 2015. Available at: https://ijrcenter.org/2015/04/22/un-human-rights-council-adopts-resolution-to-create-special-rapporteur-on-the-right-to-privacy/. Access on: 25 jan. 2024.

[53] UN Human Rights Council creates special rapporteur on right to privacy. *International Justice Resource Center*, 22 apr. 2015. Available at: https://ijrcenter.org/2015/04/22/un-human-rights-council-adopts-resolution-to-create-special-rapporteur-on-the-right-to-privacy/. Access on: 25 jan. 2024.

[54] LUTHRA, Samarth Krishan; BAKHRU, Vasundhara. Publicity rights and the right to privacy in India. *National Law School of India Review*, v. 31, n. 1, p. 125-148, 2019.

4.1 Evolution of privacy paradigms in the Indian context

The right to privacy was accorded the status of fundamental right under Article 21 in the landmark judgement case of KS Puttaswamy v. Union of India[55] in 2017. This judgement impacts Indians right from sexual orientation to sharing Aadhar card details. Right to privacy gives individuals a broadened set of rights that can be enforced against the state. The constitutional recognition of the right to privacy highlights the accommodation of newly emerging issues and in keeping with the changing needs of society.[56] In the judgement Justice D.Y Chandrachud remarked that we are in an era of "dataveillance"; where data mining transmits intimate information that gets revealed to law enforcers. In order to uphold the individual's right to data privacy, the court directedthe constitution of a special committee to create a framework for data protection with ad special focus on individual privacy.[57] There have been several discussions regarding the need for comprehensive data protection legislation in India. The Puttuswamy judgement recognised the 'horizontal applicability of privacy'. This meant that it cannot be that the individual has right to privacy just against the state. The non-state actors, who are outside the purview of enforcement of right to privacy, need to brought in data protection enforcement and have a liability towards individuals. Justice B.N Shrikrishna Committee was entrusted with responsibility of studying key issues and the report was submitted in 2018.[58]

In 2017, the Supreme Court of India made a significant decision in the case of Justice K. S. Puttaswamy v. Union of India, which provided insight into the future of privacy. However, India still lacked a comprehensive and up-to-date legislation that could be used to interpret cases related to data protection.[59] India lacked an equivalent to the General Data Protection Regulation ("GDPR") of the European Union, which it greatly felt the absence of.

Since 2018, the Indian Government has been making efforts to create and enforce a central legislation that might serve as the successor to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") and function as an independent data protection law. In 2023, the Lok Sabha passed the current version of the Data Protection Bill, known as the 'Digital Personal Data Protection Bill, 2023' ("DPDP Bill"), after several previous drafts were released. Subsequently, on August 9, 2023, the DPDP Bill was approved by the Rajya Sabha. On August 11, 2023, the President of India approved and authorized the Digital Personal Data Protection Act, 2023 ("DPDP Act"), which was then officially announced and made available in the Official Gazette of India. This paper hypothesizes that the increasing digitalization in India, coupled with evolving global privacy and surveillance norms, presents unique governance challenges. Specifically, it posits that India's regulatory framework must be significantly reformed to balance the intricate dynamics of privacy protection and surveillance, aligning with global best practices while addressing local socio-political contexts.

[55] INDIA. Supreme Court. Justice K. S. *Puttaswamy Vs. Union of India 10 SCC 1*. 2017.

[56] BHATIA, Gautam. State surveillance and the right to privacy in India: a constitutional biography. *National Law School of India Review*, v. 26, n. 2, p. 127-158, 2014.

[57] GURUSWAMY, Menaka. Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors, Writ Petition (Civil) No. 494 of 2012. *The American Journal of International Law*, v. 111, n. 4, p. 994-1000, 2017. Available at: https://www.jstor.org/stable/26568904. Access on: 26 jan. 2024.

[58] GURUSWAMY, Menaka. Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors, Writ Petition (Civil) No. 494 of 2012. *The American Journal of International Law*, v. 111, n. 4, p. 994-1000, 2017. Available at: https://www.jstor.org/stable/26568904. Access on: 26 jan. 2024.

[59] DURAISWAMI, Dhiraj R. Privacy and data protection in India. *Journal of Law & Cyber Warfare*, v. 6, n. 1, p. 166-186, 2017. Available at: https://cybersecuritysummit.com/wp-content/uploads/2017/10/JLCW_6-1_Cyber-Enhanced-Sanction-Strategies_Do-Options-Exist.pdf. Access on: 20 jan. 2024.

4.2 A close review of india's digital personal data protection act, 2023: how well does it protect privacy?

The DPDP Act encompasses a comprehensive set of provisions pertaining to the obligations of notice and consent, defines the acceptable "legitimate uses" for processing personal data without explicit consent, establishes an "Appellate Tribunal" to address grievances, and imposes heightened responsibilities on data fiduciaries in relation to the handling of children's data, among various other modifications. The DPDP Act appears to establish a symbiotic relationship with the overarching information technology regulations of the Government of India. The dimension pertaining to the acquisition of information is closely linked to the interface between the Information Technology Act[60] and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. This interface grants the Central Government the authority to request information from various entities, including the Data Protection Board, fiduciaries, and intermediaries.[61] Nevertheless, the lack of explicit particulars suggests an inquiry into the extent, objective, and protective measures linked to this data collection, thereby requiring adherence to the legal principles expounded in the Puttaswamy judgment.

Notwithstanding the presence of unresolved inquiries pertaining to the practical execution of the aforementioned legislation, there exist apprehensions regarding distinct stipulations within the law and their propensity to compromise the ostensibly granted safeguards.[62]

Firstly, the exceptions made for consent grant the state substantial authority and elevate governmental priorities above those of private businesses. While this may be valid in certain situations, such as disasters or emergencies, the legislation broadens the range of such circumstances. An illustration of this is Section 7(b) of Act[63], which allows the government to bypass the need for agreement in cases where a recipient of government services has already agreed to receive any other form of assistance from the state. Although this may facilitate convenient retrieval of personal information from recipients of government services, it also presents the possibility of the government consolidating databases. This is because fully harnessing the potential of this provision would necessitate exempting government entities from purpose constraints that mandate the deletion of personal data once its intended use has been fulfilled.

Another illustration of this phenomenon is the collection of exceptions granted by the government for investigative, prosecution, and national security objectives. According to Section 17(1)(c) of the Act, the need for notice and permission is waived for the specific purpose of processing data related to the prevention, detection, investigation, or prosecution of any offense or violation of the law.[64] Although comprehensible, Section 17(2)(a) grants a comprehensive exemption from the entire law to any government agency that the government may officially inform in order to safeguard sovereignty, security, integrity, public order and avoid incitement. Section 17(2)(a)[65] expresses Parliament's intention to fully exempt some governmental agencies from the implementation of data protection laws, in addition to the existing provision in Section 17(1)(c). Provisions of this nature establish a distinct classification of conduct that falls outside the scope of data privacy regulations. The lack of limits on the Indian state, particularly when there is no urgent need for such an exemption, is a significant difficulty.

Secondly, the government's discretionary authority to create rules, as granted by the law, may potentially weaken the safeguards established by the legislation in some situations. Under Section 17(5), the government is authorized to exclude any business or group of enterprises from the application of certain provisions

60 INDIA. India Code. *Information Technology Act*, *2000*. Section 2(1)(w).

61 INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 36.

62 KESSLER, David J. *et al.* A comparative analysis of indian privacy law and the asia-pacific economic cooperation cross-border privacy rules. *National Law School of India Review*, v. 26, n. 1, p. 31-61, 2014.

63 INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 7(b).

64 INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 17(1)(c).

65 INDIA. India Code. *Digital Personal Data Protection Act*, *2023*. Section 17(2)(a).

of this law during a period of five years from the law's commencement.[66] There is currently no specified duration for the implementation of this exemption, nor is there any guidance on the specific use of this rule. A favorable interpretation of this provision implies that it could be utilized to grant sunrise businesses or startups a grace period to adhere to the law. Nevertheless, the inclusion of this clause has already been accounted for in Section 17(3), which grants restricted exemptions to startups and other industries that the government may officially designate.[67] Hence, Section 17(5) has the potential to be employed in a way that undermines the intended objective of the legislation.[68] It is important to emphasize that the law restricts the government's authority to provide these exemptions for a specific duration of five years. There is no specified duration for these exclusions.

In a similar vein, the government possesses discretionary authority to establish rules that exclude corporations from specific obligations related to the handling of children's data. Sections 9(1) to 9(3) of the Act delineate certain prerequisites for the same—they necessitate parental approval and ban profiling, among other things. Section 9(4) grants the government the authority to exempt any firm or group of enterprises from complying with Sections 9(1) to 9(3), provided that certain circumstances are specified.[69] This section lacks clarity regarding the criteria for granting this exception and the process for determining the circumstances. Due to inadequate guidance, this clause is susceptible to misuse. Although the government has the right to prescribe conditions and set substantive regulations in other laws, the instances mentioned above offer very little assistance. This issue is more troublesome when evaluated in light of the principles of Indian administrative law, which stipulate that laws should not grant unrestricted and undue jurisdiction to the implementing body. Improper utilization of these legal provisions may potentially contravene the Indian Constitution.

Thirdly, the architecture of the DPB poses significant issues. The board functions as an autonomous entity with a specific and restricted purpose, and the government will establish procedures for choosing and appointing its members. Although the law establishes criteria for board members, it does not specify the exact number of members required. Additionally, it simply mandates that at least one member has expertise in legal matters. The aforementioned provision poses a challenge, as one of the primary responsibilities of the board is to impose sanctions and provide instructions for failure to comply. Furthermore, the chairperson of the DPB has the authority to provide any board member the capacity to carry out "any of the functions of the board and oversee any of its proceedings." The chairperson may potentially withhold authorization for the legal member of the board to oversee the proceedings that culminate in the imposition of a penalty. This design also lacks the ability to uphold an internal division of responsibilities between the members conducting the inquiry and the chairperson. Given that the chairperson has the authority to select members to carry out investigations, there is a possibility that they may not fulfill their duty with complete impartiality in certain instances.

The General Data Protection Regulation (GDPR) of the European Union and the Digital Personal Data Protection (DPDP) Act are both comprehensive frameworks for data protection. However, they have distinct differences in terms of their scope, structure, and regional application. Personal data is categorized into different subsets under the GDPR.[70] Separate compliances apply to these categories of personal data, which include the purpose for processing such information. Compliance under the DPDP, on the other hand, is not contingent upon the nature of personal data and is applicable to all types of personal data without discrimination.[71] GDPR applies to any offline data that is part of a filing system, while the DPDP

66 INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 17(5).

67 INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 17(3).

68 INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 17(5).

69 INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Sections 9(1) to 9(3).

70 ENGELKE, Peter. *AI, society, and governance*: an introduction. Washington, DC: Atlantic Council, 2020. Available at: http://www.jstor.org/stable/resrep29327. Access on: 4 jul. 2024.

71 NACHIAPPAN, Karthik *et al*. Digital and technology. *In*: SÁNCHEZ-CACICEDO, Amaia (ed.). *EU-India relations*: gaining

Act limits its applicability to digital or digitized data. In addition, the DPDP mandates that notice must only be given in cases where data processing relies on consent, rather than for legitimate purposes. According to GDPR regulations, it seems that the notice requirements are applicable whenever data is collected from the data subject, regardless of whether it is solely linked to consent.[72] Unlike the DPDP, the GDPR does not explicitly forbid the practice of behavioral monitoring or targeted advertising targeted towards children. In addition, the DPDP empowers the Central Government to limit the transfer of personal data by a data fiduciary to designated countries or territories beyond India. Therefore, with the exception of countries listed in the negative list to be released by the Central Government, personal data can be transferred without any restrictions.[73] Under the GDPR, the transfer of personal data can vary in terms of permissibility. It can range from freely transferring data to a country or international organization that has been deemed adequate, to conditional transfers using standard contractual clauses, and even limited permission to transfer under specific circumstances. Therefore, the GDPR includes more extensive and precise limitations on cross-border transfers, in contrast to the DPDP.

Hence, although the DPDP Act establishes legal safeguards for data privacy, specific elements in the legislation can potentially undercut its advantages if the government fails to adhere to them with utmost diligence. The DPDP Act represents the outcome of over five years of discussion and careful consideration, and it signifies the initiation of legal regulations for safeguarding personal data. The efficacy of personal data privacy protection will be determined by the regulatory developments and institutional arrangements that emerge in the coming years. The new legislation establishes the essential framework, although it is inadequate for the actual realization of data privacy.

4.3 Privacy concerns amidst evolution of telecommunication laws in India: transition from archaic colonial legislation to assessing spectrum of internet governance

The Telecommunication Act 2023 received Presidential assent on 27th December 2023.[74] The objective of the Act is to update and unify the regulatory framework for telecommunications and stimulate the expansion of the sector. The Telecommunications Act of 2023 superseded the outdated laws of the Indian Telegraph Act of 1885 and the Indian Wireless Telegraphy Act of 1933.[75] The British utilized these colonial regulations to exert stringent control over communications in colonial India. The Act eliminates mentions of services such as Internet-based communications and OTT communications from the definition of telecom services. However, it maintains the comprehensive definitions for 'telecommunication' and 'message'.[76] As a result, concerns remain that the Act could potentially be applicable to a wide range of IT and digital services. The Act introduces a simpler authorization system, replacing the current licensing system, and allows for administrative distribution of spectrum for satellite services.[77] The legislation maintains the

strategic traction? Paris: European Union Institute for Security Studies (EUISS), 2024. Available at: http://www.jstor.org/stable/resrep57929.7. Access on: 4 jul. 2024.

72 NACHIAPPAN, Karthik *et al*. Digital and technology. *In*: SÁNCHEZ-CACICEDO, Amaia (ed.). *EU-India relations*: gaining strategic traction? Paris: European Union Institute for Security Studies (EUISS), 2024. Available at: http://www.jstor.org/stable/resrep57929.7. Access on: 4 jul. 2024.

73 NACHIAPPAN, Karthik *et al*. Digital and technology. *In*: SÁNCHEZ-CACICEDO, Amaia (ed.). *EU-India relations*: gaining strategic traction? Paris: European Union Institute for Security Studies (EUISS), 2024. Available at: http://www.jstor.org/stable/resrep57929.7. Access on: 4 jul. 2024.

74 PRESIDENT signs Telecom Act, rulemaking to follow for implementation. *The Hindu*, 25 dec. 2023. Available at: https://www.thehindu.com/news/national/president-signs-telecom-act-rulemaking-to-follow-for-implementation/article67674004.ece. Access on: 26 jan. 2024.

75 PALIWAL, Aishwarya. Telecommunications Bill receives president's assent, becomes law. *India Today*, 25 dec. 2023. Available at: https://www.indiatoday.in/law/story/telecommunications-bill-receives-president-droupadi-murmu-assent-becomes-law-2480283-2023-12-25. Access on: 26 jan. 2024.

76 INDIA. India Code. *Telecommunications Act, 2023*. Section 2.

77 INDIA. India Code. *Telecommunications Act, 2023*. Section 3(1).

government's authority to assume control of telecommunications services and networks, while also raising the severity of sanctions.

The Internet and Mobile Association of India, a prominent industry organization representing internet companies and startups in the nation, has expressed support for the Bill that aims to exempt over-the-top platforms (OTTs) from regulation. However, this sense of celebration is likely to be misleading, as this Act would significantly affect every internet company due to the authorization regime and the associated compliance obligations. The Telecommunications Bill 2023, which was passed earlier this year, as well as the Act establishes a new authorization regime, requiring all telecommunication services to seek for authorization in order to operate within India.[78] Given the broad scope of communications and messaging, this concept can perfectly be used to all existing social media platforms such as WhatsApp, Facebook, X, Instagram, and others. It effectively establishes a licensing system for the internet. Non-compliant services in India may face the possibility of being blocked or prohibited, similar to the fate of TikTok.

Chapter IV of the Telecommunications Act of 2023 affords the Union government or a state government the prerogative to assume control over any telecommunication service or network in the occurrence of a public emergency or safety concern. The aforementioned provision grants the authorities of both the Union and state governments the power to engage in the interception, detention, or non-transmission of messages originating from an individual or a specific group of individuals. The implementation of this singular measure confers upon officials an extensive array of powers, enabling them to exercise control and surveillance over all forms of communication transmitted across the entirety of the telecommunications network, with the primary objective of ensuring public safety.[79]

The legislation additionally stipulates the compulsory implementation of biometric authentication for all individuals utilizing social media platforms, to be facilitated by telecommunication service providers. The aforementioned measure mandates the obligatory provision of personal identification details for all modes of communication, thereby extending the Know Your Customer (KYC) framework of India to encompass the realm of the internet. In order to elucidate the efficacy of these aforementioned provisions, let us consider the hypothetical scenario wherein the Delhi Police endeavors to obtain comprehensive access to the complete set of particulars pertaining to each and every individual engaging in the act of tweeting during the farmers' protest. The objective of such an endeavor would be to impede the dissemination of any message containing a specific hashtag or keyword, as well as to prevent individuals from accessing their own respective accounts.[80] The comprehensive provisions outlined in this Bill afford the police and intelligence agencies the capacity to engage in persistent surveillance of dissenting factions, encompassing individuals such as leaders within the agricultural community or students who may partake in acts of protest.

The potential peril associated with the government's establishment of encryption standards for telecommunication services is noteworthy, particularly in light of the Government of India's expressed inclination to undermine the encryption protocols employed by popular messaging platforms such as WhatsApp and Signal. This inclination, if realized, has the potential to significantly encroach upon individuals' privacy rights.

78 INDIA. India Code. *Telecommunications Bill, 2022*. Clause 3(2) and Clause 4.

79 INDIA. India Code. *Telecommunications Act, 2023*. Chapter IV.

80 PANJIAR, Tejasi; WAGHRE, Prateek. Telecom Bill 2023 is a repackaged version of the archaic colonial law. *The Wire*, 20 dec. 2023. Available at: https://thewire.in/government/telecom-bill-2023-is-a-repackaged-version-of-the-archaic-colonial-law. Access on: 27 jan. 2024.

5 Conclusion

India's judgments about the convergence of laws, technology, and public expectations have a global influence. The rulings not only affected the lives of its citizens, but also influenced worldwide perspectives on surveillance, digital privacy, and governance. India played a crucial role in this matter, and its efforts to strike a balance between internet privacy and security likely had an impact on the broader conversation around these significant subjects. The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's unique strategy to protect personal data, showcasing the result of comprehensive deliberations after its first draft. The enactment of this data protection legislation is a pivotal measure in ensuring the security of personal data, specifically addressing long-standing requirements in light of the growing number of internet users, data creation, and international commerce. The DPDP Act represents India's distinct position on contemporary data protection, enhanced by thorough discussions held after the first formulation. Although its requirements are not as comprehensive as those of regulations such as European Union's Global Data Protection Regulation [Regulation (EU) 2016/679], it requires a substantial change in the way Indian enterprises handle privacy and personal data. In a similar vein, the Telecommunication Act 2023 has brought about significant changes, replacing the outdated Telegraph Act 1885 and the Wireless Telegraphy Act 1933. However, it is worth noting that there are some contentious provisions regarding safety standards and public emergencies. These provisions grant the government extensive power, potentially encroaching on citizen privacy with limited accountability for governing officers.

Privacy should be seen as a complex and nuanced concept, rather than a simplistic binary idea. It is important to note that not all data sharing automatically leads to manipulation. Discovering a way to securely share sensitive information while preserving its confidentiality is a feasible endeavor. Maintaining the privacy of personal information is of utmost importance in creating a feeling of confidentiality. In order to accomplish this, it is crucial to establish well-defined privacy guidelines, find a middle ground between the interests of those who have been given the information and the rights of individuals, and consistently follow ethical principles when dealing with sensitive data. It is of utmost importance that the government adopts a proactive approach in tackling data privacy concerns and ensuring that tech companies are held responsible for their utilization of personal information. Through the promotion of transparency and the establishment of accountability, digital privacy rights can be significantly enhanced.

References

ALLEN, Anita. *Unpopular privacy*: what must we hide? studies in feminist philosophy. New York: Oxford University Press, 2011.

BARLETT, Jamie. *The people vs tech*: how the internet is killing democracy (and how to save it). London: Ebury Press, 2018.

BHATIA, Gautam. State surveillance and the right to privacy in India: a constitutional biography. *National Law School of India Review*, v. 26, n. 2, p. 127-158, 2014.

BLOOMBERG NEWS. The great firewall of China. *Bloomberg*, 12 out. 2017. Available at: https://www.bloomberg.com/view/quicktake/great-firewall-of-china. Access on: 19 jan. 2024.

CONFESSORE, Nicholas. Cambridge Analytica and Facebook: the scandal and the fallout so far. *The New York Times*, 4 apr. 2018. Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Access on: 5 jan. 2023.

DESOMBRE, Winnona *et al*. *Countering cyber proliferation*: zeroing in on access-as-a-service. Washington, DC: Atlantic Council, 2021. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive--Cyber-Capabilities-Proliferation-Report-1.pdf. Access on: 22 jan. 2024.

DURAISWAMI, Dhiraj R. Privacy and data protection in India. *Journal of Law & Cyber Warfare*, v. 6, n. 1, p. 166-186, 2017. Available at: https://cybersecuritysummit.com/wp-content/uploads/2017/10/JLCW_6-1_Cyber--Enhanced-Sanction-Strategies_Do-Options-Exist.pdf. Access on: 20 jan. 2024.

ENGELKE, Peter. *AI, society, and governance*: an introduction. Washington, DC: Atlantic Council, 2020. Available at: http://www.jstor.org/stable/resrep29327. Access on: 4 jul. 2024.

EUROPEAN COMISSION. *EU Charter of Fundamental Rights*. 2000. Available at: http://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life#:~:text=Everyone%20has%20the%20right%20to,family%20life%2C%20home%20and%20communications. Access on: 18 jan. 2024.

FELDSTEIN, Steven; KOT, Brian. Global context of commercial spyware and digital forensics. *In*: FELDSTEIN, Steven; KOT, Brian. *Why does the global spyware industry continue to thrive?*: trends, explanations, and responses. Washington, DC: Carnegie Endowment for International Peace, 2023. p. 8-11. Available at: https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf. Access on: 22 jan. 2024.

GALETTA, Antonella. The changing nature of presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?. *European Journal of Law and Technology*, v. 4, n. 2, 2013. Available at: https://ejlt.org/index.php/ejlt/article/view/221/377. Access on: 24 jan. 2024.

GLOBAL COMMISSION ON INTERNET GOVERNANCE. Toward a social compact for digital privacy and security. *In*: GLOBAL COMMISSION ON INTERNET GOVERNANCE. *Cyber security in a volatile world*. Waterloo: Centre for International Governance Innovation, 2017. p. 121-131. Available at: http://www.jstor.org/stable/resrep05239.14. Access on: 27 dec. 2023.

GOODMAN, Matthew P.; GERSTEL, Dylan. Championing data governance. *In*: REINSCH, William; MILLER, Scott (ed.). *Sharpening America's innovative edge*. Washington, DC: Center for Strategic and International Studies (CSIS), 2020. p. 21-24.

GREENWALD, Glenn. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*, 11 jun. 2013. Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa--whistleblower-surveillance. Access on: 28 dec. 2023.

GURUSWAMY, Menaka. Justice K. S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors, Writ Petition (Civil) No. 494 of 2012. *The American Journal of International Law*, v. 111, n. 4, p. 994-1000, 2017. Available at: https://www.jstor.org/stable/26568904. Access on: 26 jan. 2024.

INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 36.

INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 7(b).

INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 17(1)(c).

INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 17(2)(a).

INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 17(5).

INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Section 17(3).

INDIA. India Code. *Digital Personal Data Protection Act, 2023*. Sections 9(1) to 9(3).

INDIA. India Code. *Information Technology Act*, *2000*. Section 2(1)(w).

INDIA. India Code. *Telecommunications Act, 2023*. Chapter 4.

INDIA. India Code. *Telecommunications Act, 2023*. Section 2.

INDIA. India Code. *Telecommunications Act, 2023*. Section 3(1).

INDIA. India Code. *Telecommunications Bill, 2022*. Clause 3(2) and Clause 4.

INDIA. Supreme Court. *JUSTICE K. S. Puttaswamy Vs. Union of India 10 SCC 1*. 2017.

KAMPMARK, Binoy. Restraining the surveillance state: a global right to privacy. *Journal of Global Faultlines,* v. 2, n. 1, p. 1-16, 2014. Available at: https://doi.org/10.13169/jglobfaul.2.1.0001. Access on: 4 jul. 2024.

KEMP, Simon. Digital 2023: global overview report. *Datareportal*, 26 jan. 2023. Available at: https://datareportal.com/reports/digital-2023-global-overview-report. Access on: 27 dec. 2023.

KESSLER, David J. *et al*. A comparative analysis of indian privacy law and the asia-pacific economic cooperation cross-border privacy rules. *National Law School of India Review*, v. 26, n. 1, p. 31-61, 2014.

LEPORE, Jill. Edward Snowden and the rise of whistle-blower culture. *The New Yorker*, 16 sep. 2019. Available at: https://www.newyorker.com/magazine/2019/09/23/edward-snowden-and-the-rise-of-whistle-blower-culture. Access on: 28 dec. 2023.

LUTHRA, Samarth Krishan; BAKHRU, Vasundhara. Publicity rights and the right to privacy in India. *National Law School of India Review*, v. 31, n. 1, p. 125-148, 2019.

MAGRANI, Eduardo. Hacking the electorate: thoughts on misinformation and personal data protection. *Konrad Adenauer Stiftung*: Facts & Findings, n. 399, 2020. Available at: https://www.jstor.org/stable/resrep25290. Access on: 31 dec. 2023.

MCCURRY, Justin. South Korea spy agency admits trying to rig 2012 presidential election. *The Guardian*, 4 aug. 2017. Available at: https://www.theguardian.com/world/2017/aug/04/south-koreas-spy-agency-admits-trying-rig-election-national-intelligence-service-2012. Access on: 29 dec. 2023.

NACHIAPPAN, Karthik *et al*. Digital and technology. *In*: SÁNCHEZ-CACICEDO, Amaia (ed.). *EU-India relations*: gaining strategic traction?. Paris: European Union Institute for Security Studies (EUISS), 2024. Available at: http://www.jstor.org/stable/resrep57929.7. Access on: 4 jul. 2024.

NOSTHOFF, Anna-Verena; MASCHEWSKI, Felix. The platform economy's infrastructural transformation of the public sphere: Facebook and Cambridge Analytica revisited. *Philosophy & Social Criticism*, v. 50, n. 1, p. 178-199, 2024. Available at: https://doi.org/10.1177/01914537231203536. Access on: 8 jan. 2024.

O'NEIL, Cathy. *Weapons of math destruction*: how big data increases inequality and threatens democracy. New York: Crown, 2016.

PALIWAL, Aishwarya. Telecommunications Bill receives president's assent, becomes law. *India Today*, 25 dec. 2023. Available at: https://www.indiatoday.in/law/story/telecommunications-bill-receives-president-droupadi-murmu-assent-becomes-law-2480283-2023-12-25. Access on: 26 jan. 2024.

PANJIAR, Tejasi; WAGHRE, Prateek. Telecom Bill 2023 is a repackaged version of the archaic colonial law. *The Wire*, 20 dec. 2023. Available at: https://thewire.in/government/telecom-bill-2023-is-a-repackaged-version-of-the-archaic-colonial-law. Access on: 27 jan. 2024.

POZEN, David E. Privacy-privacy tradeoffs. *The University of Chicago Law Review*, v. 83, n. 1, p. 221-247, 2016. Available at: https://www.jstor.org/stable/43741598. Access on: 18 jan. 2024.

PRESIDENT signs Telecom Act, rulemaking to follow for implementation. *The Hindu*, 25 dec. 2023. Available at: https://www.thehindu.com/news/national/president-signs-telecom-act-rulemaking-to-follow-for-implementation/article67674004.ece. Access on: 26 jan. 2024.

RICHARDS, Neil. *Why privacy matters*. New York: Oxford University Press, 2022.

RYNGAERT, Cedric; TAYLOR, Mistale. The GDPR as global data protection regulation?. *AJIL Unbound*, v. 114, p. 5-9, 2020. Available at: https://doi.org/10.1017/aju.2019.80. Access on: 23 jan. 2024.

SOLOVE, Daniel J. *The digital person*: technology and privacy in the digital age. New York: NYU Press, 2004.

SPEED, John Gilmer. The right of privacy. *The North American Review,* v. 163, n. 476, p. 64-74, 1896. Available at: http://www.jstor.org/stable/25118676. Access on: 4 jul. 2024.

UN Human Rights Council creates special rapporteur on right to privacy. *International Justice Resource Center*, 22 apr. 2015. Available at: https://ijrcenter.org/2015/04/22/un-human-rights-council-adopts-resolution-to-create-special-rapporteur-on-the-right-to-privacy/. Access on: 25 jan. 2024.

UNITED NATIONS. General Assembly backs right to privacy in digital age. *UN News*, 19 dec. 2013. Available at: https://news.un.org/en/story/2013/12/458232. Access on: 25 jan. 2024.

UNITED NATIONS. *International covenant on civil and political rights*. New York: United Nation, 1966. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Access on: 18 jan. 2024.

UNITED NATIONS. *Universal Declaration of Human Rights*. New York: United Nations, 1948. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks. Access on: 15 jan. 2024.

ÜNVER, H. Akın. *Politics of digital surveillance, national security and privacy*. Istanbul: Centre for Economics and Foreign Policy Studies, 2018. Available at: https://www.jstor.org/stable/resrep17009. Access on: 27 dec. 2023.

WANG, Maya. China's dystopian push to revolutionize surveillance. *Human Rights Watch*, 18 aug. 2017. Available at: https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance. Access on: 19 jan. 2024.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890. Available at: https://doi.org/10.2307/1321160. Access on: 24 jan. 2024.

WEISER, Mark. The computer for the 21st century. *Scientific American*, 1991. Available at: https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf. Access on: 28 dec. 2023.

YOKOHAMA, Shinichi. Private sector and the regional level. *In*: SAALMAN, Lora (ed.). *Integrating cybersecurity and critical infrastructure*: national, regional and international approaches. Solna: Stockholm International Peace Research Institute, 2018. p. 23-28. Available at: https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity_0.pdf. Access on: 23 jan. 2024.

ZEEBIZ WEBTEAM. Mark Zuckerberg talks of using Facebook to build a better global community. *Zee Business*, 17 feb. 2017. Available at: https://www.zeebiz.com/companies/news-mark-zuckerberg-talks-of-using-facebook-to-build-a-better-global-community-12573. Access on: 12 jan. 2024.

ZITTRAIN, Jonathan L. *et al*. Don't panic: making progress on going dark debate. *Berkman Center Research Publication*, 1 feb. 2016. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552576. Access on: 20 jan. 2024.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. London: Profile Books, 2019.

Para publicar na revista Brasileira de Políticas Públicas, acesse o endereço eletrônico www.rbpp.uniceub.br
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.