WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Impact of Technology on Privacy Laws: Challenges and Remedies

Preetam Kumar Pradhan[1], Namrata Singh[2], Akshita Sona[3] and Divyangi Lenka[4]

[1]Student of KSOL, 2283125, Contact:- 7847067601, Email- preetamprdhn@gmail.com
[2]Student of KSOL, 2383067, Email- 2383067@kls.ac.in, Contact:-9801511615
[3]Student of KSOL, 2383014 Phone no. 9155177992, Email: 2383014@kls.ac.in
[4]Student of KSOL, 2383042, Contact:- 8480468435, Email- 2383042@kls.ac.in

ABSTRACT

The rapid progress of technology has significantly transformed various facets of society, including the realm of privacy laws. This study delves into the intricate interplay between technology and privacy regulations, scrutinizing the challenges presented and potential solutions. As digital platforms continue to proliferate, individuals face escalating risks of privacy violations, spanning from data exploitation to surveillance. The emergence of artificial intelligence and biometric tools further complicates this landscape, prompting concerns regarding consent, data control, and the preservation of anonymity. Furthermore, the global reach of technology transcends geographical borders, creating jurisdictional complexities for policymakers to navigate. This research investigates the effectiveness of existing privacy laws in adapting to technological progress, shedding light on areas of deficiency and incongruity. Additionally, it explores novel strategies such as privacy-enhancing technologies, encryption, and decentralized systems to address privacy threats. Through the examination of case studies and legal frameworks across diverse jurisdictions, this study aims to offer valuable insights for policymakers, legal practitioners, and technology experts to navigate the evolving dynamics of technology and privacy. Ultimately, the objective is to strike a balance between technological advancement and safeguarding individual privacy rights in the digital era.

Keywords:

Technology: Refers to the application of scientific knowledge for practical purposes, which has rapidly evolved and impacted various aspects of society.

Privacy laws: Legal regulations designed to protect individuals' personal information from unauthorized access or disclosure.

Study: A systematic investigation or analysis aimed at understanding a particular phenomenon or issue.

Interplay: The dynamic interaction or relationship between two or more elements, in this context, between technology and privacy regulations.

Challenges: Obstacles or difficulties that arise in the process of addressing privacy concerns amidst technological advancements.

Digital platforms: Online environments or services where users interact and share information, which pose risks of privacy violations.

Artificial intelligence: Intelligence demonstrated by machines, which introduces complexities in privacy discussions due to its ability to analyze and process vast amounts of data.

Biometric tools: Technologies that analyse physical or behavioural characteristics for identification or authentication, raising questions about privacy and consent.

Jurisdictional complexities: Issues arising from the global nature of technology, which challenge policymakers in enforcing privacy laws across different regions.

Privacy-enhancing technologies: Tools and techniques designed to enhance privacy protection, such as encryption and decentralized systems, aiming to mitigate privacy threats in the digital landscape.

Introduction

Over the past few decades, the rapid evolution of technology has drastically altered various facets of human existence, including communication, commerce, and interaction with the environment. Among the most profoundly impacted domains is privacy, as the relentless march of digital progress continuously reshapes its boundaries, presenting both obstacles and opportunities for policymakers, legal experts, and society at large.[1]

This study seeks to explore the repercussions of technological advancements on privacy legislation, with a focus on identifying challenges and potential solutions to mitigate negative consequences. The widespread embrace of social media, internet-enabled gadgets, and extensive data analysis has rendered personal information increasingly susceptible to exploitation and abuse. This erosion of privacy prompts critical inquiries into individual freedom, safety, and the distribution of authority among individuals, corporations, and governments.

By scrutinizing real-world examples, legal structures, and academic analyses, this research aims to offer a thorough grasp of the intricate relationship between technology and privacy laws. Furthermore, it will delve into emerging trends like facial recognition software, biometric data gathering, and surveillance methodologies, illuminating their implications for privacy rights and civil liberties.

Ultimately, this endeavor seeks to enrich the ongoing conversation about privacy in the digital era, providing valuable insights into the challenges posed by technological progress and suggesting strategies to safeguard individuals' privacy rights in an increasingly interconnected society.

Research Methodology

Research Questions

1. How has the evolution of technology influenced the effectiveness and enforcement of existing privacy laws, and what are the key challenges posed to maintaining individual privacy rights in the digital age?

2. What strategies and remedies can policymakers, legal experts, and technology stakeholders implement to address the gaps and shortcomings in current privacy laws, ensuring adequate protection for individuals amidst advancing technological capabilities and emerging privacy threats?

Literature Review

Research Question 1

The evolution of technology has significantly impacted the effectiveness and enforcement of existing privacy laws, presenting various challenges to maintaining individual privacy rights in the digital age. [2]As technology continues to advance rapidly, privacy laws struggle to keep pace with emerging issues such as big data analytics, artificial intelligence (AI), and the Internet of Things (IoT). Technology's breakneck pace has left existing privacy laws struggling to keep up. While advancements offer tools like encryption and anonymization, they also create unprecedented data collection capabilities and enforcement difficulties.

Information privacy refers to the desire of individuals to control or have some influence over data about themselves. Advances in information technology have raised concerns about information privacy and its impact.[3] This abstract delves into this complex scenario, highlighting how technology shapes privacy law and the key challenges we face in safeguarding individual privacy in the digital age. However, uncontrolled access to information and personal data kept in many databases presents a chance for digital age technologies to breach some fundamental principles of information security and privacy. The research aims to identify some unique aspects of information and personal data protection and to provide an overview of the primary threats to user security and privacy. Technological advancements like cloud computing, the advancements in artificial intelligence while offering progress, has a dark side. Malicious technology each with its own nefarious aims. Viruses, trojans, deepfakes, cryptocurrency mining malware, etc are some examples. The data technology can be broadly classified into two categories:-

1) The technology used in Capturing and Storing Data.

2) The method used while processing data. However, due to the exponential development in the amount of data we transmit and collect online, privacy issues are more crucial than ever. As a futurist, I think it is imperative to look into the topic of privacy in the age of artificial intelligence and to find out more about how AI impacts our privacy and personal data.

---

[1] Zeynep Tufekci, "We Need to Take Back Our Privacy," The New York Times, May 19, 2022, https://www.nytimes.com/2022/05/19/opinion/privacy-technology-data.html

[2] Alaknanda Duggirala, "Data Privacy Protection in India," Institute of Law, Nirma University, https://law.nirmauni.ac.in/data-privacy-protection-in-india-technology-vis-a-vis-law/ (accessed February 18, 2024).

[3] Wellisz, C. (2016). The Dark Side of Technology. Finance & Development, 53(3). And Alexander, John. "How Technology is Killing Privacy." In Honors Projects, Grand Valley State University, 397, 2015.

The amount of data being collected and processed is often so large that it exceeds the capacity of the current laws, which were designed for less complex information ecosystems and have gaps in their protection[4]. Modern technologies like facial recognition and the Internet of Things raise new privacy issues that aren't really addressed by current laws. Furthermore, it becomes very difficult to enforce restrictions. To maintain regulations that are applicable and enforceable, privacy laws must be updated to take into account newly developed technologies and data activities. People must have control over the collection, use, and sharing of personal data in order for there to be transparency and accountability.

India navigates a complex digital terrain where personal data fuels both opportunity and privacy concerns. Existing laws offer fragmented protection. The Constitution implies a right to privacy, but specific details reside in scattered regulations like the IT Act and sectoral guidelines. These cover aspects like data security, sensitive data protection, and consent, but their limitations are stark. The IT Act's definition of "personal data" is narrow, consent mechanisms are ambiguous, and a crucial Data Protection Authority is yet to be established.

These limitations are amplified by rapid technological advancements and challenges like cross-border data flows. While the Personal Data Protection Bill aims to provide a comprehensive framework, concerns linger regarding its alignment with the right to privacy and potential impact on free speech.

Moving forward, India needs a robust privacy ecosystem. Strengthening existing laws, enacting a comprehensive and balanced privacy law, and establishing strong enforcement mechanisms are crucial. Only then can India ensure individual privacy thrives in its dynamic digital landscape.

Impact of Technology on Privacy Laws

The evolution of technology has transformed the way data is collected, processed, and shared, posing significant challenges to the effectiveness and enforcement of existing privacy laws. One major impact is the sheer volume of data generated by individuals through their online activities, social media interactions, and connected devices.[5] This vast amount of data makes it challenging for privacy laws to adequately regulate and protect personal information.

Furthermore, advancements in data analytics and AI have enabled companies and governments to extract valuable insights from massive datasets, raising concerns about the potential misuse of personal information. Privacy laws often struggle to address these complex data processing techniques, leading to gaps in protection and enforcement.

Moreover, the global nature of the internet and digital economy complicates the enforcement of privacy laws across different jurisdictions. With data flowing seamlessly across borders, regulators face challenges in coordinating enforcement actions and ensuring consistent protection of privacy rights worldwide.

Challenges to Maintaining Individual Privacy Rights

In the digital age, several key challenges pose threats to maintaining individual privacy rights:

1. The increasing occurrence of data breaches and cybersecurity risks puts people's private information at risk of being misused or accessed by unauthorized parties. Organizations struggle to prevent and mitigate the impact of data breaches, which can result in privacy violations and identity theft, despite the existence of data protection regulations such as the California Consumer Privacy Act (CCPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union.
2. Government Intrusion and Surveillance Technology: Governments and law enforcement agencies are employing an increasing amount of surveillance technology, such as facial recognition software and mass surveillance programs, to track people's whereabouts. These technologies raise concerns about pervasive surveillance, the erosion of private freedoms, and potential abuses of power by government authorities[6].
3. Lack of Consent and Transparency: Many consumers are unaware of the ways in which online service providers and platforms collect, utilize, and distribute personal data about them. Furthermore, complex permission processes and privacy legislation often make it more difficult for users to make informed decisions about the protection of their data. The lack of true consent and transparency jeopardizes people's autonomy over their personal information and their right to privacy.

[4] Bole, Dhriti. "Right to Privacy in Digital Age." Manupatra, December 27, 2022, https://articles.manupatra.com/article-details/Right-to-Privacy-in-Digital-Age.

[5] he Stanford Encyclopedia of Philosophy, "Information Technology and Privacy", Stanford University, November 20, 2014, https://plato.stanford.edu/entries/it-privacy/. And Frischmann, Brett M., and Evan Selinger. Re-Engineering Humanity: Automation and the Future of Work. The MIT Press, 2020.

[6] Thomson Reuters. (n.d.). Internet Privacy Laws Revealed - How Your Personal Information is Protected Online. Retrieved February 18, 2024, from https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online.

4. Algorithmic prejudice and discrimination: AI systems used in banking, law enforcement, and recruitment are just a few of the industries where they may perpetuate prejudice and discrimination against particular groups based on racial, gender, or socioeconomic characteristics. Because biased algorithms can lead to unfair treatment and privacy violations, they have the potential to worsen societal inequities that currently exist.
5. [7]Data Monetization and Commercial Exploitation: One method that many firms monetize personal data is by selling user information to third parties for targeted advertising and other commercial applications. Data-driven business models promote innovation and economic success, but they also raise moral concerns about the commoditization of personal information and its potential impact on individuals' right to privacy.[8]

Analysis

We have interviewed 100 people in city of bhubaneswar, patia road in an survey.

Types of privacy and digital threats people of bhubaneshwar, odisha has suffered related to mobile phones:

1. Data Breaches: Unauthorised access to personal data stored on the device or transmitted over networks.

2. Location Tracking: Apps and services collecting and potentially sharing user's location without consent.

3. Personal Information Collection: Apps collecting sensitive information like contacts, messages, or call logs without user knowledge.

4. Device Fingerprinting: Tracking users across apps and websites based on unique device identifiers.

5. Camera and Microphone Hijacking: Malicious apps or malware gaining access to the device's camera and microphone.

6. Identity Theft: Theft of personal information stored on the device for fraudulent purposes.

7. Phishing Attacks: Attempts to trick users into revealing personal information through fake apps, messages, or websites.

8. Malware: Viruses, trojans, and other malicious software designed to steal data, spy on users, or disrupt device functionality.

9. Phishing: Attempts to trick users into revealing sensitive information by posing as legitimate entities through messages, emails, or fake websites.

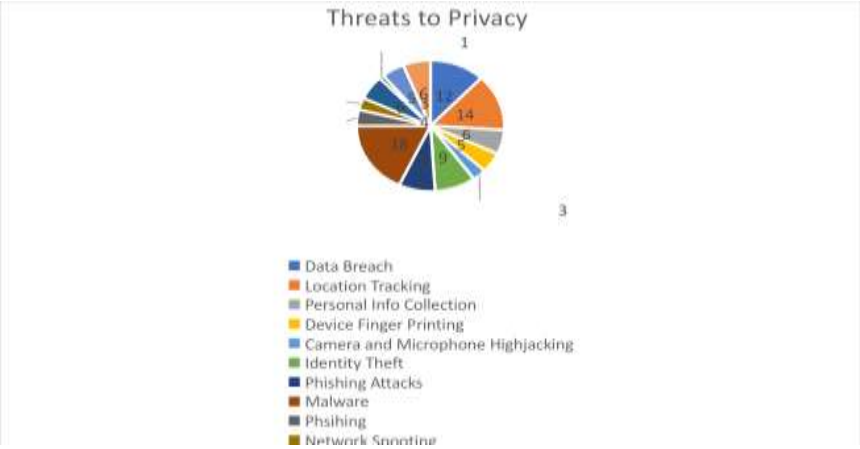
10. Network Spoofing: Creating fake Wi-Fi networks to intercept and manipulate data transmitted by the device.

11. Bluetooth and NFC Hacking: Exploiting vulnerabilities in Bluetooth or NFC connections to gain unauthorized access to the device.

12. App Vulnerabilities: Security flaws in mobile apps that can be exploited to compromise user data or device functionality.

13. Social Engineering: Manipulating users into divulging sensitive information or performing actions that compromise their security.

14. Unauthorised Acces:- Unauthorized access to the device through stolen or weak passwords, biometric spoofing, or other means.



Solutions and Mitigation Strategies

Addressing these challenges requires a multi-faceted approach involving policymakers, regulators, technology companies, and civil society. Key solutions and mitigation strategies include:

[7] Mathias, Stephen. 2023. "India Passes Digital Personal Data Protection Act." Hunton Andrews Kurth LLP. August 22. https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/.

[8] Amitosh. "The Role of Technology in the Future and Its Impact on Society." Times of India, August 1, 2023, https://timesofindia.indiatimes.com/readersblog/amitosh/the-role-of-technology-in-the-future-and-its-impact-on-society-52565/.

1. Strengthening Data Protection Laws: To address new issues brought about by technological improvements, legislators should update and strengthen current privacy laws. To do this, requirements for openness must be strengthened, approval procedures must be tightened, and consequences for data breaches and privacy violations must be made more severe.
2. [9]Encouraging Privacy by Design: When creating new products and services, technology companies should take privacy concerns into account from the very beginning. Principles of privacy by design highlight proactive measures to decrease data collection, enhance data security, and provide users control over their personal data.
3. Improving Cybersecurity Measures: In order to stop data breaches and protect people's personal information, organizations need to give cybersecurity measures top priority. This entails carrying out frequent security audits, putting strong encryption protocols in place, and supporting staff education to increase their comprehension of cybersecurity best practices.
4. [10]Regulating Surveillance Technology: In order to protect people's right to privacy, lawmakers should enact laws that restrict how surveillance technology is used and ensure that the essential safety precautions are taken. This may mean tightening restrictions on mass surveillance initiatives, setting clear guidelines for the use of facial recognition technologies, and enhancing oversight protocols for government monitoring initiatives.
5. Encouraging Ethical AI Practices: Tech companies and AI developers should prioritize ethical considerations while creating, developing, and deploying AI algorithms. This means reducing algorithmic bias, promoting algorithmic transparency, and conducting regular audits to identify and address any potentially discriminatory results.
6. Encouraging Users Through Knowledge and Awareness: It is necessary to inform users about their rights and responsibilities regarding data protection in order to empower them to make informed decisions online. This means making privacy settings, opt-out alternatives, and data collecting practices easily accessible to users of digital platforms.
7. Boosting International Cooperation: Governments, regulators, and business players need to cooperate internationally in order to effectively address global privacy concerns.[11] This means exchanging best practices for data protection, harmonizing privacy laws across different jurisdictions, and coordinating enforcement measures to stop cross-border privacy violations.

Research Question 2

With growing usage of internet, the risk of data privacy has also increased. In order to provide users with services, various websites, applications, and social media platforms frequently need to gather, process, and keep the personal data of those users. The technology advancement and use of artificial intelligence brings a question to the privacy data protection of individuals. Data protection means protecting your personal information from being misused by others. In India, misuse of personal data and breach of data privacy is one of the major concerns that is prevailing. Article 21 of the Indian Constitution guarantees the protection of life and personal liberty. In the landmark case of *K.S. Puttaswamy v. Union of India (2017),* the Supreme Court ruled that the right to privacy is a fundamental right under Article 21 of the Indian Constitution, making the protection of personal data and data privacy an integral part of that right. This suggests that each and every person is entitled to their own data. It gives them the choice over how their data is used, when to change their mind, and whether to object to processing of their data.

As everything being transferred to our digital gadgets in this era of digitalization, both our private and public data has been transferred. Consequently, the risks to our privacy regarding data have multiplied. In 2020 the India government banned 220 Chinese apps due to breach of data privacy of Indians. India's Ministry of Electronics and Information Technology stated "The Chinese apps were stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India.[12]" Despite the Information Technology Act of 2000's measures like section 72 and 43 A that addressed data safeguarding, the threat to data privacy persisted. Due to the rise in data privacy cases and the inadequacy of these legislation and statutory measures, data protection was not adequately addressed. This was especially true for personal data protection. After thorough review and modifications of the data privacy legal framework, The Digital Personal and Data Protect Act, 2023 came into force in August.

The DPDP Act seems to be less concerned with safeguarding people's privacy and more with the practical aspects of data processing.[13] The comprehensive norms for data handling, storing, and transmission make this abundantly evident, but it also seems that individual privacy rights are not given as much

[9] United Nations Conference on Trade and Development (UNCTAD). (2021, December 14). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worlwide.

[10] Thomson Reuters. (n.d.). Internet Privacy Laws Revealed - How Your Personal Information is Protected Online. Retrieved February 18, 2024, from https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online.

[11] Quach, Sara, et al. "Digital Technologies: Tensions in Privacy and Data." Journal of the Academy of Marketing Science 50.6 (2022): 1299-1323. https://doi.org/10.1007/s11747-022-00845-y.

[12] France Belanger et al , *Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems ,35,4,1017-1041(2011).*

[13] Marcelo Corrales Compagnucci , *Integrating law, technology, and design: teaching data protection and privacy law in a digital age,12,239-252,(2022).*

weight. The Act covers key ideas such as consent for data processing and duties for data fiduciaries. Though with the new law of data protection there still persist a problem of data breach and data privacy. The DPDP act have more provisions related to govt agencies and business but not for the individual whose data are collected and processed and have very less provisions and legislation for individuals concerned. A more privacy-centric approach would prioritise individual rights, including better control over the rights to personal data, clearer limitations on data processing, and more stringent exemption requirements. The legislation should establish strict privacy regulations that protect both personal and non-personal data, as well as all facets of data protection. Only when a privacy law is equally applied to private citizens, businesses, and the government can it fulfil its intended purpose. The government is released from some breach of data under Section 17(2) of the DPDP Act for reasons such as maintaining public order, safeguarding India's integrity, maintaining good relations with foreign governments, maintaining sovereignty, and preventing the conduct of any crimes that are punishable by law. Furthermore, it specifies that the Central Government may exempt some categories of Data Fiduciaries, such as startups, from the provisions of the DPDP Act. This will create a lot of problem among individuals concerning data privacy. The government itself and the cyber criminals can hack and misuse personal data. The legal experts and policymakers can bring change to this and should also held government responsible for breaching of any personal data. The state government as well as central government should be added in the provision for misappropriation of personal data. The Public sector organisations are at serious risk from government data breaches, thus protecting sensitive data is essential. It is recommended that access to sensitive data be restricted in accordance with job descriptions and duties. The government and policy makers should promote ethical data practices that respect individual autonomy and dignity. Government and tech firms should work together to create solutions that improve privacy.

There are concerns with the Act's handling of user data and business obligations. Users may not give their consent voluntarily if businesses are not required to provide them with adequate information about how their data is used, especially when it comes to data retention and sharing with third parties.[14] To overcome this there should be clear privacy notices to users for the information about data practices. There should also be embed privacy principles into the design of proud and services. Data collection of individuals should be minimum and it should also ensure default settings prioritize. The individuals should be educated about their privacy rights and how to exercise them. They should also be provided with accessible channels for them to control their sensitive personal data. There should be public awareness about privacy risk and rights and the measures they could take to protect their data.[15] The legal professional, policymakers and technologies should also be trained about the privacy issues and the laws relating to it so they could be more aware and make others aware about this.[16] There should also be strict privacy impact assessment before deploying new technologies and this should mandate for evert organization to follow for ensuring data privacy of individuals.

Conclusion

In conclusion, technological advancements have fundamentally altered the landscape around privacy laws and produced a multitude of barriers to protecting individual private rights in the digital age. The extensive use of digital technology has resulted in a multitude of complex issues, ranging from algorithmic prejudice and the commercial exploitation of personal data to data breaches and surveillance technologies, all of which require comprehensive answers and mitigation strategies. By enforcing stricter laws regarding data protection, promoting privacy by design, enhancing cybersecurity measures, regulating surveillance technologies, promoting moral AI practices, empowering users through awareness and education campaigns, and fostering international cooperation, stakeholders can address these issues and protect privacy rights in the digital age. India's privacy ecosystem requires proactive steps, legislative changes, and cooperation among stakeholders to safeguard peoples' digital age privacy rights. While there are many advantages to India's digital revolution, there are also serious privacy concerns. To properly handle the complexity of the digital age, India's current privacy framework—which is mostly embodied in the Information Technology (IT) Act and the newly passed Digital Personal Data Protection Act (DPDP) needs to be significantly improved. Strengthening data protection regulations, improving accountability and transparency frameworks, and giving people more control over their personal information should be the main goals of legislative changes. Furthermore, it is imperative to harmonise extant rules and regulations to provide an integrated privacy framework in order to address any gaps or discrepancies.

References

1. International Commission of Jurist ,*The Impact of technological development on the right to privacy,* 24,3 (1972).
2. Tamara Dinev et al, *Research Commentary : Informing Privacy Research Through Information System, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box ,* 26 , 3 , 639-655(2015).
3. Huseyin Cavusoglu et al , *Assessing the Impact of Granular Privacy Control On Content Sharing and Disclosure on Facebook, 27, 4, 848-879,* (2016).
4. H. Jeff Smith, *Information Privacy Research: An Interdisciplinary Review,35,4,27,(2011)*
5. France Belanger et al , *Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems ,35,4,1017-1041(2011).*

[14] International Commission of Jurist ,*The Impact of technological development on the right to privacy,* 24,3 (1972).

[15] H. Jeff Smith, *Information Privacy Research: An Interdisciplinary Review,35,4,27,(2011)*

[16] Huseyin Cavusoglu et al , *Assessing the Impact of Granular Privacy Control On Content Sharing and Disclosure on Facebook, 27, 4, 848-879,* (2016).

6. Marcelo Corrales Compagnucci , *Integrating law, technology, and design: teaching data protection and privacy law in a digital age,12,239-252,(2022).*
7. Alaknanda Duggirala, "Data Privacy Protection in India," Institute of Law, Nirma University, https://law.nirmauni.ac.in/data-privacy-protection-in-india-technology-vis-a-vis-law/ (accessed February 18, 2024).
8. Thomson Reuters. (n.d.). Internet Privacy Laws Revealed - How Your Personal Information is Protected Online. Retrieved February 18, 2024, from https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online.
9. United Nations Conference on Trade and Development (UNCTAD). (2021, December 14). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worlwide.
10. Hartzog, Woodrow. Privacy's Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press, 2018.
11. Quach, Sara, et al. "Digital Technologies: Tensions in Privacy and Data." Journal of the Academy of Marketing Science 50.6 (2022): 1299-1323. https://doi.org/10.1007/s11747-022-00845-y.
12. D'Souza, Anabelle Maria. "Technological Advances Leading to the Diminishing of Privacy Rights." LLM Theses and Essays, University of Georgia School of Law, 11, 2003. https://digitalcommons.law.uga.edu/stu_llm/11.
13. Amitosh. "The Role of Technology in the Future and Its Impact on Society." Times of India, August 1, 2023, https://timesofindia.indiatimes.com/readersblog/amitosh/the-role-of-technology-in-the-future-and-its-impact-on-society-52565/.
14. Turner, Jack. "The 8 Main Ways Technology Impacts Your Daily Life in 2024". tech.co, 2024. Retrieved from https://tech.co/vpn/main-ways-technology-impacts-daily-life.
15. Stepanovic, Ivana. (2014). Modern technology and challenges to protection of the right to privacy. Anali Pravnog fakulteta u Beogradu, 62, 167-178.
16. Fi, Keytech. "The Impact of Technology on Society: Positive and Negative Effects." LinkedIn, October 26, 2023 , https://www.linkedin.com/pulse/impact-technology-society-positive-negative-effects-keytech-fi.
17. Basu, Subhajit. (2010). Policy-Making, Technology And Privacy In India. Indian Journal of Law and Technology, 6(1), Article 3. doi:10.55496/WFJH9489. Retrieved from https://repository.nls.ac.in/ijlt/vol6/iss1/3.
18. LegalZoom. "Privacy and Technology: Is Technology Doing Away with Our Privacy?" https://www.legalzoom.com/articles/privacy-and-technology-is-technology-doing-away-with-our-privacy.
19. Buttarelli , Giovanni. "Privacy Matters: Updating Human Rights for the Digital Society." Health and Technology 7 (2017): 325-328. https://doi.org/10.1007/s12553-017-0198-y.'
20. Wentland, A. (2016). Imagining and enacting the future of the German energy transition: electric vehicles as grid infrastructure. Innovation: The European Journal of Social Science Research, 29(3), 285-302.
21. Mathias, Stephen. 2023. "India Passes Digital Personal Data Protection Act." Hunton Andrews Kurth LLP. August 22. https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/.
22. Thomson Reuters. (n.d.). Internet Privacy Laws Revealed - How Your Personal Information is Protected Online. Retrieved February 18, 2024, from https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online.
23. Wellisz, C. (2016). The Dark Side of Technology. Finance & Development, 53(3).
24. Alexander, John. "How Technology is Killing Privacy." In Honors Projects, Grand Valley State University, 397, 2015.
25. he Stanford Encyclopedia of Philosophy, "Information Technology and Privacy", Stanford University, November 20, 2014, https://plato.stanford.edu/entries/it-privacy/.
26. Frischmann, Brett M., and Evan Selinger. Re-Engineering Humanity: Automation and the Future of Work. The MIT Press, 2020.
27. Westin, Alan F. Privacy and Freedom. Atheneum, 1967.
28. Pasquale, Frank A. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, 2015.
29. Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. MIS Quarterly, 37(1), 275-298.
30. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355.

31. Miller, A. R. (1969). Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society. Michigan Law Review, 67(1089).

32. Ducange, P., Pecori, R., & Mezzina, P. (2018). A glimpse on big data analytics in the framework of marketing strategies. Soft Computing, 22(1), 325-342.

33. Kaplan, B. (2020). Seeing through health information technology: the need for transparency in software, algorithms, data privacy, and regulation. Journal of Law and the Biosciences, 7(1), lsaa062. https://doi.org/10.1093/jlb/lsaa062.

34. Zeynep Tufekci, "We Need to Take Back Our Privacy," The New York Times, May 19, 2022, https://www.nytimes.com/2022/05/19/opinion/privacy-technology-data.html.

35. Bole, Dhriti. "Right to Privacy in Digital Age." Manupatra, December 27, 2022, https://articles.manupatra.com/article-details/Right-to-Privacy-in-Digital-Age.