

FROM SOVEREIGNTY TO SURVEILLANCE: THE LEGAL LANDSCAPE OF “DIGITAL COLONIALISM” IN INDIA AND PAKISTAN

MUHAMMAD IMRAN ALI

Quaid-e-Azam Law College, Kasur, Pakistan

Email: principal.kasur@qlc.edu.pk

Abstract

This article examines how the practice of “digital colonialism” raises questions over conventional sovereignty and human rights in surveillance systems. The topic focuses on sovereignty on the internet level, with history and the impact of a new kind of sovereignty on national power. Based on case analysis, the article explores Indian legal measures of the 2000 Information Technology Act, the 2023 Digital Personal Data Protection Act and the 2016 Pakistan’s Prevention of Electronic Crimes Act and the 2023 Personal Data Protection Bill. Such analyses show the connection between legal procedures and surveillance, with the emphasis on the effects on freedom. In comparison with the EU’s General Data Protection Regulation (GDPR) and Vietnam’s cybersecurity law, notable differences emerge in how each framework balances national security concerns with fundamental rights to data privacy. Furthermore, the position of international law in determining digital sovereignty and human rights is evaluated. Lastly, the article explores digital dependency and the need to translate international norms into strong national laws that ensure data protection applies to foreign tech firms, shaping legal reforms and research priorities.

Keywords: cybersecurity laws, data protection, digital colonialism, digital sovereignty, India, internet, Pakistan, surveillance

Received: 25 January 2025 **Revised:** 22 March 2025 **Accepted:** 08 April 2025

In this article, the author argues that “digital colonialism” is the intentional influence of other countries through deploying, controlling, and extracting profit from technologies and data assets, making them dependent on foreign vendors and degrading their sovereignty. This modern sort of colonialism is similar to old-fashioned colonialism, whereas instead of controlling the physical space, one controls an online space.¹ The “digital colonialism” present in India and Pakistan takes shape through their technological dependence on external systems that both weaken their national control and give these systems access to perform surveillance activities. The online spaces fall under “digital colonialism” control because states depend on external technology companies, including

1 Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race & Law*, 24(2), 417–439. <https://doi.org/10.36643/mjrl.24.2.digital>

Google, Facebook, and Amazon.² Through sovereign powers, States can direct their internal operations, but foreign monitoring devices provide external entities complete control over national protection measures and database administration functions.

India and Pakistan have common backgrounds in digitalization that developed from their economic reforms and international openness. India enacted the 2000 Information Technology Act, while Pakistan implemented the Prevention of Electronic Crimes Act (PECA) in 2016. However, both governments encounter difficulties enforcing these laws. The user data controlled by foreign technology firms gets managed through offshore servers, which exposes users to risks of surveillance and exploitation. Aadhaar biometric identification systems in India³ and Pakistan's absence of domestic digital solutions serve as proof of their national cyber exposure.⁴ Rural areas, along with disadvantaged population groups, face further social exclusion because of the digital gap.

The Digital India and Digital Pakistan policies from both countries aim at digital transformation of governance, economy, and education, while persistent data ownership disputes and cybersecurity issues remain unresolved. Peaks of national security matters facing Pakistan are visible through its continuous blockings of X and YouTube, alongside India's current restrictions on Chinese products. Both nations need to create their independent digital systems along with stronger laws. The data protection initiatives of India are represented by the 2023 Digital Personal Data Protection Act, while Pakistan face difficulties in enacting personal data protection laws. A successful digital sovereignty initiative needs regional collaboration to oppose "digital colonialism" through the development of local technology and governance norms.

1. Concept of sovereignty and colonialism in a digital age

This paper investigates the changing concept of sovereignty as it has historically related to territorial mastery and independence through technological developments. The Westphalian model of sovereignty is defined itself by two core principles, including border

2 Kyris, G. (2022). State recognition and dynamic sovereignty. *European Journal of International Relations*, 28(2), 287-311. <https://doi.org/10.1177/13540661221077441>

3 Rao, U., & Nair, V. (2019). Aadhaar: Governing with biometrics. *South Asia: Journal of South Asian Studies*, 42(3), 469-481. <https://doi.org/10.1080/00856401.2019.1595343>

4 Akram, M. S., Mir, M. J., & Rehman, A. (2023). Dimension of cyber-warfare in Pakistan's context. *Journal of Positive School Psychology*, 7(6), 82-94.

integrity and state independence from outside interference.⁵ The advent of cyberspace created new complexities which alter the established sovereign principles. The digital age features a battle between two conflicting approaches that demonstrate worldwide power structures and administrative control of technical resources called digital sovereignty and digital colonialism.⁶

National control of digital systems, together with data protection and virtual processes, constitutes digital sovereignty for a nation. The European Union's General Data Protection Regulation (GDPR) indicates this concept because it forces companies of any location to protect EU citizens' data through strict privacy requirements. The 2017 Cybersecurity Law, established by China, obligates foreign technology companies to conform to national data localization requirements for maintaining cyber control within the Chinese digital space. National governments now understand that digital sovereignty involves more than data security standards since it directly impacts state security requirements. Foreign data stored anywhere in the world remains accessible to the United States law enforcement via the CLOUD Act, which demonstrates the concept of extraterritorial digital sovereignty. European countries, particularly France and Germany, have started developing GAIA-X and similar data initiatives to decrease their dependence on international digital infrastructure.⁷ The digital landscape globalization makes these policies part of a broader trend to increase decentralized and national digital management.

"Digital colonialism" emerges today as a new form of historic imperialist structures that oppose digital sovereignty. Technologically advanced nations, together with multinational corporation's control the digital infrastructure of developing countries. While doing so, they create dependencies which damage local sovereignty.⁸ The major U.S. technology companies, including Google, Facebook, and Amazon have established monopoly control over digital resources

5 Etzioni, A. (2018). *Happiness is the wrong metric*. Springer. https://doi.org/10.1007/978-3-319-69623-2_13, pp. 223-239.

6 Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, 98(6), 1977-1999. <https://doi.org/10.1093/ia/iiaa226>

7 Timmers, P. (2024). Sovereignty in the digital age. In H. Werthner (Ed.), *Introduction to digital humanism* (pp. 571-592). Springer. https://doi.org/10.1007/978-3-031-45304-5_36

8 Singler, S., & Babalola, O. (2024). Digital colonialism beyond surveillance capitalism? Coloniality of knowledge in Nigeria's emerging privacy rights legislation and border surveillance practices. *Social & Legal Studies*. <https://doi.org/10.1177/09646639241287022>

in developing countries, thus determining their technological frameworks while impeding their technological independence.⁹ Digital infrastructure governance by foreign actors reduces national autonomy, thus making countries vulnerable to outside directives in their political and economic management.

“Digital colonialism” manifests clearly through the telecommunications sector in Africa. Huawei, along with other corporations, provide inexpensive technology while retaining absolute control over network infrastructure. Nations face two interrelated consequences from this arrangement between connectivity and surveillance capabilities, since they receive their infrastructure from foreign providers. Global digital ownership regulation remains insufficient, thus making the current problems more severe. Despite its significant efforts, the Tallinn Manual on International Law Applicable to Cyber Operations cannot create legally-binding rules about cyberspace sovereignty because of which leaves developing nations vulnerable to cyber exploitation.¹⁰ “Digital colonization” has been revealed through Edward Snowden’s revelations as powerful nations conduct secret surveillance activities that monitor both their governmental and citizen targets abroad. Surveillance activities conducted against states lead to the destruction of their sovereignty through unwanted access to their confidential data.¹¹

Lawmakers need to develop systems which maintain national independence alongside modern business requirements. The implementation of data localization laws leads to better national control, yet produces negative effects of breaking up the internet and disrupting innovative solutions. The European Convention on Human Rights (ECHR) Article 8, together with United Nations Guiding Principles on Business and Human Rights, serve to protect the rights of privacy and sovereignty across cyberspace.¹² Achieving

9 Gu, H. (2024). Data, big tech, and the new concept of sovereignty. *Journal of Chinese Political Science*, 29, 591 – 612. <https://doi.org/10.1007/s11366-023-09855-1>

10 Tanodomdej, P. (2019). The Tallinn manuals and the making of international law on cyber operations. *Masaryk University Journal of Law and Technology*, 13(1), 67–86. <https://doi.org/10.5817/MUJLT2019-1-4>

11 Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: A critical empirical study of computer experts’ attitudes on commercial and state surveillance of the internet and social media post-Edward Snowden. *Journal of Information, Communication and Ethics in Society*, 15(4), 412–444. <http://dx.doi.org/10.1108/JICES-01-2016-0004>

12 Berkes, A. (2019). Human rights obligations of the territorial state in the cyberspace of areas outside its effective control. *Israel Law Review*, 52(2), 197–231. <https://doi.org/10.1017/S0021223719000050>

sovereignty in the digital era needs countries to work together with fair regulatory guidelines.

Sovereignty has developed into a modern concept which results from historical progress and technological progress. Generation of digital sovereignty by states aims to establish dominance over data operations and infrastructure networks while fighting against outside power. “Digital colonialism” creates dependence that attacks the self-sustaining capabilities of underdeveloped countries.¹³ Strong legal foundations, together with international cooperation, will create a fair sovereign digital environment to address these challenges.

2. “Digital colonialism” in India

The Indian version of “digital colonialism” exists through modern relationships of technological and economic dependence with foreign firms, including Google and Amazon. The economic and social-value of digital advances produces negative consequences for national autonomy and requires dependence upon foreign infrastructure in a way reminiscent of traditional colonial economic models.¹⁴ The digital governance framework in India consists of the 2000 Information Technology Act, as well as the 2023 Digital Personal Data Protection Act (DPDPA). The enforcement of data security measures under Section 43A of the IT Act is weak. Section 4 of the DPDPA requires data controllers in India to keep personal information in country-based storage facilities. The implementation challenges, as well as trade restrictions, create existing concerns. India faces challenges regarding digital sovereignty because foreign corporations control cloud systems while controlling social media and e-commerce operations across the country.¹⁵ Indian private data is extracted by foreign companies, which generate profits without giving adequate payment to users. Indian legislation under Section 69 of the IT Act grants surveillance powers to government authorities even though it lacks sufficient protection against misuse.

-
- 13 Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33, 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
 - 14 Dattani, K. (2023). Spectrally shape-shifting: Biometrics, fintech and the corporate-state in India. *Journal of Cultural Economy*, 17(4), 470–488. <https://doi.org/10.1080/17530350.2023.2176340>
 - 15 Ozalp, H., Ozcan, P., Dinckol, D., Zachariadis, M., & Gawer, A. (2022). Digital colonization of highly regulated industries: An analysis of Big Tech platforms’ entry into health care and education. *California Management Review*, 64(4), 78–107, p. 78. <https://doi.org/10.1177/00081256221094307>

Learned entities share information with state agencies while endangering civil rights protection. Indian “digital colonialism” debates become more complex because of surveillance tools such as the Central Monitoring System (CMS) and tools like NETRA that the government implements.¹⁶ Section 69B of the IT Act gives the government powers to conduct investigations that breach privacy rights while reducing judicial intervention. Foreign technological dependencies result in increased digital dependence because it decreases India’s ability to control its digital sphere. The “digital colonialism” system manifests when Indian governmental and financial data is stored by foreign providers such as Amazon Web Services (AWS) and Microsoft Azure.¹⁷

India faces external control because it depends on foreign cloud services, thus exposing itself to the US CLOUD Act provisions. The situation proves why domestic cloud solutions require immediate development. Critical sectors such as education continue to face data protection challenges as well as equitable access barriers because they depend on proprietary software, which demonstrates an immediate need for digital self-sufficiency.¹⁸

India’s selection of imported Learning Management Systems (LMSs) allows “digital colonialism” to thrive because it lacks Indian-developed open-source learning platforms. The Digital India initiative exists alongside foreign dependency because of public-private partnerships with multinational technological companies. A thorough reform of the DPDPA requires mandatory verification inspections and independent observation for effective implementation. Grants that support indigenous tech startup development will improve national self-reliance. Unaddressed measures will keep India as a subordinate digital entity, which threatens its national sovereignty and the digital rights of its citizens across developing digital environments.

16 Litton, A. (2015). The state of surveillance in India: The Central Monitoring System’s chilling effect on self-expression. *Washington University Global Studies Law Review*, 14(4), p. 799.

17 Atcha, N. M., Jagannadha Rao, D. B., & Polepally, V. (2024). A contemplate study on prominent cloud service providers: Amazon Web Service (AWS), Microsoft Azure, and Google Cloud Platform (GCP). In V. Bhateja, H. Lin, M. Simic, M. Attique Khan, & H. Garg (Eds.), *Cyber security and intelligent systems - Proceedings of eighth international conference on information system design and intelligent applications (ISDIA 2024)*, Volume 1 (Vol. 1056, pp. 223–233). Springer. https://doi.org/10.1007/978-981-97-4892-1_19

18 Singh, M., Adebayo, S. O., & Saini, M. (2021). Indian government e-learning initiatives in response to the COVID-19 crisis: A case study on online learning in Indian higher education system. *Education and Information Technologies*, 26, 7569–7607, p. 7569. <https://doi.org/10.1007/s10639-021-10585-1>

3. “Digital colonialism” in Pakistan

Taking the case of Pakistan, “digital colonialism” involves the dependent orientation towards foreign technology and information data harvesting with a weak domestic technological infrastructure.¹⁹ Some of these challenges are faced and dealt with under the existing laws, such as the 2016 PECA and 2023 Personal Data Protection Bill (PDPB) (still pending in the Parliament), however, such laws also reveal some deficiencies which are exploited by foreign entities. The 2016 PECA serves as Pakistan’s basic instrument to achieve effective cybercrime prevention. Under this legislation, Section 3 defines illegal access by unauthorized users, while Section 4 governs the unauthorized duplication or data transmission.

Nevertheless, enforcement measures under PECA are still insufficient, specifically in addressing the responsibilities of foreign firms engaged in operating within the cybersphere of Pakistan. For instance, the law is incapable of dealing squarely with global technology companies that harvest and sell consumer information without proper volition.

The 2023 Personal Data Protection Bill (PDPB), which is still waiting to be authenticated by Parliament, aims to fill in these gaps by passing a law that is well-equipped to fight for the privacy of data and users. According to Section 7 of the PDPB, personal sensitive data must be stored and processed within the borders of Pakistan. Despite the improvement of this provision in the aspect of digital sovereignty, the problems of its implementation are evident, for instance, the lack of adequate domestic facilities for data storage and computation. However, the said bill has few provisions for severe consequences for foreign violators; thus, giving advertisers the green light to act exploitatively. In contrast to the cross-border data transfer laws of international models like the GDPR, the PDPB indefensibly does not include rigid laws for cross-border data transfer, deepening the effects of “digital colonialism” even more.

Another aspect of “digital colonialism” in Pakistan is the surveillance practices of the government. Most surveillance tools include deep packet inspection and biometric data systems, and are developed by foreign corporations.²⁰ Under Section 32 of the

19 Shah, H. J., & Khan, A. (2023). Globalization and nation states: Challenges and opportunities for Pakistan. *Social Sciences & Humanities Open*, 8(1). <https://doi.org/10.1016/j.ssaho.2023.100621>

20 Ahmed, Z. S., Yilmaz, I., Akbarzadeh, S. & Bashirov, G. (2024). Contestations of internet governance and digital authoritarianism in Pakistan. *International Journal of Politics, Culture, and Society*. <https://doi.org/10.1007/s10767-024-09493-2>

PECA, the government maintains authority to maintain user data, yet no formal regulatory framework exists to protect against privacy violations or prevent misuse. The rights of the citizens perpetuate dependence on external forces for technology and infrastructural support.

The fight against “digital colonialism” in Pakistan demands three things: a local tech capacity construction effort, regulatory reform measures and an independent organization that monitors foreign tech companies alongside public-private digital platform development to decrease the future reliance on international institutions. For instance, South Korea has provided an example of how it has successfully nurtured effective domestic e-commerce markets with its kind policies and proper investment into technological platforms for its copy,²¹ such as Pakistan. All these steps need to be accompanied by cooperation with other countries to implement the experience and norms of protecting personal data and data sovereignty.

The “digital colonialism” in Pakistan serves as an expression of technological imperialism, which compromises national independence. PECA, together with PDPB, establishes a base, yet their enforcement requirements demand improvement. Government surveillance needs to develop mutually between transparency and effectiveness to regain public trust. If Pakistan fails to enhance its digital policies, it will experience sustained dependency, together with digital inequality, while missing out on real technological independence.

4. Coping with “digital colonialism” in other jurisdictions

“Digital colonialism” takes different forms in various countries because they have distinct approaches to digital sovereignty and surveillance measures, as well as foreign intervention levels. The analysis of Nigeria, Brazil, and Vietnam demonstrates individual methods for coping with “digital colonialism”, which India and Pakistan should adapt.

4.1. Confronting “digital colonialism” in Nigeria

The digital infrastructure of Nigeria depends mostly on worldwide technology providers such as Google, Facebook and Amazon. Foreign digital companies control the entire Nigerian digital market, which

21 Li, Y., He, Y., & Wu, R. (2023). Traversing the macroeconomic terrain: An exploration of South Korea’s economic responsiveness to cross-border e-commerce production technology alterations in the global arena. *Sustainability*, 15(15), p. 11719. <https://doi.org/10.3390/su151511719>

generates digital economic value that continues outside national borders. Local technology corporations face growth constraints because of their reliance on external companies, which restricts their capacity for both competitive activities and market innovation.²² The 2019 Nigeria Data Protection Regulation (NDPR), came into effect as a means to protect personal data for citizens. Weak enforcement exists because the system lacks sufficient funds alongside regulatory exemptions. The security needs of Nigeria cause a problem as the country depends heavily on foreign-made surveillance tools. The government's working relationship with international firms during data collection and monitoring activities triggers human rights violations through potentially weakening civil liberties.²³ The Nigerian example demonstrates that better local digital investments, together with stronger legal protections, are essential because they would decrease foreign dependency in information security.

4.2. Confronting “digital colonialism” in Brazil

Digital colonialism receives restrained attention from Brazil because the nation works to defend national autonomy while pursuing global digital marketplace integration. Brazil faces extensive pressure from international corporations, which seek dominance in its digital sector because it operates as one of the top economies in Latin America.²⁴ Brazil implemented the General Data Protection Law (LGPD) in 2020 to safeguard individual information as per EU's General Data Protection Regulation (GDPR) standards. According to LGPD, users must provide consent before data collection processes while also obtaining protection rights for their personal information and enabling data processors to maintain legal responsibility for data handling. Data processing under the LGPD must have explicit legal bases according to Articles 7 and 9, which protect both transparency and accountability. Brazil makes steady strides, but different hurdles remain regarding the development of digital sovereignty alongside surveillance policies. The country has formed partnerships with

-
- 22 Iheanachor, N., Umukoro, I., & Aránega, A. Y. (2023). Ecosystem emergence in emerging markets: Evidence from the Nigerian digital financial services ecosystem. *Technological Forecasting and Social Change*, 190, p. 122426. <https://doi.org/10.1016/j.techfore.2023.122426>
 - 23 Omotubora, A. (2021). How (not) to regulate data processing: Assessing Nigeria's Data Protection Regulation 2019 (NDPR). *Global Privacy Law Review*, 2(3), 186 – 199. <https://doi.org/10.54648/gplr2021024>
 - 24 Peron, A. E. D. R., & Evangelista, R. (2024). Beyond instrumentarianism: Automated facial recognition systems in Brazil and digital colonialism's violence. *Science, Technology and Society*, 29(4), 535-554. <https://doi.org/10.1177/09717218241281819>

multinationals, which leads to concerns about protecting data security alongside the issue of digital resource ownership within the nation. The implementation of facial recognition by police agencies leads to public arguments about constitutional rights violations, together with claims of biased treatment. Foreign technology enhances public security, but governments need to exercise strict rules to protect the freedom rights of their citizens.²⁵ Brazil serves as an example which proves that nations need complete legal systems to protect themselves from digital imperialism while continuing to develop technological advancements.

4.3. Confronting “digital colonialism” in Vietnam

Digital sovereignty in Vietnam operates with distinctive strategies than the approaches of Nigeria and Brazil. The Vietnamese government maintains strong digital control through which it protects national security while blocking external intrusion.²⁶ The 2018 Cybersecurity Law plays a crucial role in this strategy. The law requires foreign technology companies to maintain user data in Vietnam while providing must-have access to their data according to official requests from public authorities.²⁷ The digital sovereignty policy generates opposition because it endangers privacy rights while expanding surveillance activities and displaying broad regulatory risks that can lead to abuse and voluntarily inhibits innovative growth along with information distribution for national security aims.²⁸ Therefore, finding a balance between maintaining digital sovereignty and promoting technological advancement is a need. However, it is argued that excessive regulatory measures work against drawing foreign investors while dragging down technological advancement rates.²⁹ The policies implemented by Vietnam demonstrate that nations require digital infrastructure management control to compete in the economy.

25 Belli, L., Gaspar, W. B., & Zingales, N. (2024). Regulating facial recognition in Brazil: Legal and policy perspectives. In R. Matulionyte & M. Zalnieriute (Eds.), *The Cambridge handbook of facial recognition in the modern state*. Cambridge University Press, p. 228.

26 Thu, V. T. A. (2023). Protecting Vietnam’s sovereignty in cyberspace: Insights from human right laws. *The Age of Human Rights Journal*, 21.

27 Nam, B. T. N., & Hong, N. N. P. (2023). Addressing the challenges of data privacy protection law in Vietnam. *VNU Journal of Science: Legal Studies*, 39(1), 30-44, p. 35. <https://doi.org/10.25073/2588-1167/vnuls.4413>

28 Thu (2023), *supra* note 26.

29 Hang, N. H. B. (2024). Addressing fragmentation in Vietnam’s Data Protection Laws: Recommendations for a unified legal framework. *Vietnamese Journal of Legal Sciences*, 11(2), 14-26, p. 14. <https://doi.org/10.2478/vjls-2024-0008>

4.4. Lessons for India and Pakistan

The practical examples from Nigeria, along with Brazil and Vietnam, demonstrate important knowledge that India and Pakistan must learn regarding “digital colonialism” avoidance. Nigeria’s revealed enforcement structure deficiencies show the importance of legislative protection and independent regulatory regulators. Effective data governance systems in India and Pakistan require solutions for their current enforcement problems. Brazil’s LGPD serves as a detailed blueprint for India and Pakistan to implement both judicial and non-judicial “digital colonialism” controls. Both India and Pakistan need to establish proper controls for external tech power while simultaneously promoting the development of their own technology industries. For example, digital regulations in Vietnam display the significance of administrative oversight of tech firms from foreign countries, but face the challenge that excessive control measures may impede innovative potential. Besides, the two countries should establish data governance systems through their attention to protect user data rights while maintaining transparency and holding entities accountable.

5. “Digital colonialism” and the role of international law

There are legal tools to tackle “digital colonialism”, for instance, the United Nations Guiding Principles on Business and Human Rights (UNGPs). The UNGPs adopted in 2011 emphasizes the role of corporations’ entities in minimizing adverse human rights impacts and the role of the state in preventing such impacts.³⁰ The framework is built on three pillars: the international law includes the State’s obligation to fulfil human rights, corporations having the responsibility to respect human rights, while victims have a right to access justice. Guiding Principle 11 points on the concepts that require business enterprises not to cause harm to rights and provide ways to address this impact. They are essential in the digital world where multinationals depend on data and resources from the developing countries to exploit the natural resources endowment.

These protections are pursuant to international legal instruments such as the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR protects the right to privacy against a violation by arbitrary interference that forms part of “digital

30 Mutung’u, G. (2022). The United Nations guiding principles on business and human rights, women and digital ID in Kenya: A decolonial perspective. *Business and Human Rights Journal*, 7(1), 117–133. <https://doi.org/10.1017/bhj.2021.60>

colonialism” elements, like spying and data harvesting. Article 19 assures freedom of expression, which is under attack by censorship and regulation from overseas tech firms.³¹ Likewise, the African Charter on Human and Peoples’ Rights (ACHPR) places focus on economic rights. It is held that the exploitation of African resources by foreigners shall not supersede the local people’s rights. Article 21, which refers to people’s rights, entails the freedom to control their resources and change the digital sphere.³²

The most relevant international text regarding children’s rights is the Convention on the Rights of the Child (CRC), which also underlines both the prohibition of the exploitation of data as well as hazardous content. The provision of Article 16 is to protect children from intrusive surveillance and data gathering; in its response, it provides a clear and comprehensive legislative framework against such exploitation.³³ There is also another important factor operating to check “digital colonialism”, and that is the concerted efforts made by the States. Many essential issues of data protection, privacy, and, more generally, the use of technologies can be regulated with the help of multilateral agreements.

It becomes necessary that the rules of international law be implemented at the national level appropriately. These guidelines should be translated into strong national laws that show that data protection laws govern companies from other nations that sell technology products in their countries. It sustains civil liberties, thus creating an environment for technology advancement.

Conclusion

A combined solution requires Pakistan and India to create data protection measures that conform to universal human rights principles across worldwide standards. The data protection law of India needs revision to define governmental obligations better. Pakistan needs to enhance the approved rules regarding data consent and its restrictions, along with data minimization mandates. Organizations with independent oversight should implement monitoring of surveillance programs and enforce penalties against misuse of data.

31 De Baets, A. (2025). *A human rights view of the past*. Cambridge University Press.

32 Ekhtor, E. O. (2015). The impact of the African Charter on Human and Peoples’ Rights on domestic law: A case study of Nigeria. *Commonwealth Law Bulletin*, 41(2), 253–270. <https://doi.org/10.1080/03050718.2015.1049633>

33 Sandberg, K. (2018). Children’s Right to protection under the CRC. In A. Falch-Eriksen & E. Backe-Hansen (Eds.), *Human rights in child protection* (pp. 15–38). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-94800-3_2

Future investigations need to evaluate the social and economic results of digital dependency, along with developing substitute technology models for developing nations. Research conducted through comparative nation studies of Nigeria, Brazil, and Vietnam may lead to valuable findings. ●

References

- [1] Ahmed, Z. S., Yilmaz, I., Akbarzadeh, S. & Bashirov, G. (2024). Contestations of internet governance and digital authoritarianism in Pakistan. *International Journal of Politics, Culture, and Society*. <https://doi.org/10.1007/s10767-024-09493-2>
- [2] Akram, M. S., Mir, M. J., & Rehman, A. (2023). Dimension of cyber-warfare in Pakistan's context. *Journal of Positive School Psychology*, 7(6), 82-94
- [3] Atcha, N. M., Jagannadha Rao, D. B., & Polepally, V. (2024). A contemplate study on prominent cloud service providers: Amazon Web Service (AWS), Microsoft Azure, and Google Cloud Platform (GCP). In V. Bhateja, H. Lin, M. Simic, M. Attique Khan, & H. Garg (Eds.), *Cyber security and intelligent systems - Proceedings of eighth international conference on information system design and intelligent applications (ISDIA 2024), Volume 1* (Vol. 1056, pp. 223-233). Springer. https://doi.org/10.1007/978-981-97-4892-1_19
- [4] Belli, L., Gaspar, W. B., & Zingales, N. (2024). Regulating facial recognition in Brazil: Legal and policy perspectives. In R. Matulionyte & M. Zalnieriute (Eds.), *The Cambridge handbook of facial recognition in the modern state*. Cambridge University Press
- [5] Berkes, A. (2019). Human rights obligations of the territorial state in the cyberspace of areas outside its effective control. *Israel Law Review*, 52(2), 197-231. <https://doi.org/10.1017/S0021223719000050>
- [6] Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race & Law*, 24(2), 417-439. <https://doi.org/10.36643/mjrl.24.2.digital>
- [7] Dattani, K. (2023). Spectrally shape-shifting: Biometrics, fintech and the corporate-state in India. *Journal of Cultural Economy*, 17(4), 470-488. <https://doi.org/10.1080/17530350.2023.2176340>
- [8] De Baets, A. (2025). *A human rights view of the past*. Cambridge University Press
- [9] Ekhtator, E. O. (2015). The impact of the African Charter on Human and Peoples' Rights on domestic law: A case study of Nigeria. *Commonwealth Law Bulletin*, 41(2), 253-270. <https://doi.org/10.1080/03050718.2015.1049633>
- [10] Etzioni, A. (2018). *Happiness is the wrong metric*. Springer. https://doi.org/10.1007/978-3-319-69623-2_13
- [11] Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33, 369-378. <https://doi.org/10.1007/s13347-020-00423-6>

- [12] Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the internet and social media post-Edward Snowden. *Journal of Information, Communication and Ethics in Society*, 15(4), 412-444. <http://dx.doi.org/10.1108/JICES-01-2016-0004>
- [13] Gu, H. (2024). Data, big tech, and the new concept of sovereignty. *Journal of Chinese Political Science*, 29, 591-612. <https://doi.org/10.1007/s11366-023-09855-1>
- [14] Hang, N. H. B. (2024). Addressing fragmentation in Vietnam's Data Protection Laws: Recommendations for a unified legal framework. *Vietnamese Journal of Legal Sciences*, 11(2), 14-26. <https://doi.org/10.2478/vjls-2024-0008>
- [15] Iheanachor, N., Umukoro, I., & Aránega, A. Y. (2023). Ecosystem emergence in emerging markets: Evidence from the Nigerian digital financial services ecosystem. *Technological Forecasting and Social Change*, 190. <https://doi.org/10.1016/j.techfore.2023.122426>
- [16] Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, 98(6), 1977-1999. <https://doi.org/10.1093/ia/iiaa226>
- [17] Kyris, G. (2022). State recognition and dynamic sovereignty. *European Journal of International Relations*, 28(2), 287-311. <https://doi.org/10.1177/13540661221077441>
- [18] Li, Y., He, Y., & Wu, R. (2023). Traversing the macroeconomic terrain: An exploration of South Korea's economic responsiveness to cross-border e-commerce production technology alterations in the global arena. *Sustainability*, 15(15). <https://doi.org/10.3390/su151511719>
- [19] Litton, A. (2015). The state of surveillance in India: The Central Monitoring System's chilling effect on self-expression. *Washington University Global Studies Law Review*, 14(4)
- [20] Mutung'u, G. (2022). The United Nations guiding principles on business and human rights, women and digital ID in Kenya: A decolonial perspective. *Business and Human Rights Journal*, 7(1), 117-133. <https://doi.org/10.1017/bhj.2021.60>
- [21] Nam, B. T. N., & Hong, N. N. P. (2023). Addressing the challenges of data privacy protection law in Vietnam. *VNU Journal of Science: Legal Studies*, 39(1), 30-44. <https://doi.org/10.25073/2588-1167/vnuls.4413>
- [22] Omotubora, A. (2021). How (not) to regulate data processing: Assessing Nigeria's Data Protection Regulation 2019 (NDPR). *Global Privacy Law Review*, 2(3), 186-199. <https://doi.org/10.54648/gplr2021024>
- [23] Ozalp, H., Ozcan, P., Dinckol, D., Zachariadis, M., & Gawer, A. (2022). Digital colonization of highly regulated industries: An analysis of Big Tech platforms' entry into health care and education. *California Management Review*, 64(4), 78-107. <https://doi.org/10.1177/00081256221094307>

- [24] Peron, A. E. D. R., & Evangelista, R. (2024). Beyond instrumentalism: Automated facial recognition systems in Brazil and digital colonialism's violence. *Science, Technology and Society*, 29(4), 535–554. <https://doi.org/10.1177/09717218241281819>
- [25] Rao, U., & Nair, V. (2019). Aadhaar: Governing with biometrics. *South Asia: Journal of South Asian Studies*, 42(3), 469–481. <https://doi.org/10.1080/00856401.2019.1595343>
- [26] Sandberg, K. (2018). Children's right to protection under the CRC. In A. Falch-Eriksen & E. Backe-Hansen (Eds.), *Human rights in child protection* (pp. 15–38). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-94800-3_2
- [27] Shah, H. J., & Khan, A. (2023). Globalization and nation states: Challenges and opportunities for Pakistan. *Social Sciences & Humanities Open*, 8(1). <https://doi.org/10.1016/j.ssaho.2023.100621>
- [28] Singh, M., Adebayo, S. O., & Saini, M. (2021). Indian government e-learning initiatives in response to the COVID-19 crisis: A case study on online learning in Indian higher education system. *Education and Information Technologies*, 26, 7569–7607. <https://doi.org/10.1007/s10639-021-10585-1>
- [29] Singler, S., & Babalola, O. (2024). Digital colonialism beyond surveillance capitalism? Coloniality of knowledge in Nigeria's emerging privacy rights legislation and border surveillance practices. *Social & Legal Studies*. <https://doi.org/10.1177/09646639241287022>
- [30] Tanodomdej, P. (2019). The Tallinn manuals and the making of international law on cyber operations. *Masaryk University Journal of Law and Technology*, 13(1), 67–86. <https://doi.org/10.5817/MUJLT2019-1-4>
- [31] Thu, V. T. A. (2023). Protecting Vietnam's sovereignty in cyberspace: Insights from human right laws. *The Age of Human Rights Journal*, 21
- [32] Timmers, P. (2024). Sovereignty in the digital age. In H. Werthner (Ed.), *Introduction to digital humanism* (pp. 571–592). Springer. https://doi.org/10.1007/978-3-031-45304-5_36

Author Contribution

The author solely contributed to the study conception and design. The author read and approved the final manuscript.

Declarations

Conflict of Interest: The author declares no competing interests.

Disclaimer: All claims expressed in this article are solely those of the author and do not necessarily represent those of the author's affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.