Shawe, R., (2025). J Inform Techn Int, 3(2): 110
https://doi.org/10.33790/jiti1100110

Journal of Information Technology and Integrity

Cybersecurity and Human Rights: Navigating the Balance between Security and Freedom in the Digital Era

Robb Shawe, Ph.D., MS,
Department of Cyber Leadership, Capitol Technology University, Laurel, MD, United States.

Article Details
Article Type: Review Article
Received date: 24th July, 2025
Accepted date: 07th August, 2025
Published date: 09th August, 2025

***Corresponding Author:** Robb Shawe, Ph.D., MS, Department of Cyber Leadership, Capitol Technology University, Laurel, MD, United States.

Citation: Shawe, R., (2025). Cybersecurity and Human Rights: Navigating the Balance between Security and Freedom in the Digital Era. *J Inform Techn Int, 3*(2): 110. doi: https://doi.org/10.33790/jiti1100110

Abstract

Rapid digitalization has fundamentally reshaped the relationship between cybersecurity and human rights, intensifying both opportunities and risks for privacy, freedom of expression, and civil liberties. This study critically examines the dual role of cybersecurity as both a protector and potential violator of human rights, drawing on comparative case studies of the United States and China to illustrate divergent governance models and their implications. The analysis explores the impact of surveillance, data collection, and emerging technologies—including artificial intelligence, blockchain, and encryption—on individual freedoms. Policy recommendations emphasize the need for adaptive, inclusive, and internationally harmonized frameworks that embed human rights protections at the core of digital governance. Anticipated future challenges such as digital authoritarianism, the digital divide, and the complexities of global cooperation are also addressed, underscoring the urgency of multidisciplinary and anticipatory approaches to securing both security and fundamental freedoms in the digital age.

Keywords: Cybersecurity, Human Rights, Privacy, Freedom of Expression, Digital Governance, International Cooperation, Emerging Technologies, Policy, Surveillance, Digital Divide

Introduction

The rapid digitalization of nearly every facet of modern life has not only transformed how societies function and how rights are protected but also underscored the necessity of international cooperation in addressing the complex interplay between cybersecurity and human rights. As digital technologies become more embedded in daily existence, the boundaries between state security imperatives and individual freedoms are increasingly blurred. This convergence creates both opportunities and profound challenges: while robust cybersecurity measures are necessary to safeguard against evolving threats, they can also encroach upon essential human rights such as privacy, freedom of expression, and assembly. Achieving genuine security in cyberspace requires a nuanced approach that harmonizes collective safety with the preservation of civil liberties. This paper critically examines the evolving interplay between cybersecurity and human rights, addressing the gaps in current frameworks and proposing pathways for future development that uphold both security and fundamental freedoms in the digital age. Importantly, it underscores the crucial role of international cooperation in this endeavor, highlighting the significance of collaboration in addressing these complex issues.

Cybersecurity and Human Rights Overview

The relationship between cybersecurity and human rights is inherently dualistic, presenting both protective and threatening dimensions. On one hand, cybersecurity frameworks are essential for safeguarding the confidentiality, integrity, and availability of information, thus supporting fundamental rights such as privacy and freedom of expression [1]. Recent international legal developments, such as the UNESCO Guidelines for Regulating Digital Platforms, emphasize the need for multistakeholder approaches to safeguard freedom of expression and access to information in the digital age [2]. On the other hand, when national security is prioritized without sufficient oversight, cybersecurity measures can become vehicles for the infringement of individual rights, especially among vulnerable populations such as journalists, activists, and marginalized groups [3]. This tension underscores the necessity for policy frameworks that are not only robust in their protection against cyber threats but are also meticulously aligned with international human rights standards. Achieving this equilibrium requires continuous evaluation and adaptation of cybersecurity strategies to ensure that security imperatives do not become pretexts for eroding civil liberties. This section establishes the foundation for a critical analysis of how rights-respecting cybersecurity can be operationalized in practice, setting the stage for a nuanced exploration of privacy, expression, and policy responses.

Impact on Privacy

The tension between cybersecurity and privacy is most evident in the proliferation of surveillance technologies and expansive data collection practices. While cybersecurity measures can protect individuals and organizations from cyber threats, they often entail the monitoring of digital communications, which risks undermining the right to privacy—especially in the absence of transparent legal safeguards [4]. The lack of clear boundaries around data surveillance

can enable intrusive state or corporate practices, disproportionately affecting those who are unaware or unable to challenge such actions. Recent analysis by the European Union Agency for Fundamental Rights highlights that the rapid deployment of artificial intelligence for surveillance and data processing in the EU presents new risks to privacy and fundamental rights, necessitating robust regulatory responses [5]. Allahrakha [6] emphasized that without rigorous legal and ethical oversight, cybersecurity initiatives can inadvertently erode privacy rights, highlighting the need for frameworks that mandate transparency, accountability, and proportionality in data collection. A rights-respecting approach requires not only the establishment of clear legal thresholds but also ongoing review mechanisms to ensure that security measures do not become unchecked avenues for privacy violations.

Concrete examples of privacy breaches underscore the tangible risks posed by cybersecurity practices that lack sufficient oversight. In various jurisdictions, excessive or indiscriminate surveillance has led to unauthorized access and collection of personal data, violating established privacy standards and eroding trust in digital institutions [7]. Actions taken under the banner of national security have sometimes enabled authorities to monitor communications and gather metadata without meaningful safeguards, undermining the right to seek, receive, and impart information freely. Such instances highlight the urgent need for comprehensive, codified laws that establish clear boundaries and procedural protections, ensuring that cybersecurity measures are not exploited as tools for arbitrary intrusion into private life. Embedding robust oversight and redress mechanisms within legal frameworks is critical to maintaining the legitimacy of both cybersecurity and human rights protections.

Freedom of Expression

Cybersecurity measures can profoundly affect freedom of expression, particularly when used to justify censorship, internet shutdowns, or other restrictions on open discourse. Framed as necessary for national security or public order, such interventions can foster self-censorship and stifle dissenting opinions [8]. Feldstein [9] documents how digital repression has intensified globally, with governments leveraging new technologies to control information flows and suppress opposition. Legal frameworks that grant broad or vague cybersecurity powers may be weaponized to suppress criticism, silence marginalized voices, or limit access to diverse perspectives, undermining the democratic principle of free speech [10]. This dynamic demonstrates the risk that legitimate security concerns may be misused to erode core civil liberties. Achieving a sustainable balance requires vigilant scrutiny of legislative intent and implementation, with safeguards that ensure fundamental freedoms are protected even as digital threats evolve.

Additionally, cybersecurity is utilized as a tool on social media networks to limit free speech under the pretext of censorship on a larger scale. Cybersecurity regulations are made applicable on social media networks by governments of various nations, and the pretext given for the enforcement of these laws is the need to promote the safety of the nation, and this is done even at the expense of limiting voices of dissent and access to alternate opinions and viewpoints [7]. Social media networks can serve as offline extensions of the government's control when the enforcement of laws that limit free speech aligns with existing legislation that aims to regulate or outright ban activity and expression in the online atmosphere. Czuryk [7] states that the convergence of the demands of the state in the area of security and the demands in the area of network-based surveillance can lead to developments where free speech is limited in the name of cybersecurity efforts. In consideration of this fact, it can be seen that similar examples warrant a call for the establishment of principles that will ensure that cybersecurity demands do not infringe on fundamental freedoms, especially in consideration of the fact that they negatively affect the digital public sphere, and this highlights the need for the proper balance between security and the rights to free speech.

Balancing Security and Freedoms

Striking the appropriate balance between security and individual freedoms is a persistent challenge for policymakers and societies alike. Legal and legislative frameworks, particularly those grounded in international human rights instruments, play a pivotal role in mediating this balance. Recent scholarship underscores that international law and data protection regimes are struggling to keep pace with cross-border data flows and global digital governance, requiring more harmonized and adaptive approaches [11]. Effective alignment of national cybersecurity laws with universal human rights standards is essential to prevent the misuse of security justifications for the suppression of fundamental rights [4]. The most resilient frameworks are those that incorporate mechanisms for ongoing evaluation, public participation, and multilateral cooperation, ensuring that security measures are proportionate, transparent, and subject to independent oversight. This approach not only strengthens the legitimacy of cybersecurity policies but also fosters societal trust in digital governance. As the digital landscape evolves, continuous harmonization and adaptation of laws become imperative to address new threats without sacrificing core civil liberties.

Despite the existence of legal structures that integrate human rights standards, many contemporary policies inadequately balance security and freedoms, often privileging state interests at the expense of personal liberties [6]. This persistent gap is exacerbated by the rapid evolution of technology outpacing the development of adaptive regulatory frameworks. Actual progress requires policy reform that prioritizes transparency, accountability, and inclusive stakeholder participation in the creation and application of cybersecurity measures. International collaboration and ethical considerations must be embedded in regulatory updates to ensure that security objectives do not eclipse the rights and dignity of individuals. Only through such dynamic, participatory governance can societies remain resilient in the face of emerging digital threats while upholding fundamental freedoms [6].

Case Studies

Case studies offer invaluable insight into the practical consequences of cybersecurity policy on human rights, revealing how national contexts and legal cultures shape the balance between security and individual freedoms. By examining both the United States and China, this section highlights contrasting approaches to cybersecurity governance and their implications for privacy and freedom of expression. The U.S. tends to frame its cybersecurity measures within a liberal democratic tradition, often emphasizing due process and oversight, yet still grappling with surveillance overreach. In contrast, China's cybersecurity regime is characterized by extensive state control and prioritization of political stability, resulting in more pervasive restrictions on civil liberties. These divergent models not only influence domestic rights protections but also shape international debates on digital governance. Through this comparative lens, the case studies underscore the urgent need for global standards that promote security without sacrificing fundamental human rights, offering lessons for policymakers navigating the complexities of the digital age [1].

Case Study: United States of America

The United States exemplifies the complexities of balancing cybersecurity and human rights within a liberal democratic context. The enactment of the USA PATRIOT Act expanded government surveillance powers, raising ongoing debates about the right to privacy and the scope of state monitoring [12]. While the U.S. upholds constitutional protections for freedom of expression and due process, the tension between national security and civil liberties persists, especially as surveillance technologies and data collection practices evolve. Notably, the establishment of agencies like the Cybersecurity and Infrastructure Security Agency (CISA) demonstrates a commitment to defending digital infrastructure, but also prompts scrutiny regarding transparency, accountability, and

oversight of government activities [1]. The U.S. experience highlights the necessity of constant vigilance to prevent security measures from encroaching upon individual rights. It serves as a case study in the ongoing negotiation between public safety and personal freedom in democratic societies.

Also, current trends in cybersecurity policy in the US raise pertinent concerns about their impact on human rights. The most ostensible example of this is the programs introduced to advance the nation's cybersecurity posture, like the establishment of the Cybersecurity and Infrastructure Security Agency (CISA), which has strengthened the government's ability to carry out defensive operations in cyberspace. While these are among the efforts that show the dedication of the state against cyber manifestations of threats, the cybersecurity policy modules also involve implementations that may lead to violations of the privacy and freedom of expression of the members of the nation-state [12]. This is because, on a larger scale, the trends associated with cybersecurity policy-making threats are pertinent to issues involving surveillance and information collection via the Internet and information technology, as permitted by legislation such as the USA PATRIOT Act. In this regard, these are relevant within the broader context of policy concerning cybersecurity, which requires a careful inspection to ensure compliance with core human rights, necessitating the establishment of laws that would ensure transparency and protection of personal liberties in cyberspace.

Case Study: China

China's approach to cybersecurity emphasizes state authority and political stability, often at the expense of individual liberties. The PRC Cybersecurity Law enables extensive data collection and surveillance, allowing the government to monitor online activities, restrict content, and suppress dissent [13, 14]. These measures, justified by national security and social order, have resulted in significant infringements on privacy and freedom of expression. Unlike the U.S., China's system is highly centralized, with limited transparency and few avenues for independent oversight or legal redress. This approach not only affects domestic digital rights but also shapes global debates about the boundaries of state power in cyberspace. The Chinese experience highlights the risks of unchecked governmental authority and raises important questions about the future of digital rights in authoritarian contexts.

Internationally, China's cybersecurity policies have drawn widespread criticism for prioritizing state-backed narratives and control at the expense of privacy and free expression [13]. Critics highlight the transnational impact of these policies, noting that global companies and foreign institutions often struggle to comply with China's legal requirements while upholding their own human rights commitments. This tension has fueled international debates over the development of new norms for transnational cybersecurity and accountability. As a result, diplomatic engagement is essential to balance China's sovereign interests with the protection of human rights, both within its borders and in the broader digital landscape.

A comparative analysis of the United States and China reveals that starkly different philosophies and governance models shape the global landscape of cybersecurity and human rights. While the U.S. struggles to maintain democratic oversight and individual rights amid evolving security threats, China's centralized approach prioritizes state security at the expense of civil liberties. These differences not only define each country's domestic digital environment but also create friction in international forums, complicating efforts to establish universal norms. The divergence between these models underscores the urgent need for multilateral dialogue and the development of global standards that can reconcile security imperatives with the protection of fundamental human rights. Policymakers worldwide must learn from both the strengths and shortcomings of these approaches to craft adaptive, inclusive, and rights-respecting cybersecurity frameworks.

Technological Solutions

The global challenge of reconciling cybersecurity and human rights has spurred a surge in technological innovation. Among the most promising solutions are advanced encryption protocols, privacy-enhancing technologies, and decentralized systems, all of which aim to protect data integrity and individual autonomy while mitigating cyber threats. End-to-end encryption now underpins global messaging platforms, offering robust defenses against unauthorized access and surveillance [8]. Similarly, privacy-by-design frameworks and zero-knowledge proofs are gaining traction, empowering users to verify information or transactions without exposing sensitive data. Decentralized technologies such as blockchain facilitate secure, transparent, and tamper-resistant interactions that reduce the risks posed by centralized authorities. These trends reflect a broader movement toward technologies that embed human rights protections at their core. However, they also raise new questions about regulatory harmonization, law enforcement access, and ethical deployment on a global scale. As digital threats become increasingly sophisticated, the challenge for policymakers and technologists is to ensure that innovation advances both security and fundamental freedoms in a rapidly evolving digital ecosystem [8].

Encryption Technologies

Encryption technologies are at the forefront of efforts to safeguard privacy and freedom of expression in the digital age. The widespread adoption of end-to-end encryption in messaging apps and cloud services exemplifies how technical solutions can empower users to control access to their communications and data [6]. Recent innovations, such as homomorphic encryption and post-quantum cryptography, are being developed to address emerging threats and future-proof sensitive information against advances in computing power. However, these advancements also present challenges for law enforcement and regulatory authorities, sparking global debates over the appropriate balance between privacy and public safety. To avoid undermining trust or enabling misuse, the deployment of encryption must be accompanied by robust legal and ethical frameworks that are internationally interoperable, ensuring that privacy protections are not eroded by fragmented or contradictory regulations [4].

Despite its advantages in taking encryption technology to the next level, challenges and limitations exist in the overall implementation of encryption technologies universally. These primarily come from the fact that encryption technologies can be affected by the differences in technical, regulatory, and ethical demands globally. Idealistically, the pursuit of nation-states to uphold government surveillance for national security poses a significant challenge to individuals who advocate for their digital privacy through encryption [8]. In this context, encryption technologies may also have active constraints from state laws that vary from one nation to another, arguing against its implementation uniformly for fear that it may compromise national interests. In connection, a common technical challenge exists that calls for compatibility with various encryption systems to promote its cybersecurity while limiting others from exploiting its benefits. Hence, the construction of an ideal universally applicable approach may be required moving forward to mitigate the aforementioned restrictions potentially rooted in encryption technologies while allowing them to achieve their purpose of protecting citizens against any form of threat.

Emerging Technologies

Emerging technologies such as artificial intelligence (AI), machine learning, and blockchain are rapidly reshaping the cybersecurity landscape. AI-driven tools are increasingly used to detect, prevent, and respond to cyber threats, enabling more adaptive and proactive defenses [15]. At the same time, AI introduces new risks, including algorithmic bias, privacy violations, and the potential for mass surveillance if not adequately regulated. Blockchain technology continues to gain traction for its ability to provide secure, transparent,

and decentralized data management, supporting both privacy and accountability [15]. Global trends also include the rise of privacy-preserving computation, federated learning, and digital identity systems, which aim to empower users while minimizing data exposure. Harnessing the benefits of these technologies requires the creation of multidisciplinary, polycentric governance models and international standards that can adapt to rapid innovation without compromising fundamental rights [3].

Notwithstanding the vast potential of emerging technologies within cybersecurity-based systems to improve human rights, it is important to state that such systems also pose potential threats to human rights. With such technologies in place, there is the probability of autocratic regimes making excessive use of big-data for high invasion of privacy and surveillance of citizens. For example, artificial intelligence-based cybersecurity systems may be designed by governments to continue the kind of privacy invasion and high surveillance that has worsened today, through biased data. Algorithms may be programmed to continue these surveillance-based activities [16]. Also, there is the tendency for maladaptive use of blockchain technology to lead to new forms of data privacy infringement. Cybersecurity-based systems that depend on analyzed data and machine learning may open a new world of breaches if third parties depend too much on the open-market capacity of blockchain technology [16]. As such, there is a need for multidisciplinary modeling and polycentric governance to prevent emerging cybersecurity-based technologies and systems from becoming maladaptive. Moreover, there is a need for responsible use of adaptive technologies through measures that take human rights into cognizance using scientific approaches [16].

Policy Recommendations

To address the intertwined challenges of cybersecurity and human rights, policy frameworks must be both adaptive and inclusive, integrating technological, legal, and ethical perspectives. Governments should establish independent oversight bodies with the mandate to monitor, audit, and report on cybersecurity practices, ensuring transparency and accountability at every stage. Embedding human rights impact assessments into the development of cybersecurity policies is essential for proactively identifying and mitigating risks to privacy and freedom of expression. Policymaking should be a participatory process involving not only government officials, but also civil society, technical experts, and representatives from vulnerable and marginalized communities. International collaboration is crucial: harmonizing national laws with global human rights standards and fostering cross-border cooperation can help combat transnational cyber threats while upholding fundamental freedoms. Finally, policy frameworks must keep pace with technological innovation, incorporating guidance on privacy-preserving technologies, encryption standards, and responsible AI deployment to ensure that security measures do not outstrip the protections for individual rights [8].

In addition to national reforms, the harmonization of local cybersecurity legislation with international human rights standards is essential for building a fair and resilient digital environment. Countries should amend their laws to require human rights impact assessments for all significant cybersecurity measures, ensuring that privacy and freedom of expression are not compromised in the pursuit of security [7]. Transparent oversight and accountability mechanisms—spanning both government and private sector actors—must be institutionalized to address violations and adapt to new threats. Practical international cooperation is crucial: multilateral agreements, cross-border regulatory harmonization, and the engagement of the private sector and civil society are all necessary to counter transnational cyber threats and promote the protection of human rights globally [15]. Finally, continuous, multidisciplinary engagement among stakeholders—including legal, technical, and social science experts—will help ensure that cybersecurity policies remain inclusive, adaptive, and responsive to emerging ethical and technological challenges [16].

Future Challenges

Looking ahead, the intersection of cybersecurity and human rights is likely to face increasingly complex challenges as technologies evolve and geopolitical tensions intensify. One pressing concern is the rapid advancement of artificial intelligence, quantum computing, and biometric surveillance, all of which have the potential to outpace existing legal and ethical frameworks. The proliferation of cross-border data flows and global supply chains further complicates efforts to establish uniform standards for privacy and security. Daskal and Woods [17] highlight the growing trend of data nationalism, where states seek to exert sovereign control over digital information, posing new risks to global cooperation and human rights. Additionally, the rise of digital authoritarianism, where states leverage advanced technologies to suppress dissent and monitor populations, threatens to erode hard-won civil liberties on a global scale. Policymakers must also grapple with the digital divide, ensuring that cybersecurity protections and rights are accessible to marginalized and under-resourced communities. Finally, the challenge of fostering genuine international cooperation remains significant, as divergent national interests and regulatory philosophies can hinder the creation of universally accepted norms. Addressing these future challenges will require adaptive, anticipatory governance, continuous dialogue among stakeholders, and a steadfast commitment to embedding human rights at the core of technological innovation and digital policy.

Conclusion

The evolving intersection of cybersecurity and human rights demands an ongoing commitment to both innovation and ethical governance. As digital technologies become ever more integral to daily life, the challenge is not merely to balance security and freedoms, but to design systems and policies that actively reinforce both. This paper has demonstrated that national models—exemplified by the United States and China—offer important lessons but also reveal the dangers of privileging either state power or unchecked individual liberty. The most resilient path forward is one that embraces international cooperation, robust oversight, and adaptive, rights-respecting frameworks. Technological advances such as encryption, privacy-preserving computation, and AI offer powerful tools for protecting rights, but they must be deployed within globally harmonized and transparent regulatory environments. Ultimately, the future of digital society will depend on the ability of policymakers, technologists, and civil society to collaborate across borders, ensuring that cybersecurity serves as a foundation for—not a threat to—universal human rights.

Competing Interests: The authors declare that they have no competing interests.

References

1. Dunn Cavelty, M., & Kavanagh, C. (2019). Cybersecurity and human rights. In *Research Handbook on Human Rights and Digital Technology* (pp. 73–97). elgaronline.com. https://doi.org/https://doi.org/10.4337/9781785367724.00012
2. UNESCO. (2023). *Guidelines for regulating digital platforms: A multistakeholder approach to safeguarding freedom of expression and access to information*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000384723
3. Pavlova, P. (2020). Human rights-based approach to cybersecurity: addressing the security risks of targeted groups. *Peace Human Rights Governance, 4*(3), 391–418. https://doi.org/10.14658/PUPJ-PHRG-2020-3-4
4. Dalal, A. (2020). Cybersecurity and privacy: Balancing security and individual rights in the digital age. *Papers.Ssrn.Com*. https://doi.org/10.2139/ssrn.5171893

5. European Union Agency for Fundamental Rights. (2022). Artificial intelligence and privacy: Fundamental rights implications for the EU. *Publications Office of the European Union*. https://fra.europa.eu/en/publication/2022/artificial-intelligence-and-privacy
6. Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. *Cyberleninka. Ru*. https://cyberleninka.ru/article/n/balancing-cyber-security-and-privacy-legal-and-ethical-considerations-in-the-digital-age
7. Czuryk, M. (2022). Restrictions on the exercising of human and civil rights and freedoms due to cybersecurity issues. *Studia Iuridica Lublinensia, 31*(3), 31–43. https://www.ceeol.com/search/article-detail?id=1107070
8. Abbas, A. E. (2019). Ethics in cyberspace: freedom, rights, and cybersecurity. In *books.google.com*. Cambridge University Press. https://books.google.com/books?hl=en&lr=&id=sYK0DwAAQBAJ&oi=fnd&pg=PA444&dq=cybersecurity+and+freedom+of+expression+issues&ots=uOjwgqAfc7&sig=4mjxD1ju1ErHLch92x0BZIg5QF4
9. Feldstein, S. (2022). The rise of digital repression: How technology is reshaping power, politics, and resistance. *Journal of Democracy, 33*(2), 59–73. https://doi.org/10.1353/jod.2022.0022
10. Leghari, M. A., Wasiq, M. F., Younes, J., & Hassan, B. (2024). Global legislation muzzling freedom of speech in the guise of cybersecurity. *In Cybersecurity and Artificial Intelligence* (pp. 263–279). Springer. https://doi.org/10.1007/978-3-031-52272-7_11
11. Kuner, C., Bygrave, L., & Greenleaf, G. (2023). International law and data protection: The challenge of global governance. *International Data Privacy Law, 13*(2), 100–115. https://doi.org/10.1093/idpl/ipad002
12. Lukings, M., & Lashkari, A. H. (2022). Understanding cybersecurity law and digital privacy. *In Springer. Springer*. https://doi.org/10.1007/978-3-030-88704-9
13. Chen, Y. C., Liu, T. T.-T., & Romaniuk, S. N. (2021). Serving the People: China's cybersecurity policy and its implications. *In Routledge Companion to Global Cyber-Security Strategy* (p. 13). Routledge. https://doi.org/10.4324/9780429399718-27
14. Jiang, B. (2021). Contract Optimization of Renewable Energy Electricity Supply Chain on the Island for Sustainability. *Open Journal of Business and Management, 9*, 3053-3075. https://doi.org/10.4236/ojbm.2021.96171
15. Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime, 28*(2), 359–374. https://doi.org/10.1108/JFC-07-2020-0149
16. Shackelford, S. J. (2021). Should cybersecurity be a human right?: Exploring the "shared responsibility" of cyber peace. *In Music, Business and Peacebuilding* (p. 24). Publisher. https://doi.org/10.4324/9781003017882-14
17. Daskal, J., & Woods, A. (2022). Data nationalism and its discontents. *Yale Law Journal, 132*(1), 124–178. https://www.yalelawjournal.org/article/data-nationalism-and-its-discontents