T20 Policy Brief

G20 BRASIL 2024

T20 Brasil 2024 Let's rethink the world

Task Force 05

INCLUSIVE DIGITAL TRANSFORMATION

Optimizing Privacy and Security: The Role of Encryption as Foundation of Online Trust

Pedro Amaral, Researcher and Obcrypto Coordinator, Law and Technology Research Institute of Recife (Brazil)

Paula Bernardi, Senior Policy and Advocacy Advisor, Internet Society (Global)

Raquel Saraiva, President, Law and Technology Research Institute of Recife (Brazil)

Thobias Prado Moura, Director for Communication and Events, Internet Society Brazil (Brazil)

Mariana Canto, Director, Law and Technology Research Institute of Recife (Brazil)

TF05

Abstract

Our increasing reliance on digital technology for social, political and economic affairs has shed light on strong end-to-end encryption. Frequently described as the gold standard of cybersecurity and privacy, encryption is essential to the exercise of freedom of expression, protecting privacy and security, and other digital rights. Strong encryption is a fundamental part of how we remain safe both online and offline. It helps achieve security, as it reduces the utility of stolen devices and data, making identity thefts, fraudulent transactions, and mass data breaches more difficult. This layer of security empowers users, both public and private, to control access to information and its uses, thereby promoting greater autonomy and freedom. This policy brief aims to contribute to ongoing discussions on digitalization and inclusion at the G20 and T20 summits, offering a comprehensive and updated perspective on the role of encryption in shaping a fairer and more resilient digital society. Specifically, it highlights encryption as a cornerstone for developing the digital economy, fostering security, enhancing consumer and business trust, and driving economic growth. It also underscores the importance of governments and organizations prioritizing, protecting, developing and implementing robust encryption standards and protocols alongside efforts to raise awareness about the significance of digital security among users. This policy brief aims to provide practical recommendations to the G20 for strengthening its digital security agenda by examining how encryption enhances digital privacy and secures online communications. Moreover, in alignment with the G20's commitment to advancing digital security and safeguarding human rights, the policy underscores the pivotal role the G20 can play in championing a global framework that upholds privacy, freedom of expression, and secure communication rights for everyone.

Keywords: Encryption; Privacy; Cybersecurity; Human Rights.

Diagnosis of the issue

Strong encryption plays a crucial role in protecting privacy, security, confidentiality and human rights, along with national and corporate security. It renders communications and data unreadable and worthless for unauthorized access, which is why end-to-end encryption (E2EE) is widely used because intermediated services require us to trust third parties. Encryption is almost everywhere, working invisibly to protect people. Thus, encryption is relevant to advance many SDGs: it protects health and education information (SDG 3: Good Health and Well-being and SDG 4: Quality Education); it ensure privacy and security for everyone, including women around the world (SDG 5: Gender Equality); as essential to digital security, it helps foster economic growth, resilient infrastructure, and innovation and safe smart cities (SDG 8: Decent Work and Economic Growth, SDG 9: Industry, Innovation and Infrastructure and SDG 11: Sustainable Cities and Communities), as well as make the digital more secure for everyone (SDG 16: Peace, Justice and Strong Institutions).

FIGURE 1 - Main infrastructures and services that depend on encryption. From: Authors

Cryptography's importance must be recognized in the digital world, especially in information security and data protection. It enables the exercise of fundamental rights such as freedom of expression and privacy, which are protected in the Universal Declaration of Human Rights (Articles 12 and 19) and reaffirmed in the International Covenant on Civil and Political Rights (ICCPR). In the same vein, the integration of cryptographic standards into digital infrastructures, both public and private, is indispensable for mitigating risks of fraud and ensuring the confidentiality of citizens' data.

Additionally, cryptography is crucial for professionals at political risk, such as journalists and human rights defenders, as well as vulnerable groups, such as LGBTQ+ communities and ethnic and religious minorities. Attacks on the media are common tactics by authoritarian states as they inhibit the potential circulation of information necessary for democratic political construction. As noted by Irene Kahn, UN Special Rapporteur on freedom of expression, encryption is "an essential facet of women's enjoyment of freedom of opinion and expression in the online context and must be protected" (KAHN, 2021, p.21).

This position is not recent. In 2015, the then UN Special Rapporteur on Freedom of Expression concluded, "States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology" (KAYE, 2015, p.20). Thus, when reinforced by strong encryption, digitized public and private services have been more capable of ensuring citizens' security, privacy, and data protection, mitigating risks and damages from digital frauds and scams that spread, especially in developing economies.

However, the cryptography landscape has been facing significant challenges for some time. Since 1966, there has been a continuous tension between the need to protect digital communications and efforts to weaken encryption. With Edward Snowden's revelations about the National Security Agency's (NSA) mass surveillance and espionage programs in 2013, civil society, academia, governments, and industry have come together to advance the offering and adoption of more secure and private communication means (Craig Jarvis 2021).

With its increasing dependence on mobile devices, the Global South uses instant messengers more, including for accessing public and private services. Therefore, the threat of weakening and blocking of these services in the Global North have the potential to affect the South more intensely. This impact is due to the interconnected and interdependent nature of the Internet, as demonstrated during the Whatsapp blockages in Brazil in 2015 and 2016, when, due to the Internet infrastructure in South America, judicially ordered blockages impacted users in neighboring countries.

In response, Direct Action of Unconstitutionality 5527 (Brazil 2020a) and Preliminary Question of Fundamental Precept 403 were filed in the Brazilian Federal Supreme Court (Brazil 2020b). The former discusses the possibility of "suspension" and "prohibition" of services provided by application and connection providers and the constitutionality of a provision that enforces protection against non-compliance with rules protecting connection records, personal data, and private communications. Conversely, the latter discusses whether application blockages violate fundamental rights to freedom of expression, association, collectivity, and communication.

More recently, there have been some notable strides in safeguarding encryption. Canada reintroduced the Online Harms Bill in February 2024, with a clear exemption for

private messaging services and a recognition of the importance of privacy and security in private communications. Also in February, the European Court of Human Rights ruled in the case of Podchasov v. Russia (European Court of Human Rights 2023), declaring Russia's requirement for encryption keys a violation of privacy rights and the right to private communication as stated in Article 8 of the European Convention on Human Rights. Lastly, in March 2024, Chile enacted the Cybersecurity Framework Law, which recognizes encryption as a fundamental right.

In 2023, the G20 Ministers responsible for the digital economy met to discuss the role of Public Digital Infrastructure (PDI) in driving the digital economy forward. They stated that PDI should be secure, interoperable, and built based on open standards and specifications to provide equitable access to public and private services. Strong encryption protocols must be used across various layers of the Internet to ensure security and privacy.

In the past, the G20 has primarily focused on economic aspects of digitization, such as promoting digital inclusion and developing digital infrastructure, with little focus on cybersecurity and encryption. This policy brief is, therefore, unprecedented within the T20 as it focuses on the importance of encryption in driving the digital economy forward

Recommendations

As digitization continues to advance across various aspects of cultural, political, and economic life, the need for digital infrastructure has become increasingly apparent. Many countries are now searching for solutions to ensure the stability, security, and trust necessary to meet the diverse needs of their citizens in utilizing the Internet. Encryption is a crucial component in achieving these objectives. Given the growing centrality of digitization, the G20 plays a pivotal role in promoting a safer and more dependable Internet through the promotion of encryption. The adoption of these recommendations by the group has the potential to positively influence not only the populations of the G20 countries themselves but also other countries globally.

Many private messaging applications with end-to-end encryption have connected consumers, suppliers, citizens, and public services in various countries. This is particularly prevalent in the Global South, such as Brazil (See Figure 2) and India. WhatsApp is the most widely used messaging application in these two countries and has even enabled access to public and private services, especially during the pandemic. Our recommendations suggest that the States should avoid opposing strong encryption and instead implement policies to support its development, encourage its use, and facilitate its adoption

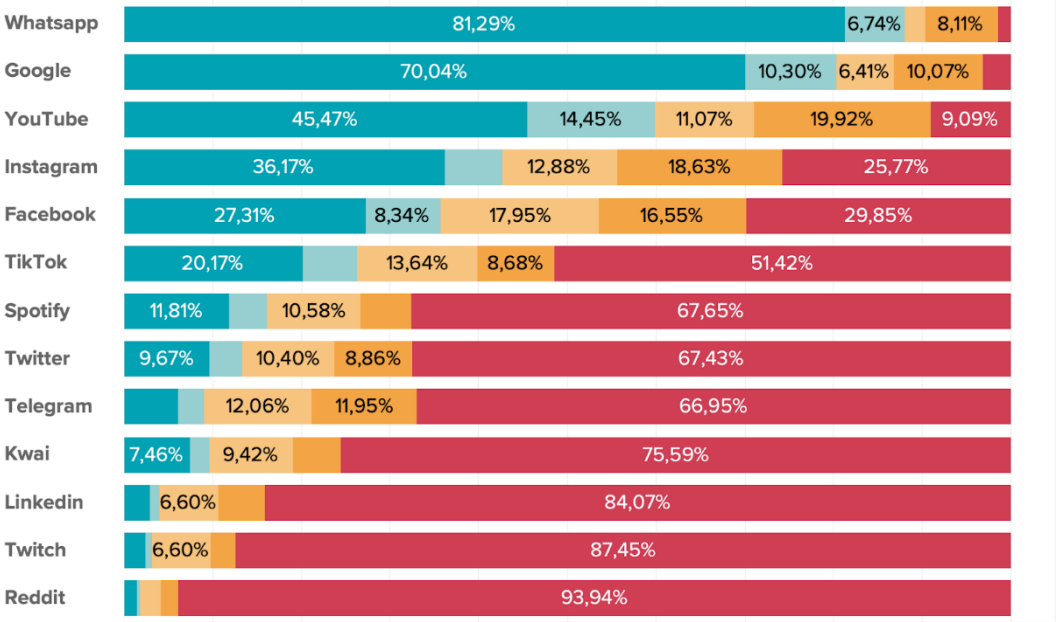

FIGURE 2 - Access to digital media, by weekly frequency, in Brazil

From**:** Atlas | Elaboração: FGV ECMI

Recommendation: Avoid policies and discourse against encryption.

Justification: In recent years, various governmental initiatives worldwide, including legislative proposals, have sought to restrict end-to-end encryption. Among them is the United Kingdom's Online Safety Act, which gives the Ofcom authority to compel platforms to conduct mass surveillance through client-side scanning, undermining the security and privacy of end-to-end encryption. These measures violate principles of proportionality and necessity, infringing on due process and the presumption of innocence. These policies and the discourses that justify and motivate them incur structural risks to citizens' security, national security, and the technological innovation ecosystem. They are incompatible with fundamental rights to privacy and security that strong encryption ensures. These discourses are often reductionist and do not see the

complexity of the issues at hand, being based on techno-solutionism by proposing apparently 'easy' solutions to persistent social problems. This is especially critical given the continued growth of data generation, sensors that generate this data, and connected devices. According to Statista data, in 2023, 15.14 billion devices were integrated into the Internet of Things. It is forecasted that by 2024, this number will reach 17.08 billion devices and 2030 will reach almost 30 billion devices. In this scenario, strong end-to-end encryption must be free of government opposition under the risk of an even more vulnerable IoT.

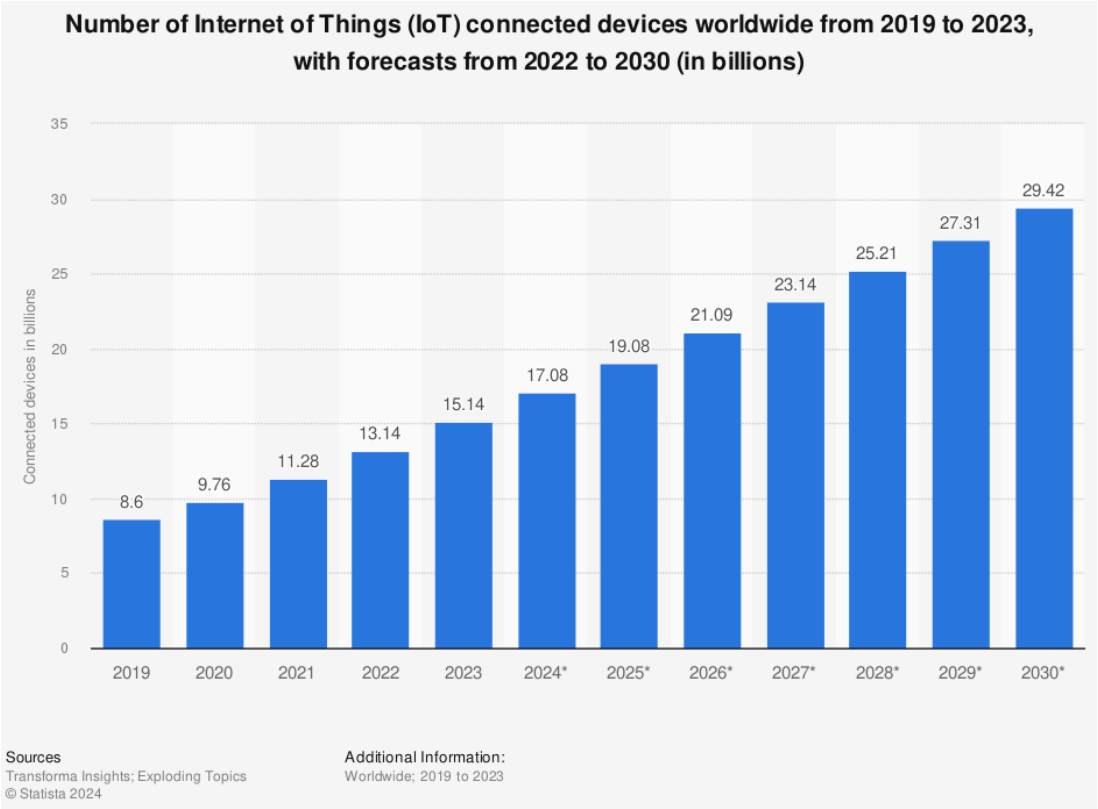

FIGURE 3: Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2024 to 2030. From: Statista

Recommendation: Companies should strengthen their commitment to implementing end-to-end encryption in its services with the goal of improving their security and trustworthiness.

Justification: Secure and trustworthy products and services, in a global economy are the foundation of human rights, social progress and economic development. As people increasingly rely on messaging services for their communications, application providers' implementation of end-to-end encryption (E2EE) becomes even more essential for secure connections. According to the "Cost of data breach report 2019" by IBM and the Ponemon Institute, extensive use of encryption is the second most crucial factor for mitigating the costs and impact of data breaches (see Figure 4). This adds to the worldwide expectation of rising cybercrime costs, as shown by data from Statista, National Cybersecurity Organizations, the FBI, and the International Monetary Fund (see Figure 5).

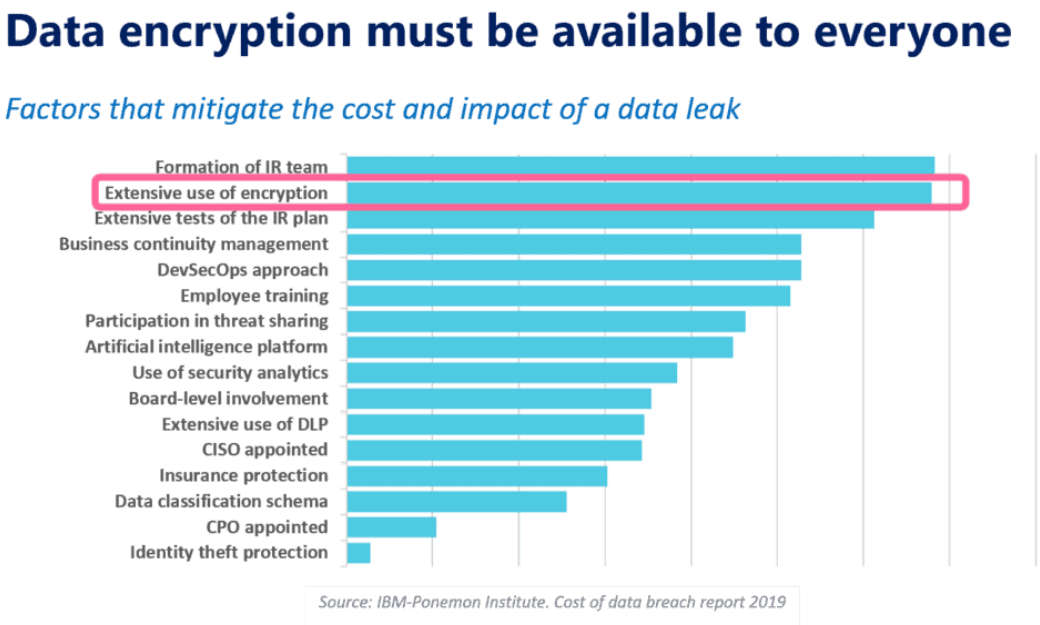

FIGURE 4: Factors mitigating the cost and impact of data breaches. From: Ponemon Institute for IBM.

Recommendation: Governments should invest in research and development of encryption.

Justification: Encryption is an essential technology for the security of institutions, organizations, businesses, and citizens of their countries and the State itself. This includes research on quantum-resistant cryptography and any other future threats to Encryption.

Justification: Given the recurring pressures on private messengers, blocking or weakening can harm their exclusive use. This means vulnerability for users of public services offered through these means. It is necessary to offer secure and reliable proprietary means as alternatives, these alternatives must meet the same standards of openness and audibility. This is urgent in light of the observed and expected growth in the costs and impacts of cybercrime worldwide, as indicated by data from Statista, National Cybersecurity Organizations, the FBI, and the International Monetary Fund (see Figure 5).

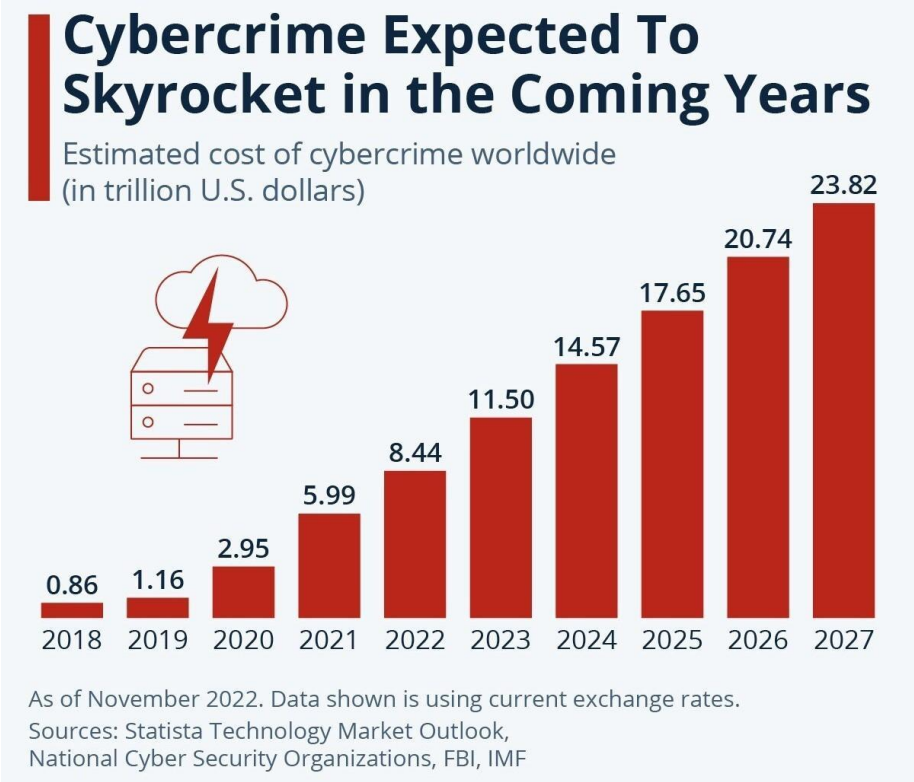

FIGURE 5: Estimated cost of cybercrime worldwide. From: World Economic Forum.In addition to positively affecting citizens, business, and culture, it is a matter of sovereignty and national security.

Recommendation: Promote openness and auditability of cryptographic protocols and their implementation.

Justification: The openness of these developed or acquired protocols allows for the examination and review of the code, as well as verification and auditing of the implementation of cryptographic functions to avoid intentional vulnerabilities, such as backdoors or accidental ones.

Recommendation: Offer secure, appropriate and auditable alternative channels for accessing public services.

Recommendation: State institutions must train their technical staff in cryptography, privacy, and security.

Justification: This measure aims to prevent actions that restrict the use of encryption, as such blocks are disproportionate and can have a negative impact nationally and often regionally, as was the case with WhatsApp blocks in Latin America. It is recommended to refrain from promoting procedural solutions that weaken encryption. Besides not guaranteeing effectiveness in combating crime, they increase vulnerabilities that can be exploited by all types of malicious agents, putting users and critical Internet properties at risk.

Recommendation: Strong encryption and, where possible and feasible, end-to-end encryption must be implemented in public digital infrastructure solutions.

Justification: Helping to ensure stability, security, and trust for the uses of PDIs in security, health, education, finance, civic participation, among others. This is urgent, considering the global scenario of accelerated digitization, data breaches, and cybercrime. Following this recommendation means acting preventively.

Recommendation: Maintain constant dialogue with specialized sectors, such as organized civil society and the scientific community, to ensure public policies which impact encryption and/or involve the Internet do not result in greater risk or unintended harm to the citizen.

Justification: In order to develop effective public policies concerning encryption and conduct criminal investigations in a way that respects fundamental rights, it is important to prioritize procedures that promote protection instead of weakening encryption. Restrictions on encryption do not reduce criminal activity (EDRi, 2016). Rather, such restrictions create more vulnerabilities that can be exploited by criminals, thereby putting network users and critical infrastructure at risk. A collaborative approach toward creating public policies that involve multiple sectors and perspectives, with a focus on protecting and respecting human rights, is essential. Processes that prioritize transparency and consensus are beneficial for users and provide greater legitimacy to democratic institutions, while promoting the use of technology for the common good.

Scenario of Outcomes

Scenario 1: *In this scenario, all sectors adopt strong encryption as the gold standard, emphasizing strengthening cybersecurity and protecting individual rights through policies promoting strong encryption. Implementing strong, end-to-end encryption in public and private digital infrastructures would not be questioned as its benefits outweigh the risks, offering robust protection against cyber threats and mass surveillance tools. Data protection, privacy, and individual rights would also be reinforced, as unauthorized access to personal communications and sensitive data is hindered. This would promote public trust in governmental and private institutions and the digital economy.*

This scenario has a relatively moderate to low probability. Resistance from certain industry sectors and governments may hinder the unquestionability of implementing

cybersecurity policies that emphasize strong encryption. However, increasing awareness of cybersecurity risks and the benefits of encryption, along with ongoing efforts by civil society actors, point towards greater recognition of encryption as an essential tool for protecting and ensuring fundamental rights.

Scenario 2: *In this scenario, the importance of encryption is recognized, but there is a focus on concerns about criminals' potential misuse of encryption. Here, the emphasis is on balancing protecting individual rights and the need to combat harmful conduct in the online environment. There may be debates about implementing additional law enforcement measures to address these concerns. While strong encryption protects communications and data, concerns arise about the misuse of technology by criminals and terrorists, who may exploit the privacy offered by encryption to engage in illicit activities. Governments may face pressure to balance protecting citizens' rights and ensuring public safety. This leads to debates about the need for additional law enforcement measures and oversight to combat cybercrime while preserving the integrity of strong encryption and user privacy.*

This scenario is highly probable. Although the benefits of strong encryption and cybersecurity are recognized, there are also legitimate concerns about the misuse of encryption by malicious actors. Governments may seek alternative solutions—unrelated to weakening strong encryption—to balance these concerns with protecting individual rights. Resistance from certain actors may hinder the implementation of cybersecurity policies emphasizing strong encryption. (Greenberg, 2024)

To Move Forward: All Must Embrace Encryption

It is possible to conclude that when governments stop undermining strong encryption, results will come in the shape of trust, stability, and security of online data and communications. If decision-makers embrace policies that acknowledge and legitimize the development, commercialization, and utilization of strong and end-to-end encryption, security, intelligence, and law enforcement agencies would diminish or cease their efforts to subvert it. Subsequently, these agencies could redirect their resources and focus towards alternative methods for gathering evidence pertaining to serious crimes, which are frequently cited in campaigns against the use of strong encryption.

References

Brasil. Supremo Tribunal Federal. 2020a. *ADI 5527 Voto Relator***:** Min. Edson Fachin. https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf

Brasil. Supremo Tribunal Federal. 2020b. *ADI 403 Voto Relator***:** Min. Rosa Weber.https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

European Court of Human Rights. 2024. *"Case of Podchasov v. Russia (Application no. 33696/19)***.**" HUDOC database. Accessed October 26, 2023. https://hudoc.echr.coe.int/eng/?i=001-230854.

Greenberg, Andy. 2024. *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. Vintage.

Jarvis, Craig. 2020. *Crypto wars: the fight for privacy in the digital age: A political history of digital encryption*. CRC Press.

David Kaye. 2015. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. U.N. Doc. A/HRC/29/32.

Irene Khan. 2021. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. U.N. Doc. A/76/258.

Riana Pfefferkorn. 2022. *"The End of Roe Will Bring About a Sea Change in the Encryption Debate."* Lawfare, May 10, 2022. https://www.lawfareblog.com/end-roe-will-bring-about-sea-change-encryption-debate.

Rudra Chaudhuri. 2023. *"Decoding the G20 Consensus on Digital Public Infrastructure: A Key Outcome of India's Presidency."* September 1, 2023.https://carnegieindia.org/2023/09/01/decoding-g20-consensus-on-digital-public-

infrastructure-key-outcome-of-india-s-presidency-pub-90467

The Economic Times. 2023. *"Cyber Security Is Global Problem, Declares G20 Digital Economy Ministers Meet."* https://telecom.economictimes.indiatimes.com/news/policy/cyber-security-is-global-problem-declares-g20-digital-economy-ministers-meet/102895117.

World Economic Forum. 2024. *"2023 was a big year for cybercrime – here's how we can make our systems safer."* https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/

G20 BRASIL 2024
BUILDING A JUST WORLD AND A SUSTAINABLE PLANET

T20 Brasil 2024
Let's rethink the world

Let's rethink the world

CEBRI Rethink Tank

FUNDAÇÃO ALEXANDRE DE GUSMÃO

ipea
Instituto de Pesquisa Econômica Aplicada