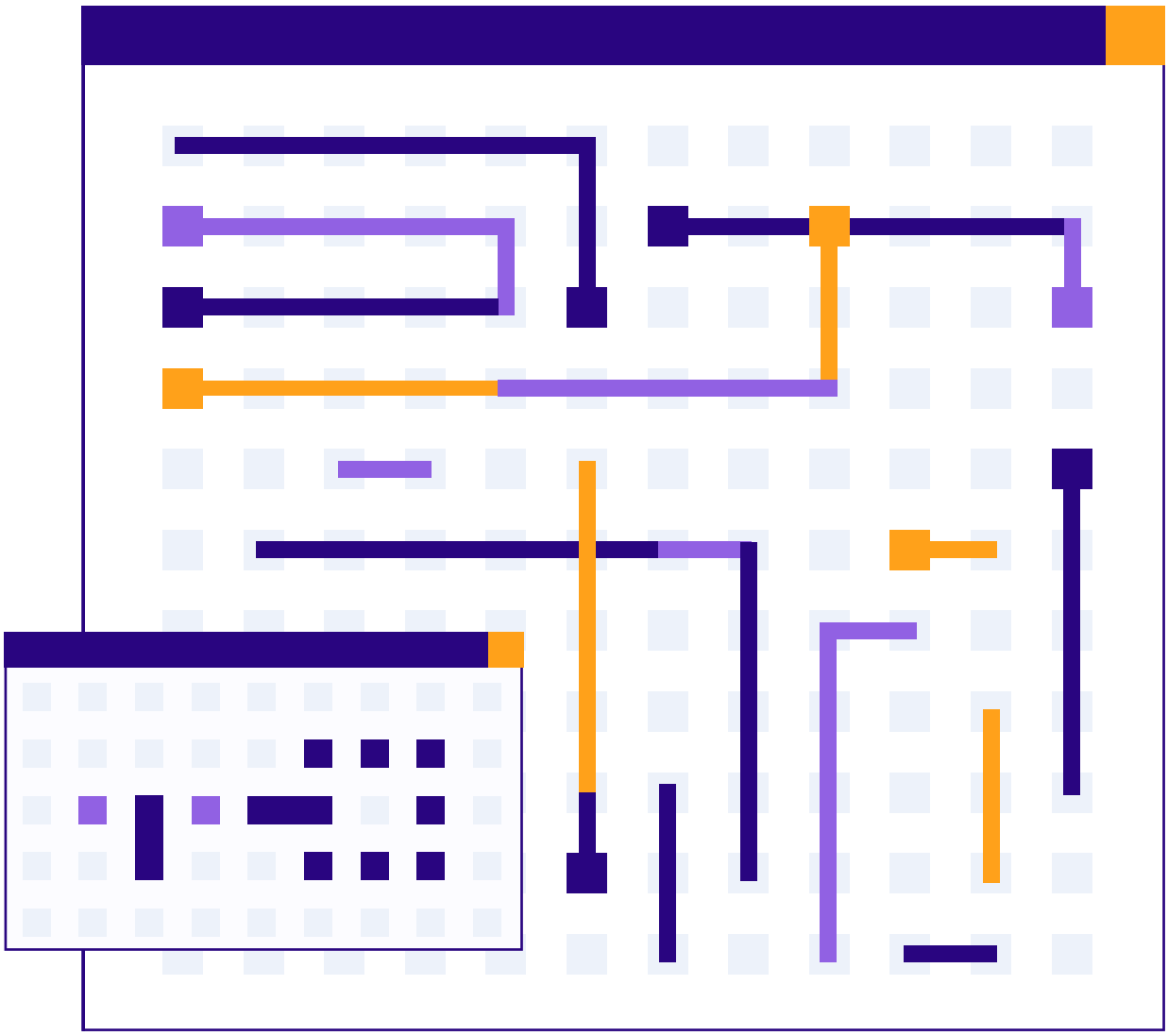
PERCEPTIONS ON ENCRYPTION AND CRIMINAL INVESTIGATIONS IN BRAZIL

mapping and analysis



INSTITUTE FOR RESEARCH ON INTERNET AND SOCIETY

supporters:

Internet Society Capítulo Brasil

Internet Society Foundation

PERCEPTIONS ON ENCRYPTION AND CRIMINAL INVESTIGATIONS IN BRAZIL

mapping and analysis

Authorship

Ana Bárbara Gomes Pereira

Gustavo Ramos Rodrigues

Victor Barbieri Rodrigues Vieira

Consultancy

Lucas Caetano Pereira de Oliveira

External review

Paulo Rená da Silva Santarém

Raquel Lima Saraiva

Translation

Luiza Brandão

Victor Vieira

Translation review

Wellington Araújo

Graphic design project, cover and layout

Felipe Duarte

This publication is part of the project "Privacy is Security: Communicating the Importance of Encryption for All", in partnership with ISOC Brasil and funding from ISOC Foundation.

research by: INSTITUTE FOR RESEARCH ON INTERNET AND SOCIETY

supporters: Internet Society Capítulo Brasil; Internet Society Foundation

INSTITUTE
FOR RESEARCH
ON INTERNET
AND SOCIETY

DIRECTRESS

Luíza Couto Chaves Brandão

MEMBERS

Ana Bárbara Gomes / Researcher

Beatriz Fernandes / Communication Trainee

Felipe Duarte / Head of communication

Gustavo Rodrigues / Head of public policy and Researcher

Juliana Roman / Researcher

Lahis Kurtz / Head of Research and Researcher

Paloma Rocillo Rolim do Carmo / Deputy directress and Researcher

Pedro Vilela Resende Gonçalves / Co-founder and Associate

Victor Barbieri Rodrigues Vieira / Researcher

SUMMARY

Executive Summary 6

1. Introduction 10

2. Context - The Crypto Wars 12

2.1. Crypto Wars in the 20th Century 13

2.2. Current Crypto Wars (2013 - present) 16

2.3. Crypto Wars in Brazil 17

2.3.1. WhatsApp blockings in the country 17

2.3.2. Encryption in the Supreme Court: ADI 5527 and ADPF 403 19

2.3.3. Encryption under the Brazilian law and other recent conflicts 20

3. Methodology 23

3.1. Interviewees selection 23

3.2. Interviews conduction 24

3.3. Data coding and analysis 25

3.4. Limitations of the methodology adopted 26

4. Results 26

4.1. About inserting backdoors mechanisms in encryption 26

4.1.1. The pro-backdoor discourse 26

4.1.2. The anti-backdoor discourse 28

4.2. On alternatives to backdoors 31

4.2.1. The risks of alternatives 34

4.3. About the national regulatory environment on encryption 35

4.4. About WhatsApp blockings and their relationship with the Internet Bill of Rights 39

5. Analysis and discussion 43

5.1. About Backdoors 43

5.2. About backdoor alternatives 47

5.3. About WhatsApp blockings in Brazil and its relationship with the Internet Bill of Rights 51

6. Conclusion 54

7. References 57

8. Appendix 1 - Interview Script 65

9. Appendix 2 - Code Families 68

Executive Summary

Context. Since the second half of the 20th century, the constant technological advances in the field of cryptographic techniques, as well as the perspectives of mass access to these technologies by civil society, represented a point of recurrent argumentative conflict. Delimited by what is conventionally called Crypto Wars – or Encryption Wars – the dispute involving the State, industry, and civil society over their right of access to strong and secure encryption techniques extends to the present day. Episodic – but perennial – in nature, Crypto Wars acquire new dimensions in the 21st century, with the exponential increase in civil society's access to the internet and, concomitantly, the development and use of increasingly sophisticated investigative technologies.

In Brazil, the import of the American Going Dark narrative – or "obscuration" – has also culminated in the reproduction of this conflict, initially materialized in the WhatsApp application blocks in the country in 2015 and 2016. Such events resulted in two lawsuits - ADI (Action of Unconstitutionality) 5527 and ADPF (Claim of Non-Compliance with a Fundamental Precept) 403 -, filed in the Federal Supreme Court, which discusses the constitutionality of the measures. Although both cases are still pending, two supreme court judges have already recognized encryption as essential to fundamental rights, such as privacy and freedom of expression. Similarly, the Superior Court of Justice has already considered, in the examinations of RMS (Appeal on Security Mandate) 60,531 and RESP (Special Appeal) 1,872,695, it is illegal to apply sanctions to an application provider that fails to comply with an interception order due to a technical impossibility imposed by encryption.

In spite of that, attempts to introduce a backdoor mechanism in encryption are still taking place in the country and not rarely become the object of legislative discussion. The dubbed "Anti-Crime Package" of former Minister of Justice and Public Security Sérgio Moro comprised predictions that expanded the powers of State interception and could imply weakening encryption, for instance. Similarly, the reform of the Criminal Procedure Code has brought back debates about the possibility of application providers' obligation to reduce the security of their systems to carry out interceptions during a criminal prosecution. Thus, the issue of backdoors and encryption governance remains urgent and current in the country.

Methodology. In this context, this study aimed to investigate the perception and opinion of professionals involved in the public debate on the topic. Forty- five interviews were done and forty-three out of them were considered valid. We interviewed representatives from the government, business and third sector. Moreover, we also interviewed representatives from the scientific and technological community. The professionals who were interviewed had different disciplinary and professional backgrounds.

Interviewees were selected by using the snowball sampling method, in which new participants are indicated by previous ones, creating a progressively expanded social network. Since this method does not generate a representative sample of any population segment and it is more sensitive to selection biases, this study is not an opinion survey. It is an empirical mapping and an analysis of the main discourses, rationalities, and beliefs that permeate Brazilian cryptographic wars.

After the interviews, we coded and analyzed the professionals' perceptions and opinions on four topics. i) the backdoor implementation to access encrypted data for criminal prosecution purposes, ii) knowledge and risks on potential alternatives for authorities' access to encrypted content without direct interference with encryption, iii) the national regulatory environment regarding encryption, and iv) the WhatsApp blocks in Brazil and its relationship with the Internet Bill of Rights. The results of this analysis are in the form of narrative reconstructions of the identified discourses. After this mapping, there was an analysis of the relations between the identified thesis and the factual contexts.

Results. Regarding backdoors, there were two main discourses around the theme. The pro-measure discourse points out an essential conflict between privacy and public safety and assumes the latter value's priority over the former. Furthermore, it understands that Brazilian Law establishes a legal duty to guarantee interceptions' conditions and compels those to carry them out under the legal terms. At the same time, the discourse against backdoors considers the measure disproportionately harmful, as it would affect all users of the system, compromising their informational security and their fundamental rights, in addition to undermining trust in the digital environment. Moreover, it raises questions about both the actual need for the measure and its alleged effectiveness. It suggests that criminality will migrate from the platforms compromised by the backdoors mechanism.

When it comes to possible alternatives for accessing data without breaching encryption, the main options cited were the seizure and unlocking of the investigated persons' devices, government hacking of these devices, metadata analysis, client side-scanning, insertion of a ghost user, and access to data stored in cloud services. Risks of violating the investigated person's rights relate to solutions based on compromising the security of the individual device, given the possibility of accessing any content on the device, including those irrelevant to the investigation. As for client-side scanning and phantom user insertion solutions, the assumption that such options would not interfere with encryption was questioned and criticized. In this sense, a frequent perception was that they would compromise encryption principles, even without direct interference on the encryption algorithm or the key management system.

The perception of the encryption regulatory environment in Brazil is frequently ambivalent: it would be simultaneously supported and threatened. The support would come from norms such as the General Data Protection Law (*LGPD)*, the Internet Bill of Rights (*Marco Civil da Internet*), and Decree No. 8771/2016. They would encourage the use of encryption by society, even with no express reference in the case of both laws. Similarly,

the opinions from the actions at STF and the STJ case law could indicate the recognition of the encryption importance for Brazilian institutions. On the other hand, the inconclusive judgment in the STF and the recurrent attempts to introduce backdoors would sign that encryption remains under threat in the country.

Regarding this subject, two distinct discourses on the issue of encryption regulation emerged. One advocates the introduction of explicit guarantees in legislation, either through an express legal statement that the use of encryption by citizens and businesses is lawful or by converting current incentives to use encryption into a binding duty applicable to specific providers and applications. On the other hand, the second discourse questions whether the expressed legal reference to encryption would be positive, understanding that such an approach contradicts the ideal of technological neutrality of regulation and that it may represent an undue interference in the scientific advancement of the field of information security.

Finally, three theses regarding the WhatsApp blockings and their relationship with the Internet Bill of Rights have appeared. The first one sees the blockings as illegitimate. This is either because their impact was out of proportion or because of the sanctions from the Internet Bill of Rights which according to them would be inapplicable. The inapplicability could be due to the technical impossibility of complying with the order whose disobedience caused the sanctions. It could also be due to the interpretation that the sanctions from the Internet Bill of Rights are for cases of rights to privacy and users' data protection violation.

The second thesis, on the other hand, sees the blockings as legitimate once the Internet Bill of Rights would predict the implementation of sanctions for the event of non-compliance with Brazilian law. Since court orders are based on Brazilian law, their non-compliance would result in the law's violation. According to the third thesis, the blockings' legality would not depend on the Internet Bill of Rights itself, as magistrates can determine atypical protective measures in the absence of a legal provision sufficient for the specific case - the so-called general power of caution.

It is important to point out the common understanding that the actual cause of the blockings was a political conflict between the company Facebook and the Brazilian criminal justice system institutions. Therefore, the episode would have economic and political impacts that would go beyond the specific legal controversy.

Analysis. With regard to the insertion of a backdoor mechanism, it is not evident that from the obligation to conduct intercepts, in the cases and terms of the law, it is possible to deduce an ability to change the system architecture to make the intercept feasible. In regard to the measures' implication, there is a scientific consensus in the field of information security about the impossibility of guaranteeing that the exploitation of the mechanism is carried out only in a lawful manner. In addition, there is empirical evidence that regulations that weaken encryption do economic harm. Finally, studies on the Brazilian political and legal environment have indicated processes of suppression of democratic

freedoms and the use of technology to enable authoritarian measures – a phenomenon sometimes referred to as techno-authoritarianism.

As for alternatives to backdoors, each one of them has different implications. The judicial order, with sanctions, to a user to deliver the password to unlock a device was recently considered unlawful by the Superior Court of Justice in the judgment of the RHC (Habeas Corpus Appeal) No. 580.664 - RJ, based on the constitutional prohibition of self-incrimination which implies the unlawfulness of this decision. It is important to point out that civil society and international organizations criticize government hacking and its excessive potential for abuse. They suggest that any practices of this nature are only allowed in exceptional cases, subject to legal requirements, necessity, proportionality, legitimate purpose, judicial supervision, among others.

Regarding the proposed insertion of a user or phantom key in communications, its implementation requires interference in the procedure of key distribution, which implies the uncontroversial conclusion that the measure represents a weakening of encryption. Then, the risks are similar to those identified in backdoors implemented by more conventional means, such as key escrow.

On client-side scanning, the potential absence of direct interference in the encryption system implies that verifying an encryption breach is more controversial. Regardless of it, however, it important to point out that there is a need to reduce the system security due to the expansion of the attack surface, which implies the possibility of producing false positives by compromising the database used for comparison. Still, the possibility of distorting the system's function represents a democratic risk that causes criticism from organized civil society.

Regarding the WhatsApp blockings and its relationship with the Internet Bill of Rights, it is crucial to reaffirm that the assumption that there is of a duty of carrying out interceptions not only lacks reasoning but it is also against the mentioned decision from the Superior Court of Justice. Concerning the Internet Bill of Rights provisions, the Federal Supreme Court plenary decision is still pending, but the rapporteurs' cases have already accepted the thesis that restricts the sanctions to privacy and protection of personal data violations. Regarding the judge's general power of caution, recognizing excessive damage caused by blocking the application implies the absence of the required proportionality.

Therefore, because of the above-mentioned reasons, we conclude that it is clear that the WhatsApp blocking was illegal regardless of what the Supreme Court decides on the applicability of the Internet Bill of Rights' sanctions. They are illegal due to the technical impossibility of complying with the data delivery orders because of factual obstacles represented by the encryption - as understood by the STJ. Even if they were lawful, they could not be based on the judge's general power of caution due to the disproportionate impact in relation to the desired goals – according to the blocking suspension orders repeatedly acknowledged.

Conclusions. The present analysis highlights the complexity and heterogeneity of dimensions and perspectives that characterize cryptographic wars. Given the impossibility of an exhaustive examination of all these aspects, the mapping of rationalities conducted in this study allowed us to to see legal and factual premises whose merit is subject to academic assessment, which can significantly contribute to the debate's maturing. At the same time, it demonstrated the existence of socio-technical rationalities and in-depth political disputes that underlie the actors' points of view, which reinforces the permanence of cryptographic wars beyond controversies about specific premises.

1. Introduction

Encryption has become one of the most relevant security tools for the digital environment over the last few years. As the use of diverse internet services spread, the demand for these services to be provided safely has also increased. Therefore, encryption was progressively widespread in society during the second half of the 20th century and the beginning of the 21st century. Some of the main current applications with this feature include private messaging platforms, electronic transactions, digital banking services, healthcare systems, and air traffic control mechanisms.

Nevertheless, the spread of encryption in society has some controversies. In recent decades, law enforcement authorities have adopted a rhetoric critical of some cryptographic applications, notably the use of strong encryption[1] to protect information stored or communicated by individuals. For these institutions, the mass consumption of strong encryption in personal devices and communication platforms has become an obstacle to the exercise of their functions, as it hinders the production of information necessary for the prevention and repression of criminal activity. Such actors sometimes use the term "obscuration" (Going Dark) to describe the alleged phenomenon that encryption would make digital communications unreadable to police authorities, which would benefit illegal acts[2].

According to this perspective, there has been some State attempts to restrict or limit the development and use of strong encryption in several countries such as Brazil, the United States, the United Kingdom, Russia, and Australia[3]. In general, such efforts relate to the demand for a mechanism's insertion that gives the State authority access to encrypted information. These proposals often meet resistance from information security experts

1 An encryption algorithm is strong or computationally secure when its security cannot be breached promptly with the computational resources available today or in the future. See SCHNEIER, Bruce. **Applied Cryptography**: Protocols, Algorithms, and Source Code in C. 20th Anniversary Edition. New Jersey: John Willey & Sons, 1996, p. 30.

2 See BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (BERKMAN). **"DON'T PANIC":** Making Progress on the "Going Dark" Debate. 2016**.** Available at: https://cyber.harvard.edu/pubrelease/dont-panic/. Access on 02/08/2021.

3 RODRIGUES, G. R. A controvérsia cifrada: o Clipper e o mito da derrota estatal nas guerras criptográficas dos anos 1990. Em: ALVES, Marco Antônio Sousa. NOBRE, Marcio Rimet. (orgs.). **A sociedade da informação em questão**: o direito, o poder e o sujeito na contemporaneidade. Belo Horizonte: D'Plácido, 2019.

and digital rights activists, who counter them with claims that such a change would reduce the security of systems and subject citizens to potential abuses of power[4].

Commonly referred to as Crypto Wars, such controversies have played an important role on debates about internet policy governance in the 2010s. They evoke duties and sanctions applicable to internet service providers, political conflicts between State actors and global technology companies, and symbolic disputes over the meanings of the concept of security and its relationship to privacy. Thus, they mobilize the perspectives of various actors, such as criminal justice representatives, heads of private technology companies, digital rights activists, information security specialists, lawyers dedicated to technological issues, among others.

In order to understand the technical, legal, political, and economic rationalities from the encryption debate in Brazil, the present work aimed to map different stakeholders' arguments, beliefs, and perceptions about the relationship between encryption, privacy, public safety, information security, and rights. For this purpose, qualitative interviews were carried out with more than 40 professionals specialized or engaged in the debate on these themes. The interviewees were selected by using the snowball sampling method. The transcripts of the interviews were then coded and submitted to systematic qualitative content analysis using the Atlas.ti 7.0 software. At last , after the analysis was done , their arguments and points of view were narratively reconstructed and presented in this work.

This research is considered relevant because of its current subject and also political importance, which have already been described. Moreover, because of its object and its innovative approach. It is important to point out that interdisciplinary impact studies that empirically address the different perceptions of those involved in the controversy are little known or non-existent in the national academia. The legal approach has predominated in the country, generally, through studies[5] that examine the blockings suffered by the WhatsApp application in light of the Brazilian legal system, analyze and compare different regulatory models or discuss the relationship between encryption and fundamental rights. In this scenario, this study has potential to contribute to future research agenda that examines in-depth thesis and perceptions here discussed.

The text has six sections, including this introduction and two appendixes. In the second section, we present a brief contextualization of the crypto wars in the United States and Brazil, recalling some of the processes and episodes that marked the history of the debate

4 RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

5 See, for example, KURTZ, Lahis P.; MENEZES, Victor. A.. Entre o direito e a força na sociedade da informação: bloqueio judicial do WhatsApp e ADI no 5.527. In: Fabrício Bertini Pasquot Polido; Lucas Costa dos Anjos; Luiza Couto Chaves Brandão. (Org.). **Tecnologias e conectividade**: direito e políticas na governança das redes. 1ed. Belo Horizonte: 2018, v. 1, p. 15-30.; CARVALHO, Thaís B.. **O bloqueio judicial do WhatsApp no território brasileiro no contexto do Estado Democrático de Direito.** 2017. 69 f. Monografia de graduação no curso de Direito - Universidade Federal de Lavras, Lavras, 2017; ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. de Políticas Públicas**, Brasília, v. 7, no 3, 2017 p. 24-42.; DONEDA, Danilo. MACHADO, Diego. (coords.) **A criptografia no direito brasileiro**. São Paulo: Thompson Reuters - Revista do Tribunais, 2019.

in these contexts. In the third section, we detail the research methodology by presenting the interviewees' selection, the conduction of the interviews, and the data codification and analysis.

In the fourth section, we present the research results with the interviewees' perceptions on the following topics: i) backdoors for a criminal prosecution, ii) possible alternatives for authorities' access to decrypted content without direct interference with encryption, as well as their risks, iii) factual and normative assessment of the national regulatory environment related to encryption, and iv) opinion on WhatsApp blocking in Brazil and its relationship with the Internet Bill of Rights.

Then, in section five, the authors discuss the results, considering contextual aspects and relevant references for the debate. Finally, the conclusions are presented in the last section, followed by the appendices - where you can find additional information on the research's methodological path.

2. Context - The Crypto Wars

As cryptographic techniques evolved, the strategic applicability of this technology for tools creations of different natures – including for military applications – became increasingly evident, which, valued encryption in the eyes of governments around the world. At the same time, technical advances in this area combined with the prospect of exporting and facilitating access to advanced cryptographic techniques for other countries and even for civil society, motivated protectionism by governments that had more advanced knowledge in the area of encryption.[6] [7]

These protectionist measures are precisely what we call the Crypto Wars. In general, they were conflicts between the public and private sectors, in which the State aimed to interpose barriers to the mass use of encryption by companies that, aware of the technology's commercial appeal, aimed to include it in their products. Traditionally, two main occurrences of these events are listed – at the end of the 20th century and from 2013 onwards –, corresponding to the First and Second Crypto Wars[8]. However, It is important to highlight that the Crypto Wars were not isolated and compartmentalized events, but

6 FROOMKIN, M. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

7 INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. Cryptologia, v. 3, n. 3, 129 - 135, 1979.

8 Despite the usual enumeration of the Cryptographic Wars in two instances, historian and cryptologist Craig Jarvis argues in favor of recognizing at least one more of these events. According to Jarvis, the First Cryptographic War would have occurred between the years 1966 and 1981, encompassing events such as the creation of the first cryptographic algorithm approved by the US government (the so-called DES, or "Data Encryption Standard"), which was accused by several cryptologists of having had its operation altered to allow extraordinary NSA access to encrypted communications. The First Cryptographic War, according to the author, would also have included the US government's attempt to prevent the publication of The Codebreakers, by David Kahn. For more information, see: JARVIS, Craig. Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. CRC Press, 2020.

rather highlight points in a context of perennial conflict involving State, business and civil interests[9]. On the following section, 2.1, a brief summary of the main events that marked this conflict and its main milestones will be presented in order to contextualize the reading.

2.1. Crypto Wars in the 20th Century

There were two main episodes that summarize the first stage of the Crypto Wars, whose roots are in the 1970s and that lasted approximately until the end of the 1990s.

During World War II, encrypted messages were used to allow radio communication between allied forces, preventing them from being interpreted by the enemy. In this scenario, efforts were made to decipher enemy communications and gain strategic advantages. Around this period – due to its enormous military utility – encryption came to be considered by the USA government as analogous to military ammunition.

In this context, the first moment of the Crypto Wars consisted of a series of tensions related to the USA's attempts to restrict the domestic and foreign spread of encryption. Externally, this took place through the imposition of strict barriers to the export of cryptographic techniques. Categorized as a form of weaponry, encryption was included among the items protected by US laws relating to the export of military equipment – the International Traffic in Arms Regulations and the Arms Export Control Act[10], both acts from 1976.

On the domestic front, the NSA's actions aimed at inhibiting the spread of strong encryption in the private sector and civil society. At this point, the government's attempt to determine the cryptographic algorithm to be used by the private sector – the Data Encryption Standard (DES), developed by the NSA and the National Standards Agency – stands out.[11] In 1977, the country's federal government selected a revised version of this standard – the LUCIFER algorithm, developed by IBM – as the national standard. The implementation of LUCIFER/DES was the object of criticism by the technical community and the private sector, as it imposed a severe limit on the size of cryptographic keys[12]. Furthermore, critics suspected that there might be a backdoor – a vulnerability purposefully inserted into the system – in the algorithm.

9 AULA 4 - Criptografia: experiências regulatórias e debates internacionais com Diego Canabarro. Belo Horizonte: Instituto Iris, 2021. (39 min.), son., color. Available at: https://youtu.be/EDaI5_z-hBo?t=2200. Accessed in: 25 ago. 2021.

10 ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, no 3, 2017, p. 24-42. p. 29.

11 LIU, H. Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause. **Journal of World Trade**, v. 51, n. 2, p. 309 - 334, 2017.

12 The standard originally proposed would allow 100-bit cryptographic keys, but the NSA required this number to be reduced to 56. Since smaller keys are more easily cracked through exhaustive key-search attacks, in which all keys are quickly traversed. possible, critics came to see LUCIFER/DES as designed so that the key was "long enough to frustrate corporate eavesdroppers, but short enough to be broken by the NSA". See: FROOMKIN, M. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. University of Pennsylvania Law Review, vol. 143, no. 3, p. 709–897, 1995, p. 735.

Moreover, the 1970s were marked by another key event: the publication of the article New directions in encryption written by Whitfield Diffie and Martin Hellman which was published in the IEEE Transactions on Information Theory magazine in 1976[13]. Currently known as public-key encryption or asymmetric encryption, the Key distribution method developed by the authors mentioned previously allowed the development of systems that don't need any trusted third party. Combined, civil resistance to LUCIFER/DES and the advent of asymmetric encryption signaled a threat to the NSA's control over encryption. Concerns of this nature were already expressed by the agency's leadership at the end of the decade. In 1979, for example, Bobby Inman, who was back then the director of the agency, wrote about the story[14]:

> Viewed from the NSA's perspective, the crux of the problem is that increased concern over telecommunications protection in the nongovernmental sector implies increased public knowledge and discussion of communications protective techniques. The principal such technique, of course, is encryption. There is a very real and critical danger that unrestrained public discussion of cryptologic matters will seriously damage the ability of this government to carry out its mission of protecting national security information from hostile exploitation.

The second tipping point came years later, in the 1990s – although during that time US pressure against the spread of encryption remained constant. The beginning of this new phase of the Crypto Wars took place in 1993 when the Escrowed Encryption Standard was proposed. As the name suggests, it was a proposal whereby the US government intended to standardize the sale of encryption to third parties, making it a condition that the cryptographic keys of the communications would be held in custody by public investigation agents[15].

This objective would be achieved through the implementation of the so-called "Clipper Chip" and "Capstone Chip" respectively in telephones and computers - coprocessors that would encrypt communications made by users but would keep a copy of the cryptographic keys in the custody of a third party deemed trustworthy by the proponents of the standard. This way, through a backdoor, US investigative entities could have access to all contents of encrypted communications from users.[16]

13 DIFFIE, Whitfiead. HELLMAN, Marin. New directions in cryptography. **IEEE Transactions on Information Theory**, 22, 644-654.

14 INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. **Cryptologia**, v. 3, n. 3, 129 - 135, 1979.

15 FROOMKIN, Michael. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

16 SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 234-235.

The proposed standard was the target of severe criticism from the business sector, aware that the marketing of devices containing Clipper and Capstone was bound to suffer in the face of international competition from foreign companies that were not subjected to these legal requirements. At the same time, there was a great mobilization against the Escrowed Encryption Standard by the technical-scientific community and civil society, who respectively pointed out the security risks of the model and the affronts it represented to civil liberties. [17]

Alongside the pressure against the use of Clipper and Capstone, the launch of PGP (Pretty Good Privacy) in 1991 was fundamental to the fall of the Escrowed Encryption Standard. PGP is a free public-key encryption software that served as the civilian population's initial exposure to truly secure cryptographic algorithms. Its creator, Phil Zimmermann, was subjected to years of investigation by US authorities but he was eventually found innocent, with the acknowledgment that US free speech legislation protected the methods used to share the software.[18]

During the 1990s, there were several public hearings held on the subject. The hearings contributed enormously to the public dissemination of the debate on encryption, security, and privacy. The discussion culminated in the public downfall of proposals such as Clipper and Capstone.

At the end of the millennium, the public defeat of the Escrowed Encryption Standard, as well as popular pressures to release the use of strong and secure encryption in the US, and international competition from countries that were also developing their cryptographic techniques culminated in the loosening of the barriers created since the 1970s for the commercialization of this technology. During this period, there was considerable growth in encrypted services utilization, which began to be used on a large scale by the civilian population.

This does not mean that the cryptographic wars have simply ended at the end of the 20th century. As sociologist Karina Rider[19] argues, the first decade of the 21st century was marked by the consolidation of massive surveillance programs conducted by the US intelligence sector with the cooperation of several technology companies. Bullrun, one of the main programs in question, aimed to ensure that an NSA would remain able to access encrypted communications, whether by intentionally weakening the algorithms or by manipulating the cryptographic market. If in the spotlight of public debate such as cryptographic wars, the 2010s can be understood as a period of concealment of the Crypto Wars, which start to take place far from the spotlight of public debate.

17 ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017, p. 24-42.

18 SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 226-237.

19 RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

2.2. Current Crypto Wars (2013 - present)

The so-called Second Cryptographic War began approximately in the year 2013, from the denunciations of Edward Snowden. The former member of both the Central Intelligence Agency (CIA) and the US National Security Agency (NSA) denounced the cyber-surveillance practices adopted by the US government, which started a global movement to search for truly effective security mechanisms.

A second notorious event took place in 2015: Apple vs. FBI. The lawsuit was filed due to the full disk encryption used in the manufacturer's cell phones. The FBI tried to find a way to force the company to unlock an iPhone 5C whose content had strong encryption protection, and which had been used by an individual accused of terrorism in San Bernardino, California. The company refused to assist the investigating body, claiming that implementing a backdoor into its operating system would result in damage to the security of the entire iOS platform user base. The FBI withdrew the lawsuit because they had access to the cell phone content by using various means. The Apple v. FBI was used as an example to increase the pressure used by investigative authorities against strong encryption techniques[20].

This pressure was well illustrated by a speech[21] given in 2014 by then FBI Director James Comey, who contributed significantly to the public diffusion of the concept of "Going Dark". It is the idea that modern security and privacy mechanisms represent an "obscuration" of State investigative tools and, therefore, represent an obstacle to the fight against cybercrime, terrorism, and the enforcement of justice.

Going Dark was later mentioned in a report[22] published in 2017 by the Office of the US Director of National Intelligence (ODNI). The document presents possible solutions to the issue of obscuration, with recommendations that include strengthening the so-called government hacking activities, as well as technical partnerships with representatives of the private sector, to provide investigative authorities with access to evidence that was considered necessary for the criminal prosecution of possible offenders.

The narrative of obscuration eventually gained international repercussions and motivated the creation of a legislation that seeks to weaken strong encryption in several countries. Notably, one can cite the approval of the Telecommunications and Other Legislation Amendment in Australia in 2018, which determines, among others, that communication service providers facilitate the access of State authorities to data, including encrypted, through technical assistance warrants or access to information.[23]

20 MITCHELL, Bonnie et al. **Going Dark**: Impact to Intelligence and Law Enforcement and Threat Mitigation. US Department of Homeland Security. Office of Intelligence and Analysis. 2017. p. 14

21 COMEY; James B. **Going Dark:** Are Technology, Privacy, and Public Safety on a Collision Course? Out. 2014, discurso realizado na Brookings Institution. [Online]. Available in https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Access on: 02 ago. 2021.

22 MITCHELL, **Bonnie et al. Going Dark:** Impact to Intelligence and Law Enforcement and Threat Mitigation. 2017.

23 Stilgherrian. **The Encryption Debate in Australia:** 2021 Update. 2021.

India has also recently become an example of a country whose legislation presents potential obstacles to the use of cryptographic techniques. This is because in 2021 the amendment to the rules applicable to digital media in the country was approved, with traceability obligations of the original perpetrators of the published content. In this regard, there is concern that instant messaging applications with end-to-end encryption to protect their users' communications might have their systems' security compromised to meet legal requirements.[24] [25]

2.3. Crypto Wars in Brazil

2.3.1. WhatsApp blockings in the country

Similar to what happened in the US and other countries around the globe, the debate regarding the obscuring of justice has also gained momentum in Brazil. The four attempts to block the WhatsApp app between 2015 and 2016 were some of the first instances of this debate in the country.

In February 2015, in the District of Teresina, Piauí, Judge Luiz de Moura Correia granted the request, made by the Intelligence Center of the Civil Police of the State of Piauí, to suspend the company's activities in Brazil. In a memo, the magistrate stated that the measure was "due to repeated non-compliance court orders issued by this Court, in various procedures that investigated crimes of the highest gravity".[26] The order was suspended on the same day by the Court of Justice of Piauí[27], which considered it out of proportion and harmful to users, in addition to understanding that there were less harmful means of investigation. The blocking was not put into effect.

The second blocking took place in December of that same year by determination of the 1st Criminal Court of São Bernardo do Campo, São Paulo, and it was suspended approximately 12 hours after its beginning[28]. As reported in the injunction suspending the blocking[29], the

24 GROVER, Gurshabad; RAJWADE, Tanaya; KATIRA, Divyank. The Ministry And The Trace: Subverting End-To-End Encryption, 14 NUJS Law Review. 1(2021). p. 2-6. Available in http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/. Access on: 02 ago. 2021.

25 RAY, Trisha. The Encryption Debate in India: 2021 Update. 2021.

26 BRASIL. Central de Inquéritos da Comarca de Teresina. **Nota**. Juiz Luiz de Moura Correia. Teresina, 26 fev. 2015. Available in: http://s2.glbimg.com/MdNVliNDOaF45o27HM8_tsG3wlI=/s.glbimg.com/jo/g1/f/original/2015/02/26/nota_juiz_whatsapp_ok.jpg. Access on: 29/07/2021.

27 BRASIL. Tribunal de Justiça do Estado do Piauí. **Mandado de Segurança nº 2015.0001.001592-4**. Rel. Des. Raimundo Nonato da Costa Alencar. Teresina, 26 fev. 2015. Available in: <http://www.migalhas.com.br/arquivos/2015/2/art20150227-03.pdf> Access on: 29/07/2021.

28 BARIFOUSE, R.; DUARTE, F.; BARRUCHO, L. G. Liberação do WhatsApp não encerra polêmica disputa com Justiça brasileira. **G1**. Tecnologia e Games. Available in: http://g1.globo.com/tecnologia/noticia/2015/12/liberacao-do-whatsapp-nao-encerra-polemica-disputa-com-justica-brasileira.html. Access on: 29/07/2021.

29 BRASIL. Tribunal de Justiça do Estado de São Paulo. **Mandado de Segurança nº 2271462-77.2015.8.26.0000**. Decisão liminar. Rel. Des. Xavier de Souza. São Paulo, 17 dez. 2015. Available in: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_22714627720158260000_17122015.pdf. Access on: 29/07/2021.

company failed to comply with a court order to intercept telematics communications from three people accused of drug trafficking, which led to the application of a drug fine and, subsequently, the blocking of the application for 48 hours. The Court of Justice of the State of São Paulo suspended the blocking on the grounds that the measure violated the principle of proportionality and that there were less harmful means of coercion by the company, such as increasing the amount of the fine.

After the first two blocks, WhatsApp announced on April 5, 2016 the implementation of end-to-end encryption[30], stating that "all messages, photos, videos, files and voice messages" exchanged between users using the latest versions of the application would be protected by encryption, using the Signal cryptographic protocol.

Later that month, the third case occurred, when the criminal court of the Comarca of Lagarto, Sergipe, ordered, on April 26, the suspension of the application for 72 hours due to new non-compliance with a court order for the delivery of personal data of users of the app[31]. The order cited articles 3, 10, 11, 12, 13, and 15 of the Internet Bill of Rights as its foundations. The blocking was suspended by the Court of Justice of Sergipe[32], which understood that the suspension of services generated "general chaos throughout the territory", as well as not being possible to say "that the information could be provided by WhatsApp or that it can be decrypted to serve justice".

Finally, the fourth blocking was ordered by the 2nd criminal court of the Judicial District of Duque de Caxias, Rio de Janeiro, also for non-compliance with a court order for breach of confidentiality and telematic interception of messages. As reported in the decision[33], the order was answered with an email written in English, which was interpreted by the magistrate as a sign of disregard towards the national authority. The document refers to articles 7, 10, and 11 of the Internet Bill of Rights, to article 139, IV, of the Code of Civil Procedure, and article 3 of the Code of Criminal Procedure. The blocking was suspended by the Supreme Court, which found that the blocking violated the fundamental precept of freedom of expression, as well as a disproportionate measure[34]. Therefore, based on the general power of caution, he reversed the decision.

30 WHATSAPP INC. **Blog do WhatsApp**. Criptografia de Ponta-a-Ponta. 05 abr. 2016. Available in: https://blog.whatsapp.com/end-to-end-encryption. Access on: 30/07/2021

31 BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. **Processo nº 201655090143**. Decisão. Juiz Marcel Maia Montalvão. Lagarto, Sergipe, 26 abr. 2016.

32 BRASIL. Tribunal de Justiça do Estado de Sergipe. **Mandado de Segurança nº 201600110899**. Decisão liminar. Rel. Des. Ricardo Múcio Santana de Abreu Lima. Aracaju, 3 mai. 2016. Available in: <http://www.omci.org.br/m/jurisprudencias/arquivos/2016/tjse_201600110899_03052016.pdf> Access on: 2 nov. 2016.

33 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Inquérito Policial nº 062-00164/2016**. Juíza Daniela Barbosa Assumpção de Souza. Duque de Caxias, RJ, jul. 2016. Available in: <https://drive.google.com/file/d/0Bw3seZUv__5ubnFudjUwMm9OZGc/view>. Access on: 30/07/2021

34 BRASIL. Supremo Tribunal Federal. **Medida cautelar de arguição de descumprimento de preceito fundamental**. Decisão liminar. Rel. Min. Ricardo Lewandowski. Brasília, 19 jul. 2016. Available in: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf. Access on: 30/07/2021.

2.3.2. Encryption in the Supreme Court: ADI 5527 and ADPF 403

The various WhatsApp blocking episodes in Brazil caused a large impact among different sectors of society: from users in general, who were impacted by the inaccessibility of the service during the validity of these court orders, to the legal and technical-scientific community, which commented extensively on the legitimacy or otherwise of blocking commands.

Concomitantly to the debate of the cases, the Claim of Non-Compliance with a Fundamental Precept (ADPF) No. 403[35] was filed before the Federal Supreme Court and, shortly after, the Action of Unconstitutionality (ADI) No. 5527[36]. The purpose of these actions was, in summary, to put the legal validity of the WhatsApp blocking orders in question before the highest level of the Brazilian Judiciary so that the decision creates a jurisprudential mechanism that prevents new blocking orders on the platform.

Filed shortly after the second determination of blocking the platform, ADPF 403 maintains that court orders of this nature violate the fundamental precept of freedom of communication – set out in article 5, IX, of the Federal Constitution. In addition, it is alleged that there was also a breach of the principle of proportionality, given that the blocking orders - related to scattered and individual cases that are being processed in the Judiciary - result in the inaccessibility of the platform throughout Brazilian society.

ADI 5527 seeks to declare the unconstitutionality of the articles of the Internet Bill of Rights (MCI - Law nº 12.965/2014) used to substantiate the court orders blocking WhatsApp. More specifically, it is argued in favor of the declaration of unconstitutionality of items III and IV of article 12 of the Internet Bill of Rights, which concern the sanctions of temporary suspension and prohibition of the activities of application providers for failure to make available content of private communications required in court (as provided for in article 10, paragraph 2, of the same law). In addition, the ADI seeks to limit the effects of article 10, §2, so that this legal provision apply only to cases of criminal prosecution - and not for non-compliance with court orders in the civil area, as occurred with the WhatsApp blocks.

Due to the similarity of themes addressed in both lawsuits, a joint public hearing was held in 2017, to gather information on technical and practical issues involved in the disputes over the platform's blockings. For two days, several entities, representing the interests of the technical-scientific, governmental, third sector, and business sectors, were heard by the reporting Ministers of both actions of concentrated constitutionality control[37]. The

35 BRASIL. Supremo Tribunal Federal. **ADPF 403**. Relator: Edson Fachin. Brasília, DF. Available in: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Access on: 06 ago. 2021.

36 BRASIL. Supremo Tribunal Federal. **ADI 5527**. Relatora: Rosa Weber. Brasília, DF. Available in: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Access on: 06 ago. 2021.

37 ABREU, Jaqueline. **Audiência Pública sobre Criptografia e Bloqueios do WhatsApp:** argumentos diante do STF.

decisions rendered by the STF in each of these processes will be paradigmatic for the future of communications protected by strong encryption in Brazil. Due to the complexity and sensitivity of the issue, however, both ADPF 403 and ADI 5527 are still awaiting final judgment, due to a request for the case records examination by Minister Alexandre de Moraes in May 2020. Regardless, important pronouncements and votes have already been made by their rapporteurs.[38]

Minister Rosa Weber, rapporteur of ADI 5527, for instance, has already stated that the provisions of items III and IV of article 12 of the Internet Bill of Rights are intended for non-compliance with obligations to protect records, personal data, and communications – and not for non-compliance with court orders.

Moreover, she argued that there is no dichotomy between the search for public safety and the right to privacy – as is often alleged by investigative bodies and defenders of the idea of obscuration. In this regard, the Minister pointed out that measures of exceptional access to encrypted communications represent violations of the rights to freedom of expression and protection of the confidentiality of communications. Furthermore, the weakening of encryption would represent a setback for the country and would be a "gift to authoritarian and criminal regimes".

Minister Edson Fachin – ADPF 403 rapporteur - defended the idea that digital rights should be as comprehensive as the rights that the population has offline and represent fundamental rights of Brazilians. Hence, the Minister argued that encryption is a means of ensuring the protection of rights that are essential for public life in a democratic society. Therefore, it would be contradictory to reduce internet security in the name of public safety. Fachin also argued that the implementation of backdoors or other systemic vulnerabilities in cryptographic algorithms – even if only intended for investigative authorities – would represent a weakening of the security of these systems in a universal way. This is because malicious third parties would also have access to these tools, putting all users of affected services at risk.

2.3.3. Encryption under the Brazilian law and other recent conflicts

The current Brazilian legislation, for the most part, makes no specific mention of cryptographic techniques. Yet, it does not mean that there is not encouragement to implement this technology in digital systems.

The Internet Bill of Rights, for example, promotes the use of technical measures compatible with international standards to preserve the stability, security, and functionality of the

26/06/2017. Bloqueios.info . Available in <http://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/ >, Access on 02 ago 2021.

38 CANTO, Mariana. RAMIRO, André. REAL, Paula C. **Criptografia no STF:** O que dizem os votos de Rosa Weber e Edson Fachin e o que podemos aprender com eles. Available in https://ip.rec.br/2020/06/22/criptografia-no-stf-o-que-dizem-os-votos-de-rosa-weber-e-edson-fachin-e-o-que-podemos-aprender-com-eles/. Access on 02 ago 2021.

network (article 3, V). The regulatory decree of this law (Decree nº 8.771/2016), in turn, lists encryption as one of the possible and recommended technological solutions to secure the management of digital records (article 13, IV).

More recently, the General Law for the Protection of Personal Data (LGPD - Law nº 13.709/2018) determined the adoption of adequate technical standards so that processing agents may guarantee the security of personal data they hold. Such provisions can be found, for example, among the guiding principles of data protection in Brazil (article 6, VI, and VII), in the legal requirements for data security and confidentiality (arts. 46, 47), in the provisions for a relaxation of the penalties applied in data protection incidents when it is proven that the processing agents involved have adopted adequate technical, administrative and operational standards to avoid the incident (article 48, § 3, and 52, § 1, VIII), among others.

Regarding the use of encryption in private messaging applications, the Superior Court of Justice (STJ) has already ruled more than once in defense of data encryption used in these services. In this regard, the Third Section[39] and the Fifth Chamber[40] of the STJ ruled that it is not appropriate to impose a fine on private messaging providers for non-compliance with a court order due to technical impossibilities inherent to the technology used.

Despite these legal statements and recent jurisprudential understandings, a series of bills that, in one way or another, seek to relativize the right to use strong encryption in Brazil, are being processed in the national Legislature. For example, Bill No. 5.285/2009, Bill No. 9.808/2018, Bill No. 11.007/2018, and Bill No. 2.418/2019. Despite having different legislative measures, all these projects have in common the objective of restricting or weakening the right to use cryptographic techniques in Brazil - either through the express criminalization of the act or even through the institutionalization of mechanisms for the State's backdoor access to encrypted communications.[41]

Nevertheless, the importation of the Going Dark narrative to Brazil had other repercussions for the national scene. In 2019, the I Symposium Going Dark Brazil was organized by the former Minister of Justice and Public Security, Sérgio Moro.[42] The event aimed to expose the difficulties of State investigative bodies regarding the use of encryption and ended with

39 BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas.** 30/12/2020. Available in < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx >, Access on 03 ago 2021.

40 BRASIL.Superior Tribunal de Justiça. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma.** 24/06/2021. Available in <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021-Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decide-Quinta-Turma.aspx>, Access on 03 ago 2021.

41 Confira: RAMIRO, André. CANTO, Mariana. REAL, P. C. et al. **O Mosaico Legislativo da Criptografia no Brasil: Uma Análise de Projetos de Lei**. IP.Rec. Available in <https://ip.rec.br/wp-content/uploads/2020/08/O-mosaico-legislativo-da-criptografia-no-Brasil-uma-an%C3%A1lise-de-Projetos-de-Lei-1.pdf >, Access on 04 ago 2021.

42 BRASIL. Ministério da Justiça e Segurança pública. **Simpósio sobre Going Dark termina com declaração de 13 países.** Available in <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2>, Access on 03 ago 2021.

the signing of a declaration[43] by representatives from 13 countries. In the document, recent technological advances – such as encryption and similar techniques – are presented as techniques used by terrorists and criminals to block the State's investigative power, which would motivate joint action by the international community to prevent abuses in this regard.

The so-called "Anti-Crime Package", also conceived by former Minister Sérgio Moro and enacted under Law No. 13.964/2019, is deserving of mention as well. In its original text, the regulation provided for the expansion of the interception powers of State investigative bodies and presupposed the duty of platforms to collaborate with criminal prosecution. Thus, the mechanism implied the extension of these obligations to service providers protected by strong encryption.

More recently, the preliminary text of the new Code of Criminal Procedure[44] has generated controversy as a result of the possible change in the current mechanisms of investigating authorities to confidential information. The project includes an expansion of State powers to intercept telematics communications. Among the content predicted ,the obligation of assistance established for telecommunications service providers stands out, according to which their providers would have a legal obligation to make available the resources and technological means necessary for their interception.

These statements aroused fear in members of organized civil society and the national[45] and international[46] technical-scientific community, due to the possibility of establishing a legal mechanism for the insertion of vulnerabilities in cryptographic systems, as a prerequisite for the regulatory compliance of communication services that employ measures of this nature which may represent a systemic reduction in the reliability and security provided by these services, in favor of alleged benefits to national security.

Therefore, the import of the Going Dark narrative into the Brazilian context, as well as the existence of an institutional war against encryption – the Crypto Wars – represent current tensions and threats to the future of this technology in Brazil.

43 BRASIL. **Declaração do Going Dark Brasil.** Available in <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2/documentos/declaracao-do-going-dark-brasil.pdf> Access on 04 ago 2021.

44 AGÊNCIA CÂMARA DE NOTÍCIAS. Relatório preliminar do novo CPP incorpora provas digitais e novas tecnologias ao processo criminal. Relator: Deputado João Campos. 13/04/2021. Available in <https://www.camara.leg.br/noticias/745824-relatorio-preliminar-do-novo-cpp-incorpora-provas-digitais-e-novas-tecnologias-ao-processo-criminal/ >, Access on 26 ago. 2021.

45 COALIZÃO PELOS DIREITOS NA REDE. Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. 20 de maio de 2021. Available in < https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>, Access on 25 ago. 2021.

46 Global Encryption Coalition. Brazilian Code of Criminal Procedure reform must not undermine encryption. June 28, 2021. Available in < https://www.globalencryption.org/2021/06/brazilian-code-of-criminal-procedure-reform-must-not-undermine-encryption/>, Access on 25 ago. 2021.

3. Methodology

This section describes the methodology used in the research. Item 3.1. details the selection and the profile of interviewees. Item 3.2 discusses the dynamics of the interviews. Item 3.3 explains the data coding and analysis procedure. Item 3.4. highlights the limitations of the adopted methodology.

3.1. Interviewees selection

Interviewees were selected using the snowball sampling method, in which some study participants indicate new participants, creating a social network that expands from the respondents' connections[47]. This method has the advantage of allowing access to groups that are difficult to reach, such as specialists. However, as it is a non-probabilistic sample, it does not guarantee the representativeness of the studied population. It is also more sensitive to selection biases, which constitutes a methodological limitation of this research. The initial participants were defined based on the project team's social networks and indications from ISOC Brazil, favoring people with expertise or previous participation in public discussions on encryption, privacy, and information security. In total, there were 76 invitations to potential interviewees.

Forty-five interviews were carried out: two of them were excluded from the analysis. The first one was excluded because the answers were insufficient and the second one because later it was found that the interviewee had no link with the presumed sector. 43 interviews were considered valid, 13 out of them were done with representatives of the private sector and 10 with each one of the other sectors (academia, civil society, and public sector). There was gender parity in all sectors, except the private sector, with 08 male and 05 female respondents.

As for the academic background, the legal field was predominant (27 interviews), followed by the computational field (08, including Computer Science, Networks and Computer Engineering), Social Sciences (05), Communication (04), Public Administration and Public Policy (03), Political Science and International Relations (02), Economics (01), History (01), Administration (01), Visual Arts (01) and interdisciplinary area (03). Furthermore, 14 of the interviewees had multiple backgrounds, either because they had various degrees or because they had undergraduate and graduated in different areas.

Regarding professional practice, the trajectories are pretty heterogeneous. The interviews were done with government relations managers from large digital platforms, researchers from technology and human rights NGOs, university professors dedicated to researching related topics, servers from regulatory agencies relevant to the technological field, master's

47 VINUTO, J. A amostragem em Bola de Neve na pesquisa qualitativa: um debate em aberto. **Temáticas** (UNICAMP), v. 44, p. 201-218, 2014.

and or doctoral researchers focused on the internet and society, lawyers specializing in digital law, criminal justice operators at the federal and State levels, national parliamentary advisors, digital rights activists, and free software, cybersecurity analysts from public and private entities, private information security consultants, among other fields.

3.2. Interviews conduction

The interview script contained questions related to the following themes. i) professional and academic trajectory, ii) importance to privacy and encryption, iii) perception of the relationship between privacy and security, iv) satisfaction with the national regulatory environment, v) opinion on backdoors and risks perception, vi) opinion on the public debate regarding privacy in Brazil, vii) opinion on alternative means of accessing encrypted content that did not involve interfering with encryption, vii) and opinion on the legitimacy of WhatsApp blocking in Brazil. We also asked interviewees with a legal background about their understanding of the application blocks' legality based on the Internet Bill of Rights. The respondents from the public sector answered about the importance of information security in the context of government digitization. The script's full version is in Appendix 1.

The interviews had a semi-structured character. Therefore, the script worked as a set of previously fixed guidelines, not as a protocol to be strictly followed in each concrete dialogue, and conducted similarly to informal conversations[48]. This methodological option favors trust and security relationships with the interviewees to make them feel more comfortable to speak more freely and sincerely - a necessary requirement for conducting interviews that produce wealthier data[49] -, especially due to the controversial and sensitive nature of some of the topics covered. Additionally, this option allowed a deeper exploration of the perspectives and specific knowledge of the interviewees.

This option, however, contributed to the fact that not all respondents answered the entire script uniformly. It was partly because of the in-depth exploration of their answers to specific questions which took longer .Thus , some themes were prioritized according to the concrete case. At the same time, the trajectories and education diversity also favored this variation, as issues relating to areas of knowledge or sectors did not necessarily make sense to everyone. For example, a question about the interpretation of specific provisions of the Internet Bill of Rights presupposed some degree of legal knowledge by the respondent, so it would not make sense to ask it in every interview.

48 BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais. **Em Tese - Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC**, Florianópolis, v. 2, n. 1 (3), p. 68-80, jan./jul. 2005, p.75.

49 GASKELL, G. Entrevistas individuais e grupais. In: BAUER, M. W.; GASKELL, G. (Org.). **Pesquisa qualitativa com texto, imagem e som**: um manual prático. Petrópolis, RJ: Vozes, 2000, pp. 64-89, p 74.

3.3. Data coding and analysis

After conducting the interviews, we transcribed their content and developed a data handling strategy to maintain the generated data confidential and secure. First, we replaced the respondents' real names with fictitious names from a name generator software, and then a conversion table was created. The files were encrypted and entered into an encrypted cloud application. The researchers involved in this part of the analysis downloaded and placed the files (interviews, transcripts, the name conversion table) in an encrypted compartment of their local devices. We shared the decryption key via a messaging application - equally encrypted and with the functionality to auto-destroy the message after a few minutes. In order to permanently delete the original files from the personal computers, we used a tool called BleachBit which destroys the digital files' traces. Once decoded, the analysis handled the materials previously allocated in the encrypted compartment. The analysis units transfer among the researchers were made through encrypted channels.

The interviews' content went through qualitative analysis, which consists of a "research technique for making replicable and valid inferences from texts (or other meaningful matter) to the contexts of their use"[50]. The qualitative data coding and statistical processing used the Atlas.ti 7.0 software, which offers a myriad of tools designed to support researchers in qualitative analysis[51]. Despite its benefits, it is important to point out that the program does not conduct the analysis by itself. Therefore, the researchers need to draw conclusions based on their conceptual and epistemological contributions.

The systematic qualitative analysis had an inductive character. The construction of both codes and categories of analysis was based on what was obtained from the data collected from initial exploration, and not from a pre-defined set of criteria. Taking an interpretive approach into account, we seek to reconstruct the meanings given by the interviewees to the topics discussed, which allows both a general apprehension of their beliefs, world perspective, and arguments and the generation of new hypotheses about the set of phenomena discussed in the interview based on the native theories from these professionals[52].

In order to narrow the analysis' scope, four general themes were selected and explored in different segments of the interviews: i) implementation of backdoors in encryption systems for access to encrypted data for purposes of criminal prosecution, ii) knowledge and risks about potential alternatives for authorities' access to decrypted content without direct interference with encryption, iii) the national regulatory environment regarding encryption, iv) WhatsApp blockings in Brazil and its relationship with the Internet Bill of Rights.

50 KRIPPENDORFF, K. **Content Analysis**: an introduction to its methodology. Thousand Oaks, Calif.: Sage Publications, 2004, p.18.

51 SILVA JUNIOR, L. A.; LEAO, M. B. C. O software Atlas.ti como recurso para a análise de conteúdo: analisando a robótica no Ensino de Ciências em teses brasileiras. **Ciênc. educ.** (Bauru), Bauru , v. 24, n. 3, p. 715-728, set. 2018.

52 ROSENTHAL, G. **Pesquisa social interpretativa**: uma introdução. Porto Alegre: Edipucrs, 2014.

For coding and analysis of each of these themes, the following procedure was followed: Firstly, the interviews were distributed among the researchers responsible for the study's empirical part for initial exploration and open coding of the segment. Then, there was a joint review of the entire coded universe and the consolidation of the codes. Based on this, we sought to establish relationships of meaning between the categories and, based on them, narratively reconstruct the main arguments and frameworks given by the interviewees to the topics covered. Due to the quadruple replication of this procedure, four distinct and independent coding schemes were produced, which are in Appendix 2.

3.4. Limitations of the methodology adopted

Due to the non-probabilistic nature of the selection methodology adopted, as well as the semi-structured nature of the interviews and variations in the script's application, the results below may represent the opinions or attitudes of any population segment.

They constitute an empirically based panorama of beliefs, arguments, and rationalities that permeate the public debate on Going Dark and Crypto Wars in Brazil, as it could be seen in the 43 interviews with professionals who participated in this debate construction.

4. Results

This section presents the content analysis' results. They are in the form of narrative reconstructions about the most frequent utterance categories. They aim to highlight the logical connections that permeate their rationalities.

All names used are fictitious and were randomly determined by using a name generator software. The highlights in bold were made by this study's researchers.

4.1. About inserting backdoors mechanisms in encryption

All interviewees answered the questions about backdoor mechanisms.

4.1.1. The pro-backdoor discourse

The support for exceptional access is based on the understanding that access to private communications **is necessary for public security (argument used 4x),** a value that should prevail when in conflict with other rights such as privacy and freedom of expression. According to this reasoning, the damages caused by certain crimes - for example, kidnappings, drug trafficking, child abuse, terrorism - are so serious that they justify the relativization of these rights in the name of the collective interest.

In addition, **citizens and companies must obey justice (7x)**, which implies the duty to comply with court orders to deliver data for criminal investigations, even if this requires making encryption vulnerable. In this sense, the law would already authorize the backdoors **as equivalent to a telephone interception (3x)**. In this case, they understand that the state's prerogative to access private communications in the cases provided for by the Telephone Interception Law extends to digital platforms. In the words of interviewee Afonso:

> I've been on the other side. I've been on the side of those who have to arrest the bad guy. And it is a lot of work when you have all the data encrypted.. [...] Backdoor is a word that also matches well. It's an exceptional access: it's wiretapping. **The police don't wiretap everybody by default, There is a rule. For me, this rule can be the same rule for wiretapping WhatsApp.**
>
> Afonso's background is in the computer field, focused on information security, and he has extensive teaching and consulting experience in private network and project management.

At this point, some even consider that **backdoors would be an investigative measure less burdensome than the currently employed (2x)**. The reasoning is as follows. Since access to such communications is necessary for investigations, backdoors would allow accurate access to the targeted channel. It would cause less damage than a search and seizure, for instance, which in addition to suppressing the inviolability of the home, makes it possible to search the entire device and all the information it contains. It is the view of the interviewee Thais, for example:

> Guys, it would be much better if we worked with a specific application that we say:'I only want to know about the messages from WhatsApp'. It's just WhatsApp; I don't want your photos, your contact list , what you talk to your wife about, got it? [...] It would be much more practical. So it turns out that **due to the lack of specific applications that can have access to these messages, we sometimes use more invasive mechanisms than we often needed.**
>
> Thais has a legal background and she works in the criminal justice system, with a focus on cybercrime.

As for the potential for abuse by authority, the existence of **robust institutional controls (11x)** would mitigate these risks. Such mechanisms include a specific and substantiated court order, determining the purpose and the exact individuals to be affected. The interviewees often emphasized that it should be **only for serious crimes (7x)**, such as those mentioned above, and **when other possibilities for investigation (3x) have already been exhausted**. Alongside, there is sometimes the perception that **it is necessary to trust institutions (2x)**. Interviewee Julian sums it up well:

> Now, I have to trust justice. I, as a lawyer. If there is a law establishing when, how, and under which conditions - only under these conditions - it can happen. And if there is a judicial authority invested by the State to make this decision. **If I don't trust this, I cannot trust anything in the justice [system]**. It would be a selective trust: "I trust justice, but not this." Why? There is a court, an internal affairs office, a CNJ. We have to trust it. [...] If there is no other resource. And if there is an eventual seriousness of the crime, with the proper law saying how this will happen, with a specific and well-founded judicial decision, I think so, I think we will have to face circumstances [in which] social peace is more important than the criminal peace.
>
> Julian has a legal background, extensive experience in the public sector with technology regulation, and he works in the institutional relations sector of a large company.

Defending that the State has access to encrypted content for investigation purposes also appears as a way to reaffirm public authority (1x). In this perspective, the defense of backdoors would symbolically reiterate that the investigative competence and the general power of the State are above the interests and decisions of private companies, which may find themselves in a position to challenge them due to their global strength. For Natalia, the defense of backdoors connects to this symbolic dispute.

> Companies need to find a way to collaborate with us, with society itself. Because the company makes its business model and they want to make money. **if there is no pressure from the government for this collaboration, why would they spend money setting up an entire sector of a company to support public authorities?** Then you think, wow, nowadays Google, Facebook, they have offices and sectors fully set up to attend law enforcement, for the investigation of public authorities. Why would they do this if there is no pressure from the public sector to do so? So, you need to pressure.
>
> Natalia has a legal background and she works in the criminal justice system, with a focus on cybercrime

4.1.2. The anti-backdoor discourse

The backdoor rejections is based on the perception that the measure **contradicts basic principles and good information security practices (20x)**. That is because the increase in a system complexity necessarily reduces its security. Especially through the intentional introduction of a vulnerability to be used regularly. Therefore, a backdoor would be a measure that "weakens the technology as a whole" and " it breaks the reliability of encryption in essence."

Such concern connects to two main risks. The first was that **malicious third parties could explore the mechanism (18x),** such as cybercriminals and foreign governments, who could use the vulnerability for illicit purposes. In this way, **the State's security would be weakened (4x)** since the confidentiality of communications from the authorities themselves depends on encrypted platforms. It is the perspective of interviewee Alvin:

> Let's assume for a moment, this is a very extreme assumption, which I don't believe in - personally, I don't - but let's presume there are good and bad actors. Let's assume that I live in a country of good actors and good politics, a good MP, great authorities, everyone is morally good, let's take that, ok? The question is: should these good people be allowed to access backdoors to investigate illegal situations? Well, I might think: yes, because they are good! I'm good, they're good, we want to protect the good guys. The problem is this logic doesn't exist. I don't believe it. It is not just good: it is everything. But following this logic, the problem is that not everyone is good in the world . There are other countries, other organizations. There are hackers, mafias, other states, right? **So when you create this backdoor for the "good guys" (these pure people who want to protect me and take care of me), when you have it for them, you also open up a vulnerability for others.** So, as a matter of fact, what is being created is a vulnerability that can be exploited by other governments, other organizations, other companies, other hackers, whatever.
>
> Alvin is an economist who has extensive experience in the public and private sectors and works in the institutional relations sector of a large platform

The second main risk was the backdoor's abuse by the authorities themselves (18x), who could use it for surveillance and opponent's political persecution or use the mechanism in a broad and generalized manner. In this regard, a concern with a possible trivialization of confidentiality breaches was highlighted (3x). The interviewee Vitória summarizes it:

> As I said before, breaks have exploratory content. And more than that, before they even have exploratory content, they are generally used as a first investigative resource. [...] Telephone and telematic interceptions... It is written in Law 9296 that they should be used as the last investigation resource when everything else fails and proves to be insufficient. But we see a trivialization, really, and a tendency of [...] the police authorities to request (and the MP too) and the judges to grant with, no criteria nor effective demonstration, that something should have been done before. So it demonstrates an insuperable need to break this type of data. Therefore, I understand that if we also embrace this discourse about encryption , [encryption] will be broken as a rule in a very extreme way.

> Vitória has a legal background and extensive experience advocating at the intersection between criminal proceedings and new technologies

Another frequent argument was that **there are or that there should be alternative means of investigation (19x)**, among which were cited: metadata analysis, search and seizure of devices, recovery of data stored in cloud backups, and police infiltration. Allied to this reasoning is the argument that the necessity and effectiveness of the measure were not sufficiently demonstrated (6x), given the lack of conclusive data regarding the actual number of investigations that are not successful due to encryption. In addition, there is a possibility **that criminals will abandon platforms that weaken encryption (8x)**, which would make the effectiveness of the backdoor null. Interviewees Gilson and Maiara summarize these last two arguments:

> I am also curious to know the number of situations that the police couldn't solve due to encryption. What is the percentage? And I think this is a much-hidden data, which is always blur . Whenever I teach a class, I'm like: man, **we don't know if encryption is a problem today.** Because, like that, maybe everything I say would change if we realized that, I don't know, 95% of crimes in Brazil have not been solved because of encryption because it is getting in the way. Okay, maybe we changed our minds. But we do not know if it is not 0.000009% of crimes, so it is hard to know these two extremes where we are.
>
> Gilson is a jurist who is experienced in the public sector and also in teaching, his academic production focuses on issues involving the internet and fundamental rights

> I have this perception: it is very complicated because as some companies begin to give this access, **we know that criminality migrates.** Just like we're going to change to Signal, they migrate. Large criminal organizations today hire technicians, and they can make their messaging application that will not give access to law enforcement, which will not access. And then you will be making all this movement, decreasing - and I have this perception, which will be decreasing, yes – the security of people's information, ours.
>
> Maiara is a journalist experienced in audiovisual production who works with education for activist groups, with a focus on digital security

From this point of view, exceptional access would be disproportionate insofar as **it affects the rights of all users (26x)** and it impacts their security, privacy, and freedom of expression in the name of solving some crimes. It would mainly hit journalists, activists,

social minorities, and government opponents, who would be more harmed if their private communication is compromised. In this sense, the single possibility of the improper governmental use of backdoors would already affect rights due to the inhibiting effect that the awareness of being watched causes on individuals, which could lead them, for example, to avoid the expression of political differences for fear of State monitoring.

According to this perspective, **backdoors negatively impact trust in the digital ecosystem (13x)**, which is necessary for citizens to feel they can use goods and services in a digitalization context. Following this perspective, **the operational and reputational costs imposed on providers (11x)** could cause negative economic repercussions. The complexity of developing and maintaining such a mechanism would be high to the platforms that use encryption as a competitive advantage associated with greater security, such as WhatsApp, would suffer enormous damage to the brand and could have their business models unfeasible.

4.2. On alternatives to backdoors

Regarding knowledge of alternative methods and techniques capable of providing authorities with access to the content of cryptographically protected data for criminal investigations, 33 of the 43 respondents answered this question. Out of the 33 respondents, **07 stated that they neither remembered nor knew any alternative**. Thus, 26 respondents spoke about alternative methods or techniques.

One of the main alternatives cited for accessing data was the **seizure of specific devices relevant to the case (6x)**. Once the inquiry happened, the authorities could access its contents. If there is content protection by some security feature, such as disk encryption, the agents could proceed in two ways. i) compel, by court order, any user who knows the password or access key to provide it, or ii) use tools that exploit vulnerabilities in the technology to circumvent conventional authentication mechanisms.

This second hypothesis is conceptually close to alternatives frequently cited and grouped under the headings of **government hacking or lawful hacking (19x)**. It uses techniques and tools designed to compromise the security of devices or software used by people under investigation to obtain the necessary data for evidence production. In this universe, specific methods mentioned included:

- **Exhaustive key search (3x):** The use of computational methods to break the security of an encryption system to decrypt text without having authorized access to the decryption key. Examples include brute-force attacks, in which a large number of possible keys or passwords are traversed at high speed, or dictionary attacks, in which a predefined list of possible keys or passwords is scrolled. This solution would be suitable for cases where the encryption used is not computationally secure or when the system does not have protections against running a very high number of attempts.

- **Social engineering (3x):** the police authority would cover up its identity in an interaction with the investigator to induce an act that would compromise the information confidentiality, such as sending account access credentials or inoculating malicious software on devices.

- **Spyware (7x):** the hidden introduction of malicious code into the system to explore unresolved vulnerabilities by its developers would favor the remote collection of data necessary for investigation. Depending on the tool used, it would be possible to activate the device's microphone, camera, and/or geolocation, record typing, and/or sent messages, websites, and applications' use.

The second set of cited solutions involve some degree of cooperation with communication channel providers. In this context, interviewees mentioned the **client-side scanning technique (2x)**, a mechanism in which the device's software or communication channel tests the content of each message sent against a pre-defined database of harmful content, flagged with unique identifiers. If it finds any occurrence of that content in the base, the submission might stop, or authorities might be alerted.

Ghost key or user (2x) solutions follow the same spirit. There is a requirement for the platform to implement a mechanism that introduces a third party into the conversation without the communicating parties being aware. An application could turn the communication between two users into a group by which the ghost would be a part of. This would occur without changing the conversation's interface and both users wouldn't receive any notification. Paula exemplifies how such practice works, besides introducing a discussion point.

> Another method we saw was the ghost key, highly advocated in the UK. It basically changes the interface, but the user doesn't realize the agent with him in a conversation, following his communication. So, instead of three people showing up in the chat, only two of them appear. **But there is a great debate on whether this is still a form of backdoor: you implement a vulnerability that can be a backdoor anyway.**
>
> Paula, legal and interdisciplinary background. Researcher in the field of privacy and surveillance. Experience in civil society and academia.

Another alternative was the **metadata analysis (5x)** in a context where they have no encryption protection. In such a way, it would be possible to apprehend information about communications time, location, frequency, etc. Eduardo, the interviewee, states that this practice also holds privacy concerns.

> [...] I don't advocate for extensive collaboration on metadata because that would also harm privacy. But thinking about it in a different way, according to the principle of minimizing data collection and punctual collaboration, I think it's possible to think of some ways. I see this is an ongoing debate where you preserve what's communicated, what's being the merit, the conversation content, but without providing the judicial authorities with some minimal kind of context information, or using metadata for technical expression. But here, again, I think it's an ongoing, rough debate. There are other messaging applications, Signal, for example, that have encrypted, that is, metadata can be encrypted. So, the object of encryption can be the chat content, but encryption can also cover some metadata. And, then, if you want access to metadata that's encrypted, that's also an encryption vulnerability.
>
> Edward. Legal background, extensive experience in the public sector, works with government relations in a large technology company.

Access to data in backups maintained by third parties was also mentioned (3x). In this regard, they highlight the existence of backups that hold the conversations' content with lower levels of protection or that are stored in a completely decrypted manner, which theoretically have been used already by authorities to circumvent encryption. In the interview, Thais described how the practice occurs:

> And actually, today, with the cloud, we already do that, you know? [...] When we remove [secrecy] from the cloud, it ends up being like this, let's say, like a backdoor, not like, it is a backdoor. Because when we ask for the cloud [secrecy] removal, it's precisely because you don't have access through encryption. But then, not everyone has the cloud, [and] there's that whole thing about you backing it up. There are clouds of certain apps that are more accessible, always have been. So not everyone uses it, and so on, but it turns out that when we have a break like that, it all comes from the person, did you understand?
>
> Thais. Legal education, works in the criminal justice system, focusing on cybercrimes.

In the same vein, **the monitoring of social networks (1x)** appears as a measure that would allow the capture of information relevant to the investigation, such as trips taken, personal relationships, goods, etc.

4.2.1. The risks of alternatives

Along with the question about alternative methods to obtain data for an investigation that does not involve breaking encryption, interviewees answered about the risks attributed to the practices.

A recurring perception was that most of the alternatives mentioned above imply **risks of abuse by a public authority (9x)**, sometimes connected to the possibility of **excessive privacy violation (6x).** This concern was mainly associated with the practices of lawful hacking and device seizure. In this case, investigative access to the device of an investigated person could result in the collection and analysis of data on a series of activities and interactions related to their intimacy and irrelevant to the investigation's content.

Another concern of this nature was the **possible violation of the due process (2x)** because of the possibility of searching for evidence in the digital medium - abundant in information - as an investigative shortcut, even if the other means of producing evidence were not exhausted. In the same perspective, there was a concern about the **vulnerability of third parties not involved in the investigation (x1)** and who may have personal information and communications allocated on the device.

In the context of practices based on some degree of direct cooperation with a platform such as client-scanning and phantom key or user, there was a clear perception that **such initiatives would present similar risks to those of a backdoor (4x)**, in Jessica's words:

> For people's rights, yes, in a more ethical view, I think it's unethical for you to have a phantom user without the person consenting it. I reckon this is ethically wrong. So, I see that this use can also, once again, violate other rights. So how do I know if these ghost users are going to be into groups? Is it just going to be used to do criminal investigations? Or suddenly, it will start trying to figure out what kinds of debates happen to undermine freedom of expression? [I] do not know. I think it all boils down to the same problem of backdoors, these other issues there.
>
> Jessica, engineering background, has extensive experience in internet governance organizations.

In this regard, two points are worth mentioning. First, there was uncertainty about such solutions not truly interfering with encryption, especially in the context of ghost-key solutions, which imply interference in the key management mechanism, even though they may not change the encryption process. Second, there is the perception that even if such approaches preserve encryption in the strict sense, they nullify its purpose: thus, the

risks of abuse, the inhibitory effect, and damage to trust in the digital ecosystem would be equally present. Alvin addresses this problem:

> Obviously, ghosting is the same [as a backdoor] [...]. **A fundamental principle of encryption is that only the people who participate in the conversation access its content**. When there is a third person without your knowledge that this person is there, obviously there is a privacy violation, and it questions what we talked about before.
>
> Alvin, an economist, has extensive experience in the public and private sectors. He works in the public policy sector of a large company.

Finally, there was a general concern about **the possibility of leaking data which public authorities have (2x)**. This is related to the lack of confidence in the information security systems employed by the government, considering the successive cases of massive data leaks of Brazilian citizens. Thus, there is a concern regarding security parameters associated with the protocols for archiving digital material by authorities.

4.3. About the national regulatory environment on encryption

42 interviewees answered questions about the regulatory environment. **05 respondents said they were not aware of the national regulatory environment related to the topic.**

Interviewees expressed the understanding that **encryption has its importance recognized and its use encouraged (9x)** in a recurrently positive view of the Brazilian regulatory environment. This incentive would result from the Internet Bill of Rights and the LGPD. The regulatory decree expressly encourages the encryption's use to guarantee data security (article 13, item IV). The LGPD compels processing agents to adopt security techniques that protect data against incidents (article 6, items VII and VIII, and articles 13, 44, 46, and 49). As argued by Carla:

> What we have in terms of fundamental and general rights is already helpful for us to base and protect the encryption's use. [...] I think that, as a person who researches this subject and follows the jurisprudence and doctrine moving towards such recognition, **I believe that what we already have enables legality and an environment that favors and understands the importance of encryption applications.**
>
> Carla, has a legal background, works as a researcher on the relationship between law and new technologies.

This perception comes with the fact that, **in recent years, there have been significant advances in the public debate on the topic (7x)**, which has been exemplified by references to the Supreme Court ministers' votes about actions regarding WhatsApp blockings in Brazil. The Superior Court of Justice Third Section's decision was also an example, which considered illegal the imposition of a non-compliance fine to a court order for data delivery due to the encryption technical impossibility of intercepting. These decisions would signalize an evolution in the understanding of the judiciary on the subject.

Following this reasoning, some interviewees evaluated that **the Brazilian scenario is more favorable to encryption than several other countries (4x)**. It considers that there is no prohibition or restriction on its use. Besides, the interaction between rules and jurisprudence developments would result in a pretty favorable environment for this technology. Carolina brings this argument into perspective with the international context.

> On the other hand, we do not have a ban, from which many countries are suffering, including democratic countries. [There] are setbacks that even democratic countries are suffering because of this national security agenda. Countries that have a history of terrorism and so on. In that sense, I think we are still well.
>
> Carolina has an interdisciplinary background, extensive experience with advocacy on technology issues, and works with digital security for human rights defenders.

On the other hand, there is a point that **the debate still needs to evolve in content and scope (6x)**. This advance would have two dimensions: first, it would be necessary to advance the authorities' understanding of the subject, the encryption's importance, and the consequences of its weakening, as well as the relationship between its protection and the realization of rights from our legal framework. Second, it would be relevant to broaden the scope of the discussion so that society as a whole, not just a few experts and activists, understands, values, and defends encryption.

In this sense, several interviewees expressed concern about the current scenario, arguing that encryption is threatened (10x). The threats cited include proposals for legislative changes that would weaken the systems' security, such as obligations to implement key-custody or mechanisms for the traceability of forwarded private messages - such as the Draft Bill n. 2630. They also highlighted that the STF has not yet concluded the judgment of actions relevant to the issue. It does not eliminate the possibility of consolidating a future understanding that compromises the encryption's use in the country, despite the initial votes of the rapporteurs of the actions. In her speech, Paula presents these concerns:

> **But the legislature is still worrying because several draft bills seek to establish mechanisms to weaken encryption, either by backdoors or other means.** So, I think this debate could be in a better position in Brazil. On a global level, I think the narrative is very similar in many

> countries, so... countries that consider themselves democratic look down on encryption. This week (if I'm not wrong, it was this week), a commissioner from the UK [United Kingdom] said that encryption is one of the biggest obstacles to fighting pedophilia. **So, these narratives and these positions have been weakening the strength of encryption as, let's say, rights guarantors around the world as well. So, it's pretty worrying [...].**
>
> Paula has a legal and interdisciplinary background and is a researcher in the area of privacy and surveillance. Experience in civil society and academia.

This reasoning is also combined with the reading that **there is little or no regulation regarding encryption in Brazil (12x)**. It interprets our legal framework, not on encryption, but on concepts with a higher degree of abstraction, such as privacy and security. In addition, the country does not have a public active entity for the establishment of technological standards, such as the National Institute of Technology Standards (NIST) in the United States.

> Well, I would say that concerning encryption, **I would say that we have almost nothing on regulation.** We have some guidelines that say the importance of using it, but I think we have very little regulation on encryption. I would say that I am pretty dissatisfied. On a scale of 0 to 10, in which totally dissatisfied would be 0, I'd say I'm there close to 1.
>
> Nicole has a legal and social science background and extensive experience in the private sector in technology companies. She currently works in a law firm.

From the understanding that there is little or no regulation, two distinct discourses emerged.

One of them demands more regulation, asserting that **there must be an explicit legal guarantee of the right to use encryption (9x)**, and suggests this normative innovation as a remedy against the threats to this resource. This guarantee could come in the form of a legal provision or jurisprudence from a higher court that would make the penalty for the use of technology illegal. For this reason, when asked about satisfaction with the regulatory environment on encryption, Marco says he is not satisfied.

> [...] At the same time that we do not have any law prohibiting strong encryption for people, we also do not have any law that approves it and says: 'This is your right.' So, I think this leaves me unsatisfied, that strong encryption should be your right to want to communicate. Your right, your civil right.
>
> Marco is a social scientist and activist and has extensive experience in working with free software diffusion.

But, in addition to this demand for a usage assurance, it has been argued several times that **there should be a legal parameterization of encryption to provide greater security to users (14x)**. Such standardization could consist of an obligation to encrypt information imposed on specific categories of public and private entities, such as public safety authorities, financial institutions, and messaging service providers. Alternatively, a standards-setting entity could be instituted, such as the NIST in the United States.

> [...] I would clarify the question of its inviolability [of encryption]. So in which cases encryption is essential and cannot be the target of court orders for [inaudible] that encryption and in which cases it is good but not essential. **I would even say that encryption was mandatory for some internet applications.** So, I honestly think that there is an essentiality to it, that is, when it is imperative. And another point is when it can be relative.
>
> Nicole has a legal and social science background, extensive experience in the private sector in technology companies, and currently works in a law firm.

On the other hand, the second discourse considers that **it is not evident that regulating encryption is positive (6x).** It questions both the need for it and the potential adverse effects of proposals of such nature. It argues that encryption development and use are already permitted insofar as it is not subject to legal restriction or prohibition. Furthermore, it notes that encryption is both a technique and science. The regulations on the field's development can unduly affect the intellectual autonomy and the scientific progress of information security researchers. This concern appears in Cristiano's speech, for example:

> We don't have it, so... I don't know if I want a regulatory environment. I do not know now. So, it depends on what this question means, because I don't want anyone regulating how I can or cannot use encryption, someone to tell me, as I had years ago. [...] i**f we're talking about this kind of thing, which will say the size of the key I can use, the algorithms I can or cannot use, in terms of limiting the strength of the algorithms I can use or force myself to use some backdoor or master key... forget it. I'm pretty glad I don't have anything.**
>
> Cristiano, a computer scientist with extensive experience in the field of information security in academia and the private sector.

The main foundation of the discourse against regulatory proposals that expressly deal with encryption is the perception that **technological neutrality is positive and must be preserved (4x)**. Thus, the fact that the present instruments do not expressly address encryption would be a virtue, not a shortcoming. Since it is not possible to predict technological developments in the coming decades, any regulation that focuses on specific technologies has the potential for accelerated obsolescence, even those that might presently appear positive, such as establishing a duty to use encryption.

> **The problem with regulating more is that, in computing as a whole, it changes a lot. It changes daily.** If you meet a minimum standard, you can be comfortable, right, but it's been a year, two, sometimes that standard is out of date, and you will present a certificate that you comply with, and may not even get punishment, but the system will be hacked the same way, right.
>
> Sergio has training in Computer Science. He is a federal servant and researcher.

4.4. About WhatsApp blockings and their relationship with the Internet Bill of Rights

41 out of 43 respondents answered the question about the assessment of WhatsApp blockings. The question of whether or not the Internet Bill of Rights authorizes such measures was answered by 23 of them.

A frequent perception among the interviewees was that t**he judicial blocking of WhatsApp in Brazil was illegitimate (17x)**.

One of the reasons for such an assessment was that **the blockings were based on inadequate interpretations of the Internet Bill of Rights (11x)**, especially its chapter III, section II, which deals with the protection of personal data and private communications records. From this point of view, this section would contain **sanctions only to providers that violate the users' privacy and data protection guarantees (11x)**. At the time of the blocking, this requirement would not be present, as failure to comply with a court order to share data with the authorities for the purposes of criminal prosecution would not correspond to a violation of such rights.

> [It was] totally illegitimate because, first, it was a case of total misinterpretation by the MCI. There was a provision in articles 11 and 12 that brought **sanctions that should apply in the context where the data controller - although the MCI does not use the term data controller, that is the context - [...] is operating, and it does not ensure the principles of privacy.** And then, for misuse, it could be sanctioned.
>
> Ian has legal and computer background and extensive experience in the public sector.

On the contrary, when this non-compliance resulted from the operational inability to produce the information requested due to encryption, it would result precisely from the duty's fulfillment to guarantee data security. Additionally, in this case, the sanction to the provider would be illegitimate because **such a technical obstacle would make the original order fulfillment impossible (6x)**. Thus, the order compliance would be an obligation

similar to produce a diabolical prove. In addition, it would represent a penalty for the provider itself.

The blockings' material effectiveness was also negatively evaluated by respondents, who considered them **ineffective due to the possibility of bypassing them through virtual private networks (VPNs)**[53] **(4x)**.

From this perspective, there were criticisms on **a lack of knowledge from the judicial authorities about the technology's functioning (8x).** Because of this lack of encryption knowledge, decision-makers would expect quick access to the private communications' contents as **a shortcut to criminal investigations (2x)**, as well as frustration when this expectation is not fulfilled.

Regardless of the Internet Bill of Rights' interpretation, however, **the main reason for the negative assessment of the blockings was that the damages resulting from the measure were disproportionate (22x).** The rights of the application's tens of millions of users were affected, **causing them even economic damage (6x)**. This disproportionality would make the blockings illegitimate regardless of the content of the Internet Bill of Rights. It would directly affront constitutional precepts such as freedom of expression and free enterprise.

In the same field, **there were doubts on the competence of the Brazilian Judiciary to unilaterally determine the blockings (2x)** because the measure reached users in other Latin American countries, representing an undue extrapolation of the Brazilian jurisdiction.

> [...] [...] And also from the social point of view. It is a very drastic decision because Whatsapp is one of the most used communication means by Brazilians. **It has negative consequences both for people who are using these applications, for work, to talk to their families and for economic reasons because there are people who depend on it** to sell lunchboxes, sell... I don't know, things that they have the contacts there, and they count on it to do daily activities. So, this level of blocking is so drastic that it has very adverse effects on people as a whole. I think it is a very wrong decision.
>
> Laura has a legal background. Experience with research and activism involving technology and society in the third sector.

In addition to the debate on episodes' merits, the respondents also reflected on their concrete causes, generally attributing them to **a political dispute between Facebook and the Brazilian criminal justice system institutions (10x)**. They recall that the first data sharing order (whose non-compliance resulted in the blocking) preceded the end-

53 VPN is a technology resource that establishes a private network connection created over a public network infrastructure. The VPN allows the user to encrypt their traffic and hide their identity and their online location.

to-end encryption implementation and the non-compliance attribution to the company's negligence towards national authorities. Such disregard would have caused a reaction to reaffirm national sovereignty through the determination of blocking, to compel companies to comply with the national scenario.

> So, these blockings ended up happening due to a company's disrespect. It establishes itself in Brazil, has an office in Brazil - which is Facebook's marketing office - makes money in the national territory from the data collected from people in the national ground, but that **didn't bother to have a legal department to deal with Brazilian justice system.**
>
> Natalia, with a legal background, works in the criminal justice system with a focus on cybercrimes.

> If encryption is legal in the country and its use is not prohibited, we must accept the technical inability to deliver this type of content. [That] the Brazilian justice staged on that occasion was an arm wrestling with companies that did not have good results. It had good results neither for the specific case nor for the broader regulatory issue. **Since encryption is legal, I don't think companies are, in this case, wrong or resisting a court order. They are preserving the integrity of a system that relies on the use of encryption.**
>
> Tatiana has a legal background, extensive work in civil society defending human rights, and is a researcher in privacy and security.

Less frequently, some respondents considered **that the blockings were legitimate (6x)**.

The first thesis in this regard stated that **article 11 substantiates the blocking by conditioning the processing of data to comply with Brazilian legislation (3x).** According to this reasoning, non-compliance with a legitimate court order for data sharing implies non-compliance with Brazilian Law, once the order in question is based on norms that make up the national legal framework.

According to these respondents, as the company could not claim that the encryption represented a technical impediment to complying with the order, the first blocking would be particularly relevant. Thus, the option of not complying with the order would not only represent a political challenge to the authority of the national judiciary but also an effective violation of the Brazilian legal order. Therefore, it would constitute an infringement of the Internet Bill of Rights article 11. It would attract the application of the sanctions provided for in its article 12, including the suspension and prohibition of activities involving the acts provided for in article 11.

> I understand that yes, it is authorized indeed because when it says: [...] 'in any collection, storage and treatment or communications operation, in which at least one of these acts takes place in national territory, it must comply with the Brazilian legislation, and the rights to privacy, personal data protection and the confidentiality of private communications and records'. So, we understand that **in article 11, if all these acts - it is very clear here -, they must comply with Brazilian legislation, any court order that determines the removal of the right to privacy or protection... to remove this right to privacy or to remove communications' secrecy, Brazilian legislation must be complied with**. When it says that, it already means that the sanctions for non-compliance with the court order [are applicable]. This [non-compliance with the order] is already a breach of Brazilian law. That's what we understand.
>
> Natália has a legal background and works in the criminal justice system, with a focus on cybercrimes.

Alternatively, another thesis understood that the blocks could be determined independently of the Internet Bill of Rights due to the judge's general power of caution (3x). As a guarantee of procedural effectiveness, this figure implies that the magistrate has the duty-power to grant atypical precautionary measures - not provided for in the legal norm - when the options provided are not adequate nor sufficient to the specific case. From this point of view, the matter under discussion would trigger such prerogative mainly because there was the determination of previous measures with which the company refused to comply, even being significant crimes - drug trafficking.

> I understand that the Internet Bill of Rights has sanctions there, that it does not inform who will apply it, and the Judiciary has used this article to justify the blocking. **But I also see that the court could determine blockings without [the] Internet Bill of Rights because the judge has a general caution power. It invokes the necessary measures for evidence or the court decision's compliance without any need for the Internet Bill of Rights.** So much so that there was a discussion in the STF [...] and no need to declare those provisions unconstitutional. With or without them, the Judiciary could have taken action. And we're going to discuss whether this is legitimate or not in light of the constitution, it's another discussion. But in terms of the normative framework itself, I think it is no different if the Internet Bill of Rights says it or not. I think the actual discussion about constitutional parameters, the control of judicial decisions, and not specifically about the wording of the civil framework.
>
> Silvana has an interdisciplinary background in the legal area and in the field of communication and extensive experience in the public sector.

5. Analysis and discussion

This section discusses the content of some of the statements extracted from the interviews. Each of its subsections focuses on one of the themes reported in the previous chapter. It does not discuss the regulatory environment perceptions, as this environment has already been the object of sections 2.4.2 and 2.4.3 of this study.

5.1. About Backdoors

Our interviewees justified the support for backdoors mechanisms with legal-political reasoning, in which the premise is grounded on the priority of public security over other rights possibly threatened by the measure. They reckon that if guaranteeing public safety requires access to private communications (and there are cases estimated by the law in which such access is allowed), then it is paramount that the law is complied. In this logic, the risks resulting from access are seen as an unwanted but necessary burden, a kind of 'lesser evil' if the alternative is non-compliance with the law and impeding investigations. In any case, the risks of abuse could be prevented by institutional guarantees, such as judicial control and reserving this access to exceptional situations: grave crimes, after other means exhaustion. Finally, it would be necessary to trust the institutions by principle. The legal controversy evoked by this point of view is not limited to the duty to intercept but implies a debate on the existence or not of an obligation to produce a technological architecture that makes the interception feasible. As Jacqueline Abreu observes[54], reasonings such as this 'seem to want to extract from the very legal provision in the Brazilian law on breach of confidentiality procedures the duty that the ability to breach confidentiality always exists.' For the author, although the existence of this duty is evident in the telecommunications sector due to several resolutions of the National Telecommunications Agency that expressly provide for it[55], it is not possible to conclude that it extends to technology companies and internet application providers since such companies are not public service concessionaires and, therefore, remain outside the scope of entities subject to these resolutions.

The Internet Bill of Rights, in turn, restricts compelling companies to guard metadata related to IP, date, and time of access. Therefore, the legal duty to have the ability to break communications' confidentiality 'is not evident; lacks reasoning - and it may well be that the conclusion is that it does not exist.'[56] The question posed, therefore, is whether or not such a duty should exist. It evokes considerations about its benefits and harms. Within

54 ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 24-42. p. 32 Free translation.

55 The most relevant rules in this regard would be Resolutions Number 73/1998 (Regulation of Telecommunications Services), Number 426/2005 (Regulation of Switched Fixed Telephone Service), Number 477/2007 (Regulation of Personal Mobile Service), and Number 614/2013 (Regulation of the Multimedia Communication Service)

56 ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 24-42. p. 34

the evaluative rationality that underpins the backdoor's defense in the empirical material, the calculation is evident. The obstacles to criminal prosecution significantly outweigh the risks and damages that arise from weakening encryption, mainly because such a point of view is grounded on a principled trust in the due capacity of institutions to curb abuses of power.

One must note that such trust is fundamentally based on institutional controls over intentional abuses by public authority. However, it does not include the risk of usurping the security hole by malicious third parties such as cybercriminals or foreign governments.

The stance contrary to backdoors offers a divergent perspective, which has two axes: the emphasis on the damage resulting from the measure in the technical, legal-political, and economic field and the questioning of its need and effectiveness. The first axis asserts that, once a vulnerability is introduced, it will be subject to misuse by criminals and malicious rulers. It would cause a series of undesirable repercussions, like security and trust reductions in the digital environment, the violation of users' rights, and the imposition of substantial economic burdens on providers.

The current scientific consensus in information security supports the concerns related to it. It attests that it is impossible to ensure that only the lawful and legitimate will explore a vulnerability. Furthermore, the scalability requirements associated with the key-custody systems impose the need to revert to best security practices - such as forward secrecy, an arrangement in which decryption keys are replaced immediately after each use, to reduce the damage of its eventual compromise[57]. In this sense, the security reduction resulting from the vulnerability would be graver because the correlated reversal of these good practices would imply an increase in the gains of an eventual attacker, which would increase the incentives for the flaw exploitation to materialize.

Legal and political concerns, in turn, are in line with the understanding of the rapporteurs' judges of the actions related to WhatsApp blocking in the Supreme Court, as well as the growing international recognition that encryption is necessary to protect the rights to privacy and freedom of expression[58]. But beyond the abstract reflection, the interviewees' notes come from the context of the Brazilian legal-political scenario, including a skepticism regarding the capacity of institutions to curb abuses and a perception that there would be a trivialization of confidentiality breaches in the Brazilian criminal justice system.

As for institutional skepticism, the examination of the Brazilian political environment offers elements to consider its relevance. In a joint report[59] about the Brazilian political

57 ABELSON, Hal *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. **Journal of Cybersecurity**, v. 1, n. 1, p. 69-79, 2015. p.69.

58 HOBOKEN, J. V.; SCHULZ, W. **Human rights and encryption**. Paris: UNESCO, 2016.

59 ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA; CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO (LAUT). Retrospectiva - Tecnoautoritarismo 2020. **LAUT,** 2021. Available in: https://laut.org.br/wp-content/uploads/2021/01/RETROSPECTIVA-TECNOAUTORITARISMO-2020.pdf. Access on: 04/08/2021.

and technological environment in 2020, the Center for the Analysis of Freedom and Authoritarianism (LAUT) and the Data Privacy Brazil Research Association (DPBR) identifies thirteen state initiatives that favor information and communication technologies' uses to unduly broaden population surveillance and control. They are risks to democratic freedom. Among the examined measures were authorizations for the registration of data confidentiality breaches without a court order, the construction of dossiers on individuals called 'anti-fascists,' and the monitoring and classification of journalists, parliamentarians, and opinion makers according to their ideological position. Other surveys also support such considerations[6061]. They show a progressive trend towards criminalization and restriction of the right to protest in the country since 2013.

As for the specific question about the existence of a judicial tendency to trivialize confidentiality breaches, its measurement encounters methodological obstacles. CNJ Resolution No. 59/2008 determines that all criminal courts in the country should provide regular reports on requests for interception of communications and decisions to breach confidentiality. Part of this data is in an aggregated format through the National Telephone Interception Control System (SNCI)[62]. However, the system only displays the number of decisions by a court, court segment, and decision category. Then it is not even possible to measure the percentage of requests granted and rejected. Even if it were, that would not resolve the issue, which has a double dimension. From a descriptive point of view, it would be necessary to map which empirical conditions were sufficient to meet the requirements set out in Law 9296. From a normative point of view, it would be relevant to assess whether such interpretations are reasonable concerning procedural guarantees. Jurisprudential content analyzes may explore this gap in the debate.

It is important to note, however, that there was an extreme percentage increase in the number of decisions to breach telematic confidentiality in the last five years: throughout 2015, 1,943 decisions of this nature were produced, against 6,898 in the first six months of 2020 alone, representing a percentage increase of 255%. This growth would already be noticeable, but the absence of data for the second half of 2020 suggests it is significantly higher. Also in this regard, researchers from InternetLab[63] note that the numbers presented in the system may not reveal the actual magnitude of the interceptions' volume. It is because of a historical discrepancy between the system information and data from the private sector. In 2016, the company Telefónica (which operated as Vivo in Brazil) transparency report stated it received 326,811 interceptions requests in Brazil in 2015.

60 ALMEIDA, Frederico de. MONTEIRO, Filipe Jordão; SMIDERLE, Afonso.a criminalização dos protestos do movimento passe livre em são paulo (2013-2015). **Revista Brasileira de Ciências Sociais** [online]. v. 35, n. 102, 2020.

61 ARTIGO 19. **As restrições ao direito de protesto no Brasil**. 5 anos de junho de 2013: Como os três poderes intensificaram sua articulação e sofisticaram os mecanismos de restrição ao direito de protesto progressivamente. Artigo 19, 2018. Available in: https://artigo19.org/5anosde2013/. Access on: 04/08/2021.

62 BRASIL. Conselho Nacional de Justiça (CNJ). Sistema Nacional de Controle de Interceptações Telefônicas. **CNJ**, Brasília, 2021. Available in: https://www.cnj.jus.br/sistemas/sistema-nacional-de-controle-de-interceptacoes-telefonicas/. Access on: 04/08/2021.

63 ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. p. 44-45. Free translation.

The number exceeds both the number of demands sent to companies (95,481) and the sum of telephones and VOIP intercepted that year (294,217) according to SNCI data.

According to the researchers:

> All of this points out that the numbers related to interceptions in Brazil deserve a study of their own. If they turn out to be high, they may suggest, on the one hand, that the theoretical protection sought by the need for a court order and the provision of stricter requirements for carrying out this procedure in the Law of Interceptions does not reflect in practice. On the other hand, it can also point to structural deficiencies in the investigative capacities of the judicial police, making it heavily dependent on this aggressive means of evidentiary instruction. There are not few demonstrations that public security authorities use interception and confidentiality breach measures as a *prima ratio*.

Still, on the Brazilian interceptions culture, the InternetLab recalls that the Human Rights Inter-American Court has condemned Brazil for illegally conducting telephone interceptions on the communications of rural workers of the Landless Movement. The irregularity resulted from the interceptions' authorization by the Military Police - which was not competent to do so - without notification to the Public Ministry and outside the scope of an ongoing criminal investigation.[64] It is relevant to note that the authorities responsible for the offense were not held liable for it.

Concerns about the negative impacts on trust and the digital economy, finally, also demand empirical testing. In this regard, it is worth mentioning the research conducted by researchers at Law & Economics Consulting Associates and commissioned by the Internet Society on the subject[65]. The work investigated the potential costs and benefits of the Telecommunications and Other Legislation (Assistance and Access) Act (TOLA) Amendment passed in Australia in 2018. This standard compels information technology providers to assist authorities in accessing content from encrypted data, including through changes in the architecture of their systems. The survey linked in-depth interviews with the 09 biggest multinational providers operating in the country to an anonymous questionnaire application to another 79 providers.

The study concluded that TOLA would have several potential negative impacts on providers and their customers. In this regard, the increase in uncertainty in the business environment, damage to the brand image of providers vulnerable to the weakening of their services,

64 Conferir MASI, Carlos Velho. O caso Escher e outros v. Brasil e o sigilo das comunicações telefônicas. **Revista dos Tribunais**, v. 932, Junho de 2013, pp. 309-352

65 BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. The Economic Impact of Laws that Weaken Encryption **Law & Economics Consulting Associates** (LECA). 2021. Available in: https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/ .Access on: 04/08/2021.

and a reduction in trust in the digital environment stand out. This last aspect may imply a decrease in aggregate demand by encouraging companies to assume higher costs to minimize damage. More studies are needed to specify the extent of these damages and verify whether other legislation with similar provisions has similar effects in other jurisdictions.

The second axis of the stance against backdoors, in turn, consists in questioning the alleged benefits of this measure: its necessity and its effectiveness would lack conclusive and empirical demonstration. And it would likely result in the migration of criminals to other platforms. Combined with the previous axis, this stance understands backdoors as a disproportionately harmful and potentially ineffective measure. The first claim bases on the absence of data or studies that show that implementing strong encryption on platforms and devices affects the rates of successful criminal investigations. The second, in turn, requires further studies, which should investigate the effects of implementing backdoors mechanisms on illicit activity on platforms.

5.2. About backdoor alternatives

There were two main sets of potential solutions as alternative methods or techniques to provide the authorities access to information without compromising encryption. One is based on the information security breach at one end by the State authority, whereas the other is based on the cooperation with technology providers in which information is stored or communicated.

In the first set, there is the initial possibility of arresting and unlocking the relevant devices. If, on the one hand, such a solution offers the benefit of not interfering in the system encryption, it has significant repercussions on the citizens' rights, especially concerning the protection of personal data stored on devices and conditions of legitimate confidentiality removal of static data. The respondents noted such impacts and expressed concern about the possibility of an excessive intimacy breach as an individual's mobile devices presumably contain information that goes far beyond what is relevant to the investigations.

It raises, then, the question of the judicial compulsion legitimacy to the handing over of passwords. In this regard, the Sixth Chamber of the STJ signed the understanding that the judicial call to unlock the device is legitimate. However, there is no obligation for the defendant to inform the password due to the constitutional prohibition of self-incrimination[66]. Regarding the vote, the judge rapporteur, Minister Nefi Cordeiro, considered that 'the court order for the delivery of the passwords of the seized electronic devices is valid, but the defendant is not required to provide these passwords, and should not suffer sanctions.'

66 BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 580.664 - RJ**. Rel. Ministro Nefi Cordeiro. Brasília, 20 out. 2020. Available in:https://stj.jusbrasil.com.br/jurisprudencia/1206242995/habeas-corpus-hc-580664-rj-2020-0111177-4/inteiro-teor-1206243005 . Access on: 05 ago. 2021

Following this precedent, therefore, access to the contents of the seized device would require the use of methods and tools aimed at offensive security. It raises the debate over whether to use lawful or government hacking to compromise one end of the encrypted channel. As evidenced by the analysis of the interviews, although these terms generically designate the use of resources and methods aimed at exploiting vulnerabilities, the universe of resources and tools can vary a lot, since the concept encompasses approaches as different as social engineering and the use of spyware to gain targeted access.

Since they do not enjoy an express provision in Brazilian criminal procedural law, government hacking practices have been discussed primarily in the Legislative, which established a working group to prepare a draft bill of the Code of Criminal Procedure's reform. In the substitute text from the WG, up to the completion date of this paper[67], the matter is considered in two hypotheses for obtaining evidence: the 'remote collection, hidden or not, of data at rest accessed remotely' and the 'collection by forced access of computer systems or data networks.'

The generic content of these propositions echoes concerns described in the encryption and anonymity follow-up report by the United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in 2018. The document warns of a tendency of States to standardize the hacking practices through legal authorizations written in 'vague and ambiguous language, providing the authorities open-ended powers with minimal external oversight[68].' To address such risks, the rapporteur recommends that government hacking be authorized only in exceptional circumstances, subject to legality, necessity, proportionality, and legitimate purpose requirements, whose existence must be attested case by case by an independent and impartial judicial body[69].

Similarly, a report on this matter produced by the reference center on digital rights *Access Now*, in 2016[70], recommends a preventive ban on government hacking because of its human rights risks. The document advises that potential authorizations comply with the parameters of user notification, transparency, public oversight, systems integrity, international cooperation, effective remedy, and safeguards against illegitimate access, in addition to those proposed by the UN rapporteur.

67 BRASIL. Câmara dos Deputados. **Parecer do Relator, Dep. João Campos (REPUBLIC-GO) da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 8045, de 2010, do Senado Federal, que trata do "Código de Processo Penal" (revoga o Decreto-Lei nº 3.689, de 1941. Altera os Decretos-Lei nº 2.848, de 1940; 1.002, de 1969; as Leis nº 4.898, de 1965, 7.210, de 1984; 8.038, de 1990; 9.099, de 1995; 9.279, de 1996; 9.609, de 1998; 11.340, de 2006; 11.343, de 2006), e apensados ao Projeto de Lei nº 8.045, de 2010**. Portal da Câmara dos Deputados. Brasília, 26 abr. 2021. Available in: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/gt-anteprojeto-do-novo-codigo-de-processo-penal/documentos/outros-documentos/substitutivo-relator-joao-campos. Access on: 05 ago. 2021. p. 481.

68 UNITED NATIONS. **Encryption and Anonymity follow-up report.** 2018. Available in:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Access on: 05 ago. 2021. p. 8.

69 UNITED NATIONS. **Encryption and Anonymity follow-up report.** 2018. Available in:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Access on: 05 ago. 2021. p. 18.

70 STEPANOVICH, Amie et al. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Available in:https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf. Access on: 05 ago. 2021.

The second main set of alternatives to encryption differs from the first, as it relies on collaborative practices with the platform. In this context, the main possibilities raised were the user methods or phantom key, and client-side scanning systems.

The debate over the phantom-key or user methods has recently gained traction as a result of an article published by two technical directors at Government Communications Headquarters, the UK's top authority[71]. The authors argue that the veiled addition of a third party to the investigated conversations - as a mechanism for accessing information necessary for investigations - would not interfere with encryption, which would make it a viable way out for the debate on Going Dark.

The proposal had negative repercussions in the information security community, resulting in an open letter[72], signed by 23 civil society organizations, 07 technology, and commerce companies, and 17 globally recognized experts in digital security and its governance. In the letter, the signatories claim that the phantom key proposal 'undermine the authentication process that enables users to verify that they are communicating with the right people, introduce potential unintentional vulnerabilities, and increase risks that communications systems could be abused or misused.' The Internet Society reiterated the position in a fact sheet about the proposal[73]. Similarly, an opinion piece written by computer scientist and jurist Ross Schulman questioned the fundamental premise that such a method would not interfere with encryption. In his words:

> In their proposal, Levy and Crispin assert that the ghost keys proposal would not "touch" encryption. That claim is simply not true by any normal definition of "encryption." While the proposed method may not always involve changing the fundamental encryption algorithms [...], it would require "touching" and modifying the encryption keys. The processes of key distribution and authentication and the keys themselves are integral pieces of the entire encryption system. Weakening those has a similar impact on security as undermining the algorithm itself.[74]

The author notes that implementing these services would require massive scale changes to systems to produce a key addition mechanism to get active on-demand on specific devices. The resulting impacts would be similar to those of a key escrow system. The increasing system's complexification and a related reduction in its security, the possibility

71 LEVY, Ian. ROBINSON, Crispin. Principles for a More Informed Exceptional Access Debate. **Lawfare - Hard National Security Choices**, 29 nov. 2018. Available in: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate . Access on 05 ago. 2021.

72 BRADFORD, Sharon. THOMPSON, Andi Wilson. Open Letter to GCHQ on the Threats Posed by the Ghost Proposal. **Lawfare - Hard National Security Choices**, 30 mai. 2019. Available in: https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal. Access on: 05 ago. 2021.

73 INTERNET SOCIETY. Fact Sheet: Ghost Proposals. **Internet Society**, 24 mar. 2020. Available in: https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/. Access on: 06 ago. 2021.

74 SCHULMAN, Ross. Why the Ghost Keys 'Solution' to Encryption is No Solution. **Just Security**, 18 jul. 2019. Available in: https://www.justsecurity.org/64968/why-the-ghost-keys-solution-to-encryption-is-no-solution/. Access on: 05 ago. 2021.

of exploitation by malicious third parties, and reduced trust in the platform. For these reasons, it concluded that the proposals to implement a user or phantom key constitute another backdoor mechanism and involve similar technical, social, legal, political, and economic risks and problems.

Another alternative based on cooperation with device and channel providers is the client-scanning system, sometimes called endpoint filtering. The proposal has also received criticism from the information security community in recent years. In a published fact sheet on the subject, the Internet Society[75] noted that the proposal would increase the system's complexity by increasing the attack surface exploitable by malicious attackers. They could monitor and interfere with users' communications by manipulating the harmful content database. Furthermore, it warned of possible abusive uses of this capacity, such as political censorship of legitimate content communication.

In a public statement on the topic, the Electronic Frontier Foundation warned of other problems related to the proposal:[76] the database would probably get stored on the server, which would access each image's identifiers sent by the user. Once one implements such a system, it could incorporate similar features to provide access to textual content to combat misinformation. The potential for using this type of mechanism to access communications content would imply a continued incentive to the undue expansion of the database. Ultimately, the entire dictionary could be incorporated into this base, effectively enabling the total decryption of messages and nullifying the purpose of encryption.

Concerning metadata, the debate over its access has been a point of lesser legal controversy. The Internet Bill of Rights data custody regime defines the information that internet service providers must store to the competent authorities' access upon court order. Following the logic of data processing minimization and necessity principle from the LGPD, the collection, and storage of personal data, including metadata about accounts and communications, must be limited to the minimum necessary to achieve the processing objectives.

Furthermore, experts have warned of risks associated with the construction of social graphs designed from metadata, such as their improper monetization by platforms and their use for mapping social networks of political dissidents, journalists, and activists. In the previously described techno-authoritarian context, such concerns acquire greater gravity, which reinforces the need to minimize the collection and storage of metadata and the consistency of the parameters determined by the Internet Bill of Rights with such a preventive perspective.

75 INTERNET SOCIETY. Fact Sheet: Client-Side Scanning. **Internet Society**, 24 mar. 2020. Available in: https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/. Access on: 06 ago. 2021.

76 PORTNOY, Erica. Why Adding Client-Side Scanning Breaks End-To-End Encryption. **Electronic Frontier Foundation**, 1 nov. 2019. Available in: https://www.eff.org/pt-br/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption. Access on: 06 ago. 2021.

On the other hand, given the pressure to moderate content in encrypted environments, some scholars have considered metadata analysis as a less invasive alternative than others. In a recent report on the topic[77], the Center for Democracy and Technology considered this method able to preserve the user's privacy and encryption, as long as the analysis takes place exclusively on the user's device and does not imply access to decrypted content.

In addition to these notes on specific proposals, examining the respondents' statements about alleged alternatives to backdoors shows socio-technical rationality. They recognize the encryption systems' technical structures as inseparable from the political connotations they have acquired over the years concerning rights defense, such as privacy and freedom of expression. For this reason, alleged alternatives - such as client scanning and metadata analysis - face varying degrees of resistance even when their implementation does not necessarily imply a direct interference with the encryption algorithm or key management.

5.3. About WhatsApp blockings in Brazil and its relationship with the Internet Bill of Rights

The interviewees' understanding of WhatsApp blocking and its relationship with the Internet Bill of Rights evidenced different interpretations of the law. The legal controversy specifically concerns the law chapter III, section II. Such provisions, in short, provide for the regime applicable to operations of collection, storage, custody, and processing of records, personal data, or communications carried out in the national territory. They also involve such activities taken by a legal entity headquartered abroad, provided that it offers services to the Brazilian public and has at least one member of its economic group headquartered in the national territory.

In this regard, we must note that article 10 establishes that the information custody and availability must preserve the image, private life, honor, and intimacy of the parties involved. Article 11, in turn, conditions such activities to respect 'Brazilian law and the privacy rights, personal data protection and the private communications and records' secrecy.'[78] Article 12, finally, establishes sanctions for non-compliance with articles 10 and 11. Furthermore, items III and IV determine the temporary suspension or prohibition of the activities covered in article 11.

Regarding the interpretation of these provisions, two main theses raise. The first one

77 KAMARA et al. **Outside Looking In**: Approaches to Content Moderation in End-to-End Encrypted Systems. Center for Democracy and Technology Research, Washington, ago. 2021. Available in: https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/. Access on: 26 ago. 2021.

78 BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. DF: Presidência da República, 2014. Available in: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Access on: 05 ago. 2021.

considers the article 12 sanctions inapplicable to cases of non-compliance with court orders for data delivery because it does not imply a violation of privacy and data protection. On the contrary, when resulting from encryption implementation, such non-compliance corresponds to the success in protecting such rights. This interpretation bases on the articles' express references to these rights defense. It considers as well the more general commitment of the bill to the privacy defense. It is a reading akin to rationality primarily committed to privacy and refractory to backdoors and measures seen as invasive to privacy in general.

On the other hand, the second thesis applies such sanctions to the blocking cases. It understands that non-compliance with the court order implies the article 11 violation because the wording of article 11 would establish respect for Brazilian legislation as an autonomous duty from the privacy and data protection duty. Thus, companies that did not comply with a properly grounded court order issued by a competent authority would violate national law. Consequently, they are subject to suspension of their services under the terms of article 12. This position connects to the idea of crypto wars primarily as a political conflict between states and global technology companies and commits to the reaffirmation of state authority in the face of the threat posed by such companies to it. This thesis was one of the third attempts' reasoning at WhatsApp blocking (the second blocking carried out) in Brazil.

In assessing the merits of these interpretations, it is worth reiterating that, as previously argued, the existence of a duty of aptitude to breach confidentiality applicable to technology companies and internet application providers in Brazilian law is not evident. Thus, a question arises on the lawfulness of fixing sanctions to the economic agent that fails to comply with a court order for data delivery because, acting lawfully, it has produced an informational architecture that makes it incapable of breaching confidentiality. In this regard, the STJ Fifth Chamber confirmed the decision of Minister Ribeiro Dantas in Special Appeal Number 1871695 - RO (2020/0095443-3). It ruled out this possibility by understanding that no one should be obliged to do the impossible and that the encryption benefits far outweighs its possible burden on society[79].

In this regard, it is also relevant to highlight the understanding of Minister Rosa Weber in her vote at the Declaratory Action of Unconstitutionality (ADI) Number 5527. According to her, the Internet Bill of Rights' sanctions specifically regards non-compliance with the duty to comply with Brazilian legislation in activities related to the processing of records, personal data, and communications. According to Weber, the provisions - in particular, the legal sanctions -, do not apply in the context of non-compliance with court orders.

Then, the sanctions' inapplicability is supported both by the rapporteur judge's

79 BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas.** 30/12/2020. Available in < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx >, Access on 03 ago 2021.

understanding, despite the case at STF pending conclusion, and the STJ jurisprudence.

Another interviewees' segment pointed out that, regardless of whether or not there is legal permission in the Internet Bill of Rights to blocking orders, these judicial determinations would result from the so-called judge's general power of caution. It is a mechanism initially provided for in article 798 of the 1973 Code of Civil Procedure, through which the judge would have the discretion to apply preventive measures other than those previously stipulated by the law to ensure the process's feasible outcome.

This instrument was, to some extent, expanded in the 2015 Code of Civil Procedure, which failed to list the legally prescribed methods of preventive measures. Alternatively, article 301 sets out the general permission according to which 'injunctive relief of a preventive nature may use arrest, sequester, assets listing, registration of protest against the sale of assets and any other suitable measure to ensure the right.' The civil procedure rule in the current code, in this sense, is entirely centered on the judge's general power of caution to determine preventive measures and advance protections during the process.

In the scope of Criminal Procedural Law, the judge's general power of caution bases on a jurisprudential understanding that brings the subsidiary applicability of the Code of Civil Procedure - and, consequently, the statement of article 301 – for criminal proceedings. It is an interpretation arising from article 3 of the Criminal Procedure Code, which authorizes 'extensive interpretation and analogical interpretation, as well as the supplement to the general principles of law.' This allows legal institutes outside the criminal process to fill any legal gaps.

The legal doctrine regarding the applicability of the judge's general power of caution in criminal proceedings diverges. However, the majority jurisprudence in the country recognizes a necessary prerogative to the activity of the law enforcer - especially concerning non-personal preventive measures, that is, different from those applied to the defendant in the course of the criminal process. In this sense, it stems from the judge's implicit powers theory in favor of the justice enforcement. It is a prerogative recurrently used, for example, to determine who are members of the procedural relationship other than the defendant (to which only the precautionary measures expressly provided for by law are applicable) and who failed to comply with court orders considered necessary for the investigation process.

In the imposition of atypical measures through the judge's power of caution, however, observing the precepts of the measure proportionality and necessity is essential for the decision. The precepts' examination at WhatsApp blockings involves a topic widely discussed by the interviewees: they reckon that the blockings were unjustified due to their disproportionality, more than because of the Internet Bill of Rights.

In this sense, the impact of blocking orders is central. For several interviewees, the illegitimacy of the blockings results from their damage rather than from the Internet Bill of

Rights' wording. As we explained in the section of this paper that described the blockings, all the suspension orders evoked the proportionality principle. Furthermore, two of them understood that there would be less burdensome means of guaranteeing the enforcement of the law. In this sense, although the STF's position pends, the four decisions to suspend the blocking examination suggest that the requirements of necessity (there would be less burdensome means available) and proportionality (the resulting damage was diffuse and excessive) were not present.

Thus, the analysis of WhatsApp blocks and their relationship with the Internet Bill of Rights leads to three conclusions. i) The rapporteur Minister Rosa Weber supports the restrictive thesis of the sanctions provided for in article 12 of the Internet Bill of Rights to privacy and data protection violation, pending the conclusion of the judgment, so that article 11 could not justify the blockings; ii) The judge's general power of caution could also not adequately substantiate the blocking, given the absence of proportionality and necessity requirements, as evidenced by the blocking suspension orders; iii) Any economic sanctions could not be applied either, according to the understanding signed by the STJ, due to the factual impossibility of delivering the data together with the weighing up of the costs and benefits of encryption, which legitimizes its maintenance in the system.

6. Conclusion

The dialogue, which covered more than 40 interviewed professionals, highlighted the multiplicity of dimensions and perspectives that permeate the debate on encryption policies in the 21st century, especially concerning the Crypto Wars. Although this complexity makes it impossible to carry out an exhaustive investigation of all aspects of the controversy in question, the systematic analysis of the interviews' content resulted in the mapping of its main contentious elements, as well as the evaluative and factual assumptions that underlie the actors' positions. From this mapping, the relationships between the actors' perceptions and the socio-economic, legal, political, and technical contexts with which they objectively relate were examined.

During phases I and II of the Crypto Wars, the heart of the controversy has sometimes been identified with the issue of exceptional access to content protected by strong encryption. In the analyzed statements, it was observed that the defense of measures of this sort is articulated through an essentially political-legal rationality. Its fundamental assumptions are the primacy of security - understood as success in criminal prosecution, especially in the case of serious crimes - over privacy and the existence of a duty of aptitude to breach confidentiality applicable to technology companies and application providers. Still, it understands the belief in the reliability of institutional controls as a normative principle whose acceptance is necessary for the functioning of the State, at the risk of disqualifying the entire institutionality, and from it inferred the risks of abuse of the tool by public authorities.

Discourse against backdoor access, in turn, takes on a different emphasis. On the one hand, it argues that the damages of the measure are excessive at the technical (reduction of system security), legal-political (disproportionality, risks to users' rights, and damage to trust in the digital environment), and economic (too much burden on providers and prejudice to the entire digital economy). On the other hand, it questions the effectiveness and necessity of the measure, arguing that it is not possible to know to what extent encryption actually contributes to investigative failure and that it is likely that targeted criminals would evade the weakened platform.

The mapping of the arguments that permeate these discourses highlights the existence of legal and factual premises that can be hermeneutically or empirically examined, which can significantly contribute to the maturing of the debate. The analysis presented showed, for example, that the existence of a duty of aptitude to breach confidentiality applicable to the technology and digital applications sectors in Brazil is, at least, legally contestable. Similarly, it demonstrated that concerns about the damages of exceptional access find theoretical support in cryptographic science and empirically in studies on the Brazilian political environment and on the economic impacts of restrictive encryption rules.

On the other hand, it found that there are methodological obstacles to a qualified assessment of the alleged trivialization of breaches of confidentiality in the country - even though the explosive growth in the volume of breaches is a phenomenon worthy of note in itself. Furthermore, it draws attention to the need for studies that investigate the effective dimension of the alleged obstacle represented by encryption in the success of the criminal investigation and investigate the empirical backing of the thesis of migration of criminality as a result of the implementation of backdoor access.

Although this qualification can be positive for the debate, the contrast between the emphases and the ethical-political premises of the two rationalities exposed also suggests that the simple fact-testing of the two sides' claims has limited potential for resolving the established controversy. That is because the actors' points of view are inserted in more general narratives, attitudes, and affective dispositions about the relations between State and individual, between privacy and security. The defense of backdoor access treats the reliability of institutional controls as a normative principle, while opposition to such a measure is based on skepticism about the effectiveness of these controls. One side associates security with images of effective criminal prosecution, whereas the other associates it with technological platforms designed for maximum protection of the information transmitted. One side sees the repressive role of the State as fundamentally a guarantor of the public interest, while the other sees it as highly susceptible to political instrumentalization against democratic freedoms.

Take as an example the thesis that there is a duty of aptitude to breach confidentiality applicable to the technology and digital applications sectors in Brazil. Its challenge would hardly resolve the controversy: advocates of backdoor access could simply replicate it, mobilizing other legal arguments to substantiate the existence of such a duty, or, alternatively, shift the debate from the descriptive plane to the normative plane, arguing

that if such a duty does not exist, it should come into existence by force of law or higher court-law. That is because this position assumes, in addition to the specific question about the existence of this provision in the Brazilian order, that it is fundamentally unacceptable that there are communicative spaces inaccessible to the eyes of the State authority.

That is similarly supported by examining the controversies surrounding alleged alternatives to backdoor access. Proposals like client scanning, government hacking, and extensive use of metadata tend to meet tremendous resistance among digital rights activists and academics. Although they do not necessarily interfere with the algorithm used or with the processes of generating and managing keys, such solutions are seen as undermining encryption because they reach the values that the use of encryption conventionally seeks to protect. Thus, it is observed that the defense of encryption is connected to broader concerns such as the protection of privacy, freedom of expression, political rights, and democratic values, in a context in which these are threatened by cybercrime and State vigilantism. In this light, the expansion of vigilantism is seen as an attack on encryption even though it does not involve direct interference with the cryptographic system.

Likewise, the controversy surrounding the interpretation of arts. 10, 11, and 12 of the Internet Bill of Rights evoke this deeper dissent about the values that should guide the interpretation of the law. The interpretation against blocking emphasizes the protective sections of privacy and personal data protection of devices precisely because these are the fundamental values that such rationality embraces. On the other hand, the interpretation favorable to the blockings emphasizes the obligation to respect Brazilian legislation because its primary concerns regard the threat posed by global technology companies to the State authority, which they are in a position to challenge because of their transnational economic power. From the perspectives of both actors, what is at stake goes deeper than the wording of these specific devices.

Throughout this study, the objective was to present the argumentative dimensions that permeate the current debate between public security and state defense versus the rights to privacy and freedom of expression in the digital environment – at the heart of the use of strong encryption techniques. It is a longstanding debate, dating back to the second half of the 20th century, which has remained perennial ever since. It is clear, however, that this is a deeper issue than what can be observed at first sight: the arguments in favor of both positions acquire multiple dimensions, which go beyond the very legitimacy of encryption. Thus, the multiple faces of this discussion – social, political, legal, among others – cannot be considered individually in favor of the complete resolution of the controversy.

Finally, this research attempted to contribute to the perspectives that make up the debate on the use of encryption. The mapping of interviewees' data, as well as the analysis of these pronouncements in the light of the Brazilian legal mechanisms, can be used for a deeper qualification of the debate, based on future studies.

7. References

ABELSON, Hal *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. **Journal of Cybersecurity**, v. 1, n. 1, p. 69-79, 2015. p.69.

ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017, p. 24-42. p. 29.

ABREU, Jaqueline. Audiência Pública sobre Criptografia e Bloqueios do WhatsApp: argumentos diante do STF. 26/06/2017. Bloqueios.info . Available in <http://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/>, Access on 02 ago 2021.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. p. 44-45

AGÊNCIA CÂMARA DE NOTÍCIAS. **Relatório preliminar do novo CPP incorpora provas digitais e novas tecnologias ao processo criminal.** Relator: Deputado João Campos. 13/04/2021. Available in <https://www.camara.leg.br/noticias/745824-relatorio-preliminar-do-novo-cpp-incorpora-provas-digitais-e-novas-tecnologias-ao-processo-criminal/ >, Access on 26 ago. 2021.

ALMEIDA, Frederico de. MONTEIRO, Filipe Jordão; SMIDERLE, Afonso.a criminalização dos protestos do movimento passe livre em são paulo (2013-2015). **Revista Brasileira de Ciências Sociais** [online]. v. 35, n. 102, 2020.

ANTONIALLI, Dennys. M.;ABREU, Jacqueline; MASSARO, Heloisa. M. M. ; LUCIANO, Maria. Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. **Revista Brasileira de Ciências Criminais**, v. 154, p. 177-214, 2019.

ARTIGO 19. **As restrições ao direito de protesto no Brasil**. 5 anos de junho de 2013: Como os três poderes intensificaram sua articulação e sofisticaram os mecanismos de restrição ao direito de protesto progressivamente. Artigo 19, 2018. Available in: https://artigo19.org/5anosde2013/. Access on: 04/08/2021.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA; CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO (LAUT). **Retrospectiva - Tecnoautoritarismo 2020. LAUT,** 2021. Available in: https://laut.org.br/wp-content/uploads/2021/01/RETROSPECTIVA-TECNOAUTORITARISMO-2020.pdf. Access on: 04/08/2021.

BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. The Economic Impact of Laws that Weaken Encryption **Law & Economics Consulting Associates** (LECA). 2021. Available in: https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/ .Access on: 04/08/2021.

BARIFOUSE, R.; DUARTE, F.; BARRUCHO, L. G. Liberação do WhatsApp não encerra polêmica disputa com Justiça brasileira. **G1**. Tecnologia e Games. Available in: http://g1.globo.com/tecnologia/noticia/2015/12/liberacao-do-whatsapp-nao-encerra-polemica-disputa-com-justica-brasileira.html. Access on: 29/07/2021.

BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (BERKMAN). **Não Entre em Pânico**: Avançando no debate sobre "obscurecimento" (Going Dark). 2018. Tradução pelo Instituto de Tecnologia e Sociedade do Rio. Available in: https://itsrio.org/wp-content/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_PT.pdf Access on 02/08/2021.

BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais. **Em Tese - Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC**, Florianópolis, v. 2, n. 1 (3), p. 68-80, jan./jul. 2005.

BRADFORD, Sharon. THOMPSON, Andi Wilson. Open Letter to GCHQ on the Threats Posed by the Ghost Proposal. **Lawfare - Hard National Security Choices**, 30 mai. 2019. Available in: https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal. Access on: 05 ago. 2021.

BRANDÃO, et al. (Org.). **Tecnologias e conectividade**: direito e políticas na governança das redes. 1ed. Belo Horizonte: 2018, v. 1, p. 15-30.

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. DF: Presidência da República, 2014. Available in: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Access on: 05 ago. 2021.

BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. **Processo nº 201655090143**. Decisão. Juiz Marcel Maia Montalvão. Lagarto, Sergipe, 26 abr. 2016.

BRASIL. Tribunal de Justiça do Estado de Sergipe. **Mandado de Segurança nº 201600110899**. Decisão liminar. Rel. Des. Ricardo Múcio Santana de Abreu Lima. Aracaju, 3 mai. 2016. Available in: <http://www.omci.org.br/m/jurisprudencias/ arquivos/2016/tjse_201600110899_03052016.pdf> Access on: 2 nov. 2016.

BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Inquérito Policial nº 062-00164/2016**. Juíza Daniela Barbosa Assumpção de Souza. Duque de Caxias, RJ, jul. 2016. Available in: <https://drive.google.com/file/d/0Bw3seZUv__5ubnFudjUwMm9OZGc/view>. Access on: 30/07/2021

BRASIL. Conselho Nacional de Justiça (CNJ). Sistema Nacional de Controle de Interceptações Telefônicas. **CNJ**, Brasília, 2021. Available in: https://www.cnj.jus.br/sistemas/sistema-nacional-de-controle-de-interceptacoes-telefonicas/. Access on: 04/08/2021.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **Mandado de Segurança nº 2271462-77.2015.8.26.0000**. Decisão liminar. Rel. Des. Xavier de Souza. São Paulo, 17 dez. 2015. Available in: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_22714627720158260000_17122015.pdf. Access on: 29/07/2021.

BRASIL. Central de Inquéritos da Comarca de Teresina. **Nota**. Juiz Luiz de Moura Correia. Teresina, 26 fev. 2015. Available in: http://s2.glbimg.com/MdNVliNDOaF45o27HM8_tsG3wll=/s.glbimg.com/jo/g1/f/original/2015/02/26/nota_juiz_whatsapp_ok.jpg. Access on: 29/07/2021.

BRASIL. Tribunal de Justiça do Estado do Piauí. **Mandado de Segurança nº 2015.0001.001592-4**. Rel. Des. Raimundo Nonato da Costa Alencar. Teresina, 26 fev. 2015. Available in: <http://www.migalhas.com.br/arquivos/2015/2/art20150227-03.pdf> Access on: 29/07/2021.

BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas.** 30/12/2020. Available in <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx>, Access on 03 ago 2021.

BRASIL.Superior Tribunal de Justiça. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma.** 24/06/2021. Available in <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021-Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decide-Quinta-Turma.aspx>, Access on 03 ago 2021.

BRASIL. Ministério da Justiça e Segurança pública. **Simpósio sobre Going Dark termina com declaração de 13 países.** Available in <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2>, Access on 03 ago 2021.

BRASIL. Supremo Tribunal Federal. **Medida cautelar de arguição de descumprimento de preceito fundamental**. Decisão liminar. Rel. Min. Ricardo Lewandowski. Brasília, 19 jul. 2016. Available in: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf. Access on: 30/07/2021.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental Nº 403.** Relator: Edson Fachin. Brasília, DF. Available in: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Access on: 06 ago. 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade Nº 5527**. Relatora: Rosa Weber. Brasília, DF. Available in: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Access on: 06 ago. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus Nº 51.531 - RO**. Rel. Ministro Nefi Cordeiro. Brasília, 09 mai. 2016. Available in: https://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7/inteiro-teor-340165652. Access on: 05 ago. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 580.664 - RJ**. Rel. Ministro Nefi Cordeiro. Brasília, 20 out. 2020. Available in:https://stj.jusbrasil.com.br/jurisprudencia/1206242995/habeas-corpus-hc-580664-rj-2020-0111177-4/inteiro-teor-1206243005 . Access on: 05 ago. 2021

BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. Processo nº 201655090143. **Decisão. Juiz Marcel Maia Montalvão**. Lagarto, Sergipe, 26 abr. 2016.

BRASIL. **Declaração do Going Dark Brasil.** Available in <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2/documentos/declaracao-do-going-dark-brasil.pdf> Access on 04 ago 2021.

BRASIL. Câmara dos Deputados. **Parecer do Relator, Dep. João Campos (REPUBLIC-GO) da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 8045, de 2010, do Senado Federal, que trata do "Código de Processo Penal" (revoga o Decreto-Lei nº 3.689, de 1941. Altera os Decretos-Lei nº 2.848, de 1940; 1.002, de 1969; as Leis nº 4.898, de 1965, 7.210, de 1984; 8.038, de 1990; 9.099, de 1995; 9.279, de 1996; 9.609, de 1998; 11.340, de 2006; 11.343, de 2006), e apensados ao Projeto de Lei nº 8.045, de 2010**. Portal da Câmara dos Deputados. Brasília, 26 abr. 2021. Available in: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/gt-anteprojeto-do-novo-codigo-de-processo-penal/documentos/outros-documentos/substitutivo-relator-joao-campos. Access on: 05 ago. 2021. p. 481.

CANABARRO, Diego. AULA 4 - Criptografia: experiências regulatórias e debates internacionais com Diego Canabarro. Belo Horizonte: **Instituto Iris,** 2021. (39 min.), son., color. Available in: https://youtu.be/EDaI5_z-hBo?t=2200. Access on: 25 ago. 2021.

CANTO, Mariana. RAMIRO, André. REAL, Paula C. Criptografia no STF: O que dizem os votos de Rosa Weber e Edson Fachin e o que podemos aprender com eles. **IP.Rec – Instituto de Pesquisa em Direito e Tecnologia do Recife.** Available in <https://ip.rec.br/2020/06/22/criptografia-no-stf-o-que-dizem-os-votos-de-rosa-weber-e-edson-fachin-e-o-que-podemos-aprender-com-eles/ >, Access on 02 ago 2021.

CARVALHO, Thaís Bernardes. **O bloqueio judicial do WhatsApp no território brasileiro no contexto do Estado Democrático de Direito.** 2017. 69 f. Monografia de graduação no curso

de Direito - Universidade Federal de Lavras, Lavras, 2017; Available in http://repositorio.ufla.br/handle/1/30751. Access on 16 de agosto de 2021.

CRABTREE, B. & MILLER, W. **Doing qualitative research**. Thousand Oaks, Calif.: Sage Publications, 1999.

COALIZÃO PELOS DIREITOS NA REDE. **Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia.** 20 de maio de 2021. Available in <https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>, Access on 25 ago. 2021.

COMEY; James B. **Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?** Out. 2014, discurso realizado na Brookings Institution. [Online]. Available in https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Access on: 02 ago. 2021.

DIFFIE, Whitfiead. HELLMAN, Marin. **New directions in cryptography.** IEEE Transactions on Information Theory, 22, 644-654.

DONEDA, Danilo. MACHADO, Diego. (coords.) **A criptografia no direito brasileiro**. São Paulo: Thompson Reuters - Revista do Tribunais, 2019.

FROOMKIN, Michael. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

GASKELL, G. Entrevistas individuais e grupais. In: BAUER, M. W.; GASKELL, G. (Org.). **Pesquisa qualitativa com texto, imagem e som**: um manual prático. Petrópolis, RJ: Vozes, 2000, pp. 64-89.

GEC - Global Encryption Coalition. **Brazilian Code of Criminal Procedure reform must not undermine encryption.** June 28, 2021. Available in <https://www.globalencryption.org/2021/06/brazilian-code-of-criminal-procedure-reform-must-not-undermine-encryption/>, Access on 25 ago. 2021.

GROVER, Gurshabad; RAJWADE, Tanaya; KATIRA, Divyank. The Ministry And The Trace: Subverting End-To-End Encryption, 14 NUJS Law Review. 1(2021). p. 2-6. Available in <http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/ >. Access on: 02 ago. 2021.

HOBOKEN, J. V.; SCHULZ, W. **Human rights and encryption**. Paris: UNESCO, 2016.

INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. Cryptologia, v. 3, n. 3, 129 - 135, 1979.

INTERNET SOCIETY. Fact Sheet: Ghost Proposals. **Internet Society**, 24 mar. 2020. Available in: https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/. Access on: 06 ago. 2021.

INTERNET SOCIETY. Fact Sheet: Client-Side Scanning. **Internet Society**, 24 mar. 2020. Available in: https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/. Access on: 06 ago. 2021.

INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. **Internet Society**, 27 nov. 2020. Available in: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/. Access on: 06 ago. 2021.

JARVIS, Craig. **A New Crypto Wars Chronology (I)**. 21 fev. 2020. LinkedIn: Craig Jarvis. Available in: https://www.linkedin.com/pulse/new-crypto-wars-chronology-craig-jarvis/. Access on: 29 jul. 2021.

JARVIS, Craig. **A New Crypto Wars Chronology (II)**. 20 jul. 2020. LinkedIn: Craig Jarvis. Available in: https://www.linkedin.com/pulse/new-crypto-wars-chronology-ii-craig-jarvis/?articleId=6690894456150859776. Access on: 29 jul. 2021

JARVIS, Craig. Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. CRC Press, 2020.

KAMARA et al. Outside Looking In: Approaches to Content Moderation in End-to-End Encrypted Systems. **Center for Democracy and Technology Research,** Washington, ago. 2021. Available in: https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/. Access on: 26 ago. 2021.

KRIPPENDORFF, K. **Content Analysis**: an introduction to its methodology. Thousand Oaks, Calif.: Sage Publications, 2004.

KURTZ, Lahis P.; MENEZES, Victor. A.. **Entre o direito e a força na sociedade da informação: bloqueio judicial do WhatsApp e ADI nº 5.527.** In: Fabrício Bertini Pasquot Polido; Lucas Costa dos Anjos; Luiza

LEVY, Ian. ROBINSON, Crispin. Principles for a More Informed Exceptional Access Debate. **Lawfare - Hard National Security Choices**, 29 nov. 2018. Available in: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate . Access on 05 ago. 2021.

LIU, H. Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause. Journal of World Trade, v. 51, n. 2, p. 309 - 334, 2017.

MASI, Carlos Velho. O caso Escher e outros v. Brasil e o sigilo das comunicações telefônicas. **Revista dos Tribunais**, v. 932, Junho de 2013, pp. 309-352

MITCHELL, Bonnie et al. Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation. 2017.

PORTNOY, Erica. Why Adding Client-Side Scanning Breaks End-To-End Encryption. **Electronic Frontier Foundation**, 1 nov. 2019. Available in: https://www.eff.org/pt-br/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption. Access on: 06 ago. 2021.

QUEIROZ, Rafael Mafei Rabelo. PONCE, Paula Perdigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, v.1,n.1, fev/2020, p.64-90.

RAMIRO, André. CANTO, Mariana. REAL, P. C. et al. **O Mosaico Legislativo da Criptografia no Brasil: Uma Análise de Projetos de Lei**. IP.Rec. Available in <https://ip.rec.br/wp-content/uploads/2020/08/O-mosaico-legislativo-da-criptografia-no-Brasil-uma-an%C3%A1lise-de-Projetos-de-Lei-1.pdf >, Access on 04 ago 2021.

RAY, Trisha. The Encryption Debate in India: 2021 Update. 2021.

RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

RODRIGUES, G. R. A controvérsia cifrada: o Clipper e o mito da derrota estatal nas guerras criptográficas dos anos 1990. Em: ALVES, Marco Antônio Sousa. NOBRE, Marcio Rimet. (orgs.). **A sociedade da informação em questão**: o direito, o poder e o sujeito na contemporaneidade. Belo Horizonte: D'Plácido, 2019.

ROSENTHAL, G. **Pesquisa social interpretativa**: uma introdução. Porto Alegre: Edipucrs, 2014.

SCHNEIER, Bruce. **Applied Cryptography**: Protocols, Algorithms, and Source Code in C. 20th Anniversary Edition. New Jersey: John Willey & Sons, 1996, p. 30.

SCHULMAN, Ross. Why the Ghost Keys 'Solution' to Encryption is No Solution. **Just Security**, 18 jul. 2019. Available in: https://www.justsecurity.org/64968/why-the-ghost-keys-solution-to-encryption-is-no-solution/. Access on: 05 ago. 2021.

SILVA JUNIOR, L. A.; LEAO, M. B. C. O software Atlas.ti como recurso para a análise de conteúdo: analisando a robótica no Ensino de Ciências em teses brasileiras. **Ciênc. educ.** (Bauru), Bauru , v. 24, n. 3, p. 715-728, set. 2018.

SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 234-235.

STEPANOVICH, Amie et al. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Available in:https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf. Access on: 05 ago. 2021.

STILGHERRIAN. The Encryption Debate in Australia: 2021 Update. 2021.

UNITED NATIONS. **Encryption and Anonymity follow-up report.** 2018. Available in:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Access on: 05 ago. 2021.

VINUTO, J. A amostragem em Bola de Neve na pesquisa qualitativa: um debate em aberto. **Temáticas** (UNICAMP), v. 44, p. 201-218, 2014.

WHATSAPP INC. **Blog do WhatsApp**. Criptografia de Ponta-a-Ponta. 05 abr. 2016. Available in: https://blog.whatsapp.com/end-to-end-encryption. Access on: 30/07/2021

8. Appendix 1 - Interview Script

Part I - Presentation and general themes

1. How old are you?
2. Where do you live?
3. What is your study background?
4. Where do you work nowadays? (Position and assignments)
5. Tell more about your professional trajectory? (Explore: Where did you work? What were your assignments? How was your contact with internet and society issues?)
6. How the transformations that the internet brought to society impacted your professional trajectory?
7. Considering the internet's transformations to society, is there something you understand as especially positive or negative?

Part II - Encryption, Privacy and Security

8. On a scale of 0 to 10, what importance do you place on privacy in **today's society**? Why?
9. On a scale of 0 to 10, what importance do you place on **your** privacy? Why?
10. How do you assess the public debate on privacy today? (Explore: Brazil, other countries, etc.)
11. How do you see the relationship between privacy and security today? (Explore: are there contexts in which these values conflict?)
12. In your perception, what are the relationships between public security and information security?
13. On a scale of 0 to 10, what importance do you place on encryption in **today's society**? Why?
14. On a scale of 0 to 10, how important do you place on encryption in **the applications you use**? Why?
15. On a scale of 0 to 10, how satisfied are you with the current regulatory environment on

encryption? Why?

16. If you could, would you change anything in this environment? What?

17. In your opinion, are there situations where the encryption uses conflicts with the public interest? (Explore different understandings of the audience)

18. Would you support the introduction of a backdoor mechanism in encryption for criminal investigation purposes? (Explore: Why? If so, what are the legitimate and illegitimate situations for using this mechanism? Are there related risks? If so, what? Are there associated economic, reputational, or social costs? Is there any middle ground?)

19. In your opinion, is it possible to reconcile user security with the introduction of a backdoor mechanism in encryption?

20. How do you assess the WhatsApp blockings' legitimacy that occurred in 2015 and 2016 in Brazil? (Explore the legitimacy dimension)

21. **To Law professionals:** In your opinion, does the Internet Bill of Rights authorize application blocking for non-compliance with data delivery orders for criminal investigation purposes?

22. Do you know any alternative for accessing this data that does not involve a backdoor? (Explore: if so, what? what are the risks associated with each?)

23. Have you ever worked in any situation that somehow involved the issue of access to encrypted data?

24. In your work, do you deal with issues related to encryption regulation in any way?

25. **To public servers/agents**: In your opinion, are the efforts to modernize the public service and digitize the government accompanied by a concern with information security?

Part III - Training and education

26. Considering technical and regulatory aspects, from 0 to 10, what grade do you give to your level of knowledge about encryption? Why? (Explore: Are there gaps? If so, which ones?)

27. Have you ever taken any course or training focused on this field? (Explore: If yes, which institution was responsible for it? How long was it? What was the modality - live online, recorded online, in person?)

28. What should a course that aims at advancing this discussion address?

29. Is there anything I didn't ask that you think would make sense for me to ask?

9. Appendix 2 - Code Families

I - Backdoors for Criminal Investigation Purposes Codes (AE::)

AE:: Support

AE:: Confidentiality's breaches banalization

AE:: Service evasion

AE:: With hard institutional controls

AE:: Compromise the evidence legality

AE:: Operational costs for providers

AE:: Reputational costs for providers

AE:: Unnecessary, as there are other investigation means

AE:: Need to trust in justice

AE:: It violates the Information Security and encryption principles

AE:: It violates the State security

AE:: It impacts trust in the digital ecosystem

AE:: Important in the name of security

AE:: Support not determined

AE:: Lack of knowledge, doubt or uncertainty manifestation

AE:: No support

AE:: No evidence of gains

AE:: The defense is needed to enhance public authority

AE:: Cooperation with justice obligation

AE:: Compliance to court order obligation

AE:: As or less serious than the means currently employed

AE:: For specific crimes

AE:: Risk of authority's abuse

AE:: Risk of third malicious part's usurpation

AE:: Risk for rights

AE:: Similar to phone intercept

AE::Last remedy

AE:: Third party's vulnerability

II - Regulatory Environment Satisfaction on Encryption Codes (AR::)

AR:: Brazil is better than abroad

AR:: An institution creation to define standards

AR:: Encryption is under threat

AR:: STF's decision are good

AR:: Does not know

AR:: There must be standardization for a higher security level

AR:: There must be protection against backdoor/app blocking

AR:: Enforcement is fragile

AR:: Encryption importance is recognized

AR:: Does not exist

AR:: Technological neutrality is positive/important

AR:: Positive, debate about going dark has advanced

AR:: Poorly regulated, does not cover most uses

III - Legitimacy of Whatsapp blocking in 2015/16 (BW::) and on whether the Internet Bill of Rights authorizes such a measure Codes (MCI::)

BW:: Investigative shortcut

BW:: Authorizes, if proportional

BW:: Blockings were disproportionate

BW:: Blockings were illegitimate

BW:: There was a lack knowledge about the technology

BW:: There was forces dispute motivation

BW:: There were economic damages

BW:: Companies' ignorance

BW:: Inconstitutional

BW:: Ineffective as people downloaded VPN

BW:: Wrong interpretation of the Internet Bill of Rights

BW:: The Brazilian Justice is not competent

BW:: Legitimate, the law must be fulfilled

BW:: Tool's penalization

BW:: It is possible to authorize

BW:: The first blocking did not involve encryption

MCI:: It authorizes, as the article 11 talks about "Brazilian law"

MCI:: Out of the general caution power

MCI:: Regardless of the Internet Bill of Rights, due to the general caution power

MCI:: Regardless of the Internet Bill of Rights, due to foundation at the Criminal Procedure Code

MCI:: It does not authorize

MCI:: It does not authorize, because the measure is too grave

MCI:: It does not authorize, because it is a diabolic evidence

MCI:: Sanctions are only to protect privacy

MCI:: Sanctions must exist as a final resource

MCI:: Refuse to answer

IV - Known alternative methods of accessing encrypted information and their risks Codes (MA::)

MA Risks:: Security incident

MA Risks:: Others

MA Risks:: Risk of authority's abuse

MA Risks:: Indiscriminate violation of intimacy

MA Risks:: It vulnerates third parties

MA:: Back up

MA:: Search, seizure, and deblocking

MA:: Client-side scanning

MA:: Exhaustive key-search

MA:: Do not know or do not remember

MA:: Social Engineering

MA:: Number mirroring

MA:: Ghosting

MA:: Traditional infiltration

MA:: Lawful hacking

MA:: Metadata

MA:: Others

MA:: Phishing

MA:: Spyware