http://dx.doi.org/10.5902/2357797570703

InterAção

Vol. 13, nº 01,
Jan/Jun 2022

Dossiê
Relacionalidade entre
Política e Ciência Moderna

Luciano Vaz Ferreira[1]

ENSAIO

CYBERSECURITY AND RANSOMWARE IN THE BRAZILIAN GOVERNMENT

CIBERSEGURANÇA E RANSOMWARE NO GOVERNO BRASILEIRO

Abstract:
The increasing reliance on digital services and the lack of a solid cybersecurity infrastructure and framework have made Brazil one of the biggest targets for cyberattacks in the world. One increasingly common type of attack is known as ransomware, in which perpetrators lock systems and databases and demand money to unlock them. The essay aims to provide an overview of ransomware as a threat to cybersecurity in the public sector, with special attention to the Brazilian context. Therefore, the Brazilian institutional and legal framework for cybersecurity and ransomware control is examined. From a methodological point of view, the study is limited to a literature review composed of academic scholarship and official documents (international and national) on the subject. As a partial result, it was found that the issue of cybersecurity and ransomware has been gradually included in the government's agenda through strategic documents, new organizational structures, legislative reforms, and international cooperation measures.

Keywords: Cybersecurity; Ransomware; Brazil; Government.

Resumo:
A confiança crescente nos serviços digitais e a falta de uma infraestrutura e de um framework sólido de cibersegurança fizeram do Brasil um dos maiores alvos de ciberataques do mundo. Um tipo de ataque cada vez mais comum é conhecido como ransomware, em que os perpetradores bloqueiam sistemas e bases de dados e exigem dinheiro para o desbloqueio. O ensaio tem como objetivo fornecer uma visão geral do ransomware como uma ameaça à cibersegurança no sector público, com especial atenção para o contexto brasileiro. Sendo assim, é examinado o framework institucional e jurídico brasileiro para a cibersegurança e o controle de ransomware. De um ponto de vista metodológico, o estudo limita-se a uma revisão bibliográfica composta por pesquisas acadêmicas e documentos oficiais (internacionais e nacionais) sobre o tema. Como resultado parcial, verificou-se que as questões de cibersegurança e de ransomware foram gradualmente incluídos na agenda do governo por meio de documentos estratégicos, novas estruturas organizacionais, reformas legislativas, e medidas de cooperação internacional.

Palavras-chave: Cibersegurança; Ransomware; Brasil; Governo.

INTRODUCTION

In recent years, Brazil has undergone an intense digitalization process that has impacted various sectors of society, including the government. The increasing dependence on digital services and the lack of a solid cybersecurity infrastructure and framework have made Brazil one of the biggest targets for cyberattacks in the world. One increasingly common type of attack is known as ransomware, in which perpetrators lock systems and databases and demand money to unlock them. Public organizations in Brazil have already been victims of ransomware, most notably the recent incident at the Superior Court of Justice, which is considered the worst cyberattack in Brazil's history.

The essay aims to provide an overview of ransomware as a cybersecurity threat in the public sector, with special attention to the Brazilian context. Therefore, the Brazilian institutional and legal framework for cybersecurity and ransomware

[1] Ph.D. in International Strategic Studies (UFRGS). Professor at University of Brazilian Air Force (UNIFA) and Federal University of Rio Grande (Brazil). lvazferreira@gmail.com. https://orcid.org/0000-0002-7174-4109

control is examined. From a methodological point of view, the study is limited to a literature review composed of academic scholarship and official documents (international and national) on the subject.

The essay is divided into two parts. The first part analyzes the digitalization process of society, the emergence of electronic and digital government, the advances in cybersecurity threats, the conceptual aspects of ransomware and the role of the Budapest Convention. The second part focuses on Brazil, including an analysis of the Brazilian government's progress in digitalization, the inclusion of cybersecurity in the federal government's agenda, and the challenges of creating an institutional and legal framework to control ransomware.

DIGITAL GOVERNMENT AND RANSOMWARE

In recent decades, the world has been fundamentally transformed by the emergence of new information and communication technologies such as artificial intelligence, Big Data, the Internet of Things, and cloud computing. By analyzing data collected on the Internet (such as location, age, and personal preferences), it is possible to provide information and services to a user according to his network behavior, thus creating a “customized” experience (MAYER-SCHONBERGER; CUKIER, 2013). The expansion of the use of cyberspace has created new opportunities for shopping (e-commerce), managing finances (e-finance), studying (distance learning), working (home office), moving (mobility apps), building interpersonal relationships (social networks), and governing (digital government). The recent Covid 19 pandemic appears to have further accelerated this process.

The digitalization of society has also changed the actions of States and governments. One of the first experiences was with the beginning of computer development in the 1990s, when the idea of e-government emerged. The goal was to provide government information and services through the Internet and other digital means (WEST, 2004, p. 16). The implementation of e-government includes different stages: a) the exclusive provision of electronic content on a website; b) the opening of interactive communication channels; c) the provision of online services; d) the full digital integration between different sectors (UNITED NATIONS, 2002). The OECD (2020) is already taking this model to a higher level in the form of “digital government”, which includes a continuous government digitalization policy; the use of data as a standard method for planning, implementing, and monitoring public policies; government as a platform with a focus on the user experience; comprehensive transparency of government data and the policy-making process; and proactivity in developing digital solutions.

Despite potential gains in efficiency and effectiveness, the increasing reliance on digital services also introduces new vulnerabilities. In recent years, personal computers, businesses, network infrastructures, and governments have repeatedly been targets of cyberattacks. Although there are no reliable statistics on the subject, it is estimated that thousands of attacks take place every day, causing millions of dollars in losses[2]. The attackers' motives vary and can be money, fame, promoting an ideological movement, or waging a cyberwar sponsored by a foreign state (KALLIEROS, GERMANOS, KOLOKOTRONIS, 2021, p. 04). In this context, one of the key aspects of the digitalization of society is the development of cybersecurity capabilities, defined as “the ability to protect or defend the use of cyberspace from cyberattacks” (KISSEL, 2011, p. 57). With the advent of e-government, public institutions also have their own cyber vulnerabilities and require cybersecurity investments.

An increasingly common type of cyberattack is ransomware. This is the use of some type of code or malicious software (malware) to

[2] Several organizations, usually cybersecurity service providers and law enforcement agencies, frequently publish statistics on cyberattacks, but their sources and methods are not presented.

extort money (ransom) from other users (MARION; TWEDE, 2020, p. 351). First, the criminal invades and controls a user's devices to prevent access to his files, such as photos, spreadsheets, and other documents. In exchange for releasing the victim's access, the criminal demands payment of a certain amount and sets a deadline. If the payment is not made, the perpetrator can increase the demanded amount, destroy the data, or reveal sensitive information. The first ransomware cybercrime spread via floppy disk in 1989, known as PC Cyborg. Over the decades, new methods of spreading have been developed. Currently, mainly spearphishing emails are used for this type of cybercrime.

Ransomware victims may suffer from temporary or permanent loss of sensitive data, disruption of regular operations, financial losses in recovering their files and systems, and possible damage to the reputation of a particular organization (UNITED STATES OF AMERICA, 2017). It is common for a ransom to be paid to the criminals to minimize the damage caused (HOLT; BOSSLER; SEIGFRIED-SPELLAR, 2018, p. 157). This payment is made with crypto assets, as this guarantees a secure and secret transfer that is difficult to trace (MARION; TWEDE, 2020, p. 351).

Sonicwall (2022, p. 29) estimates that the number of ransomware incidents doubled between 2020 and 2021, reaching the mark of 623.3 million attacks per year. This means that there is a ransomware attack every 20 seconds. Although the targets are usually enterprises, attacks on critical infrastructure and public institutions have increased.

The Center for Strategic & International Studies (CSIS) (2022) has compiled some of the most significant ransomware attacks on public administrations worldwide since 2006: 1) San Francisco Municipal Transportation Agency, USA, the public transportation payment system was blocked (November 2016); 2) Ukraine's Infrastructure System (June 2017); 3) Baltimore City Emergency Services, USA (March 2018); 4) Atlanta City Government, USA, with a loss of 2.6 million of dollars (March 2018); 5) Hospital Administration System in Germany, which caused the death of a patient who was ultimately transferred to the wrong hospital (September 2020); 6) Scottish Environment Protection Agency (December 2020); 7) Colonial Pipeline, the largest fuel pipeline in the United States, with a $5 million ransom payment (March 2021); 8) Ireland's Public Health System (May 2021); 9) CS Energy, a state-owned company in Australia, (December 2021); 10) Costa Rica's Ministry of Finance (April 2022).

Ransomware is a transnational threat, which increases the complexity of its control (HOLT; BOSSLER; SEIGFRIED-SPELLA, 2018, p. 27). One of the main problems is related to authorship, as it is very difficult to determine the identity, nationality, origin, or organization of the criminal (SINGER; FRIEDMAN, 2014, p. 74). Another important aspect is the fact that criminalization and processing of a possible ransomware claim is a prerogative of national sovereignties. This means that a country that is the target of a transnational cybercrime cannot take police or judicial action in another country, as this is a violation of sovereignty. In this context, the consent of the foreign country or international instruments, such as bilateral legal cooperation agreements, is required.

One of the most important initiatives in this area is the Convention against Cybercrime (Budapest Convention), which was drawn up by the Council of Europe in 2001. Its goal is to promote international cooperation among member States in combating cybercrime and to establish common measures (MARION; TWEDE, 2020, p. 76-78). The Convention obliges to criminalize certain acts and to harmonize the legislation of the participating States. It also allows for the maintenance of channels of communication between jurisdictions (police and judiciary) which includes, for example, the exchange of information, the sharing of evidence, and joint operations.

Unfortunately, the language of the Budapest Convention has not kept pace with recent technological advances, so devices and systems that were in use when the Convention was written are now obsolete (CLOUGH, 2012, p. 375; MARION; TWEDE, 2020, p. 78). There is no specific definition of ransomware in the international treaty, so it can be broadly categorized under the offense of invasion of electronic device. This would be sufficient to use the international cooperation mechanisms provided in this treaty to help investigate and deal with these crimes. One problem for which there is no obvious solution is the countries that refuse to cooperate or bind themselves to the international treaty, thus becoming safe havens for this type of activity (CLOUGH, 2012, p. 370).

THE BRAZILIAN CONTEXT

Brazil has had experience with digitalization in the federal government since 2000, when the first working groups and projects in this area began. In the following years, several committees, permanent structures, programs, and legislative reforms were created to develop information and communication technology in the Brazilian public administration. In terms of strategic planning, several guiding documents were created and regularly revised[3].

As a result, the Brazilian federal government has implemented several initiatives, such as the creation of systems for digital certification, open data availability, procurement, human resources management, business registration, and tax and labor inspection. In recent years, the unification of the different databases and communication channels with citizens has been intensified, especially in the context of pandemics. Currently, Brazilian citizens have access to more than 1,000 digital public services of a federal nature. These include access to social security programs, issuing documents, applying for public licenses and permits for certain activities, and making personal appointments with public institutions, among others. The Brazilian judiciary, both at the federal and state levels, has made an intense movement to digitize its activities since 2006. Currently, most court proceedings are conducted electronically.

Although Brazil has not yet reached the final stage of digitizing its administration, which would mean full integration of the different systems, the increase in data flow and online delivery of Brazilian public services is remarkable. This means that Brazil is increasingly exposed to its potential cybersecurity vulnerabilities. According to a 2022 survey conducted by Sonicwall (2022), Brazil already ranks as the fourth most ransomware-attacked country (public and private sectors), behind only the United States (1st), Germany (2nd) and the United Kingdom (3rd).

The first cases involving Brazilian public institutions have already been registered. In 2020, the database of the Superior Court of Justice (STJ), one of the largest federal courts in the country, was attacked, making its systems inaccessible. As a result, deadlines for thousands of cases were suspended, causing significant delays in the delivery of court service. This was considered the worst cyberattack in the country's history (BRASIL, 2021). A similar case was the ransomware attack on the Rio Grande do Sul State Court (TJ-RS), which demanded a ransom of $5 million of dollars. Also in the same year, the computer systems of the port of the city of Fortaleza, operated by the state-owned company Companhia Docas do Ceará, were blocked for several days, resulting in heavy losses as electronic operations such as the control and issuance of cargo had to be performed manually (BRITO, 2019).

Given the inevitable increase in ransomware attacks, it is appropriate to analyze whether Brazil has an institutional and legal framework that helps protect and control this threat in public institutions. In this context, two approaches are presented: ransomware prevention, represented by the maintenance of cybersecurity policies in public organizations; the processing and punishment of these acts related

[3] General Information and Communication Technology Strategy (started in 2008 and updated until 2015), Digital Governance Strategy (2016), Brazilian Digital Transformation Strategy (2018) and the Digital Government Strategy for the Period 2020 to 2022.

to ransomware, represented by the existence of national legislation aimed at assigning responsibility when incidents occur.

In 2000, the Brazilian federal government began developing its cybersecurity policy. The topic became increasingly present in official documents and new organizational structures were created. This process was favored by two important facts: the hosting of mega-events in Brazil (World Cup and Summer Olympic Games), which required capabilities to protect against cyberattacks, and the emergence of Wikileaks, which allegedly indicated possible espionage against the Brazilian government.

Among the various structures that have been developed, it is worth mentioning the creation of the Cabinet for Institutional Security of the Presidency of the Republic (Gabinete de Segurança Institucional da Presidência da República - GSI) in 2003 and the Center for Prevention, Treatment and Response to Cyber Incidents in Government, in 2006. In 2010, the GSI produced the Green Paper on Cybersecurity, which established general guidelines. In parallel, Brazil has also introduced a cyber defense policy[4].

In the following years, Brazil implemented a number of national legal norms that indirectly addressed cybersecurity: The Cybercrime Law of 2012, which amended the Brazilian Criminal Code to criminalize acts related to cybercrime[5]; the Civil Rights Framework for the Internet (Marco Civil da Internet) of 2014, which is responsible for establishing principles, guarantees, rights, and obligations for Internet use in Brazil; the General Data Protection Law (Lei Geral de Proteção de Dados - LGDP) of 2018, which regulates the processing of personal data to protect the fundamental rights of freedom, privacy, and free development of the natural person. In 2018, the National Information Security Policy was published. Finally, in 2020, the most important document to date in this area, the National Cybersecurity Strategy (E-Ciber), was published.

The LGPD, which addresses both private and public organizations, makes some interesting contributions to cybersecurity. According to the "security principle" (Article 6, VII and Article 46), data controllers (such as public organizations) must minimize exposure to threats by implementing security, technical and administrative measures to protect personal data from unauthorized access and accidental or unlawful destruction, loss, alteration, disclosure, or any form of inappropriate or unlawful processing (MASSENO; MARTINS; FALEIROS JÚNIOR, 2020, p. 08-09). The National Data Protection Authority (ANPD), which is responsible for monitoring and enforcing sanctions in this area, may establish minimum technical security standards (Article 46, §1). Security incidents (such as a ransomware attack) must be reported to the ANPD and the affected individuals (Article 48). The data affected, the risks involved, and the measures taken to reverse and mitigate the incident must be outlined.

Despite reported efforts, Brazil has traditionally been considered a country with modest cybersecurity policies. The recent National Cybersecurity Strategy, while highlighting the importance of strengthening the issue in the Brazilian context, has been criticized for being more of a "letter with good intentions" than a document with clear implementation goals, monitoring mechanisms, and a budget plan. Another point concerns the overreliance on the GSI and the low level of dialog with private actors and other sectors of civil society (HUREL, 2021 p. 21, 32).

It is important to note that recent efforts have focused on the Brazilian federal executive branch, and the extension to other branches

[4] Cyber defense is the development of offensive and defensive cyber capabilities in the context of armed conflict, a recurring task of military institutions. Brazil referred to the issue in the National Defense Policy of 2005 and in the National Defense Strategies of 2007 and 2012. In 2010, the Cyber Defense Center was established, and in 2014, the Joint Cyber Defense Command was created.

[5] The law was created in response to an incident in which intimate photos of a famous Brazilian actress were published after her electronic device was hacked.

(legislative and judicial) and other federated entities of the Brazilian Republic is uncertain. Considering that Brazil has 26 States, one Federal District, and 5,568 municipalities with widely varying digital and cybersecurity capabilities, concerns about vulnerability to cyberattacks and potential ransomware attacks do not appear to be exaggerated.

An additional concern for cybersecurity of public institutions in Brazil is the issue of perpetrator responsibility in ransomware incidents, which can theoretically serve as a deterrent. As this is still an emerging practice, there is no provision in Brazilian criminal law for the specific criminal conduct associated with ransomware. However, the Brazilian Criminal Code provides for some behaviors defined as cybercrimes that can be applied in these situations.

According to the Brazilian Criminal Code, ransomware can be classified as follows: (a) intrusion into a computer device (Article 154-A) for unauthorized access to the system; (b) electronic fraud (Article 171, § 2-A) for inducing error; (c) extortion (Article 158) for demanding a ransom; (d) attack on the security of public utilities (Article 265) or interruption or disruption of telegraph, telephone, computer, telematics, or utility information service (Article 266), if essential services are involved (WENDT; MASSENO, 2017, p. 11).

In addition to criminal responsibility for ransomware, recent Brazilian legislation (LGPD) also provides penalties for individuals and institutions that are negligent in implementing cybersecurity measures and incident response. The data controller and data processor associated with public entities may be held liable if they cause harm to the data subject (Article 42 of the LGPD). In this context, the improper collection of user data in a ransomware situation, the deletion of such data or even the unavailability of the electronic service can be mentioned as possible damages. The National Data Protection Authority may impose sanctions on public entities, such as a public reprimand, publication of the breach, suspension or prohibition of data processing. In addition, public officials may lose their posts and be ordered to compensate the public administration. The data subject may also file a claim for damages in the Brazilian courts to obtain compensation for possible losses (Article 52).

Regarding international cooperation in the fight against cybercrime, Brazil has taken its first steps. In 2019, Brazil was invited to join the Budapest Convention. The Federal Prosecution Service (MINISTÉRIO PÚBLICO FEDERAL, 2020) expressed its support for Brazilian accession, following the example of other Latin American countries (Argentina, Chile, Costa Rica, Dominican Republic, Panama, Paraguay, and Colombia). The instrument would be a step forward in harmonizing Brazilian legislation according to international standards and in strengthening international cooperation in investigations, evidence gathering, and extradition related to cybercrime in general.

The agreement obligates all signatories to cooperate, which allows for the expansion of cooperation with countries that have not yet signed a bilateral agreement in criminal matters with Brazil. The international treaty maintains direct contact points between authorities, which allows the existence of communication channels that can be accessed quickly and are available 24 hours a day. It is even possible to directly access databases and digital evidence hosted in other countries, if they agree. The potential obsolescence of the agreement has been minimized by the Federal Prosecution Service as it is indicated that the States Parties usually maintain working committees in which there is a mutual evaluation of the efforts implemented in the national legal systems and a continuous exchange of experiences (MINISTÉRIO PÚBLICO FEDERAL, 2020). Despite the lack of direct mention of ransomware, the fight against this transnational crime could certainly benefit from the mechanisms of the treaty.

In 2021, Brazil finally signed the Budapest Convention. Currently, the document is awaiting presidential sanction. The lack of public debate in this process has been sharply criticized by activists and civil society groups. They believe that implementing the Budapest Convention without reservations could mean limiting fundamental rights in Brazilian legislation on the use of cyberspace (COALIZATION OF RIGHTS IN THE NETWORK, 2022).

CONCLUSION

The digitalization of society is advancing and directly impacting the redesign of public institutions. As digital government becomes a reality, more attention needs to be paid to cybersecurity. This is especially true for the spread of ransomware, which is characterized by the use of some type of code or malicious software to extort money from other users. Victims have suffered the loss of sensitive data, disruption of their operations, financial losses and damage to their reputation. There are already records of several public institutions being attacked around the world. As this is a complex, transnational crime, its control requires the establishment of international cooperation mechanisms.

Although the Brazilian public sector has not yet reached the stage of full digitalization of its functions, it is already advanced in this regard. It should be noted that the issue of cybersecurity has been gradually included in the government's agenda, through the elaboration of strategic documents and the creation of organizational structures dedicated to this issue. There are also some legislative reforms in this area, such as the implementation of the General Data Protection Law, which dedicates part of its provisions to cybersecurity. Brazilian law appears to criminalize acts similar to ransomware and to place the responsibility for maintaining cybersecurity systems on public actors and institutions. Finally, the country appears to be making progress in international cooperation.

This is a small exploratory contribution on the topic of cybersecurity and ransomware in Brazilian public institutions, a subject that is still neglected in public and academic debate. Given the increasing number of incidents in Brazil and the importance of the topic, it is hoped that new research will emerge from the issues raised in this essay.

BIBLIOGRAPHY

BRASIL. *Supremo Tribunal Federal*, 2021. Available on: < http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=454634&ori=1>. Accessed on 15 jun. 2021.

BRITO, Paulo. *Porto de Fortaleza completa 7 dias refém de ransomware*. CISO Advisor, 2019. Available on: < https://www.cisoadvisor.com.br/porto-de-fortaleza-completa-7-dias-refem-de-ransomware/>. Accessed on: 21 jul. 2021.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. *Significant Cyber Incidents Since 2006.* Available on: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>. Accessed on: 15 jun. 2022.

CLOUGH, Jonathan. The Council of Europe Convention and Cybercrime: Defining 'Crime' in a Digital World. *Criminal Law Forum*, v. 23, p. 363-391, 2012.

COALIZAÇÃO DE DIREITOS NA REDE. *Carta aos Membros do Senado Federal sobre a Convenção de Budapeste*. Available on: <https://direitosnarede.org.br/2021/10/21/carta-aos-membros-do-senado-federal-sobre-a-convencao-de-budapeste/> Accessed on: 13 jun. 2022.

HOLT, Thomas; BOSSLER, Adam; SEIGFRIED-SPELLAR, Kathryn*.* *Cybercrime and Digital Forensics:* An Introduction. New York: Routledge, 2018.

HUREL, Louise Marie. *Cibersegurança no Brasil:* Uma Análise da Estratégia Nacional. 2021. Available on: <https://igarape.org.br/ciberseguranca-no-brasil-uma-analise-da-estrategia-nacional/>. Accessed on: 15 jun. 2022.

KAVALLIEROS, Dimitrios; GERMANOS, Georgios; KOLOKOTRONIS, Nicholas. Profiles of Cyber-Attackers and Attacks. In: KOLOKOTRONIS, Nicholas; SHIAELES, Stavros (Org.). *Cyber-security Threats, Actors, and Dynamic Mitigation.* Boca Raton: CRC Press, 2021, p. 01-26.

KISSEL, Richard. *Glossary of Key Information Security Terms*. Washington: U.S. Department of Commerce, 2011.

MARION, Nancy E; TWEDE, Jason. *Cybercrime:* An Encyclopedia of Digital Crime. 1 ed. Santa Barbara: ABC-CLIO, 2020.

MASSENO, M. D.; MARTINS, G. M.; FALEIROS JÚNIOR, J. L. M. A segurança na proteção de dados: entre o RGPD europeu e a LGPD brasileira. *REVISTA DO CEJUR/TJSC*, v. 8, p. 01-28, 2020.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big Data:* A Revolution that Will Transform How We Live, Work and Think. New York: Houghton Mifflin Harcourt, 2013.

MINISTÉRIO PÚBLICO FEDERAL. *Ofício nº 736/2020-SUBCAP/SEJUD/PGR*. 2020. Available on: <http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf>. Accessed on: 15 jun. 2022.

OECD. *The OECD Digital Government Framework: Six Dimensions of a Digital Government.* OECD, 2020.

SINGER, P.W.; FRIEDMAN, Allan. *Cybersecurity and Cyberwar:* What Everyone Needs to Know. Oxford: Oxford University Press, 2014.

SONICWALL. *2022 Sonicwall Cyber Threat Report*. Available on: <https://www.sonicwall.com/2022-cyber-threat-report/>. Accessed on: 15 jun. 2022.

UNITED NATIONS. Benchmarking E-government: A Global Perspective. 2002. Available on: <https://publicadministration.un.org/egovkb/portals/egovkb/documents/un/english.pdf>. Accessed on: 13 jun. 2022.

UNITED STATES OF AMERICA. *How to Protect your Networks from Ramsonware.* 2017. Available on: <https://www.justice.gov/criminal-ccips/file/872771/download>. Accessed on: 15 jun. 2022.

WALL, David. *Crime and the Internet.* New York: Routledge, 2001.

WENDT, E.; MASSENO, M. D. O Ransomware na Lei: Apontamentos Breves de Direito Português e Brasileiro. *REVISTA ELETRÔNICA DIREITO & TI* , v. 1, p. 01-13, 2017.

WEST, Darell M. E-Government and the Transformation of Service Delivery and Citizen Attitudes. *Public Administration Review*, v. 64, n. 1, p. 15-27, Jan./Fev. 2004.