FGV EBAPE

RAP
BRAZILIAN JOURNAL OF PUBLIC ADMINISTRATION

The use of cyberspace by the public administration in the COVID-19 pandemic: diagnosis and vulnerabilities

Breno Pauli Medeiros [1]
Luiz Rogério Franco Goldoni [1]
Eliezer Batista Junior [1]
Henrique Ribeiro da Rocha [1]

[1] Escola de Comando e Estado-Maior do Exército / Graduate Program in Military Sciences, Rio de Janeiro / RJ – Brazil

The COVID-19 pandemic, while demanding social distancing, imposes approximation and coordination of efforts by public and private entities through the Internet and digital services. This article analyzes the use and operationalization of cyberspace by the public administration in the fight against SARS-CoV-2. It presents a diagnosis of the vulnerabilities and challenges related to this growing operationalization. The public administration began to operationalize cyberspace more vigorously from the 1990s, with e-government. Inter-governmental and governmental coordination strategies imposed by the current situation would be impossible without the intensification of the operationalization of cyberspace by the public administration apparatus, which transposes unusual and even unprecedented practices and actions to the digital domain. Given its artificiality, cyberspace can only be operated by those with the means to do so. Cyber-democratization comes up against the digital divide. The current need for social distancing highlights technical and socio-economic challenges arising from the transposition of the public administration apparatus into cyberspace.
Keywords: COVID-19; administration; cyberspace; e-government.

O uso do ciberespaço pela administração pública na pandemia da COVID-19: diagnósticos e vulnerabilidadess

A pandemia da COVID-19, por demandar isolamento social, impõe aproximação e coordenação de esforços de entes públicos e privados por intermédio da Internet e dos serviços digitais. O artigo analisa o uso e a operacionalização do ciberespaço pela Administração Pública no combate ao SARS-CoV-2 e apresenta um diagnóstico das vulnerabilidades e desafios referentes a essa crescente operacionalização. A administração pública passou a operacionalizar o ciberespaço com mais afinco a partir da década de 1990, com o e-government. Estratégias de coordenação (inter)governamental impostas pela atual conjuntura seriam impossíveis sem a intensificação da operacionalização do ciberespaço pelo aparato administrativo público, que transpõe para o domínio digital práticas e ações pouco usuais ou mesmo inéditas. Dada sua artificialidade, o ciberespaço só pode ser operacionalizado por detentores de meios para tal. A "democratização" cibernética esbarra na exclusão digital. O atual isolamento social evidencia desafios técnicos e socioeconômicos decorrentes da transposição do aparato de administração pública para o ciberespaço.
Palavras-chave: COVID-19; administração; ciberespaço; *e-government*; exclusão digital.

El uso del ciberespacio por la administración pública en la pandemia de COVID-19: diagnóstico y vulnerabilidades

Por exigir aislamiento social, la pandemia de COVID-19 impone la aproximación y coordinación de esfuerzos de las entidades públicas y privadas por medio de Internet y de los servicios digitales. El artículo analiza el uso y operacional actual del ciberespacio por parte de la Administración Pública en la lucha contra el virus SARS-CoV-2 y presenta un diagnóstico de las vulnerabilidades y desafíos relacionados con esta creciente utilización operacional. La administración pública comenzó a usar el ciberespacio con mayor ahínco desde la década de 1990, momento en que surgió el e-government. Las estrategias de coordinación (inter)gubernamental impuestas por la situación actual serían imposibles sin la intensificación de la utilización operacional del ciberespacio por parte del aparato administrativo público, que transpone al dominio digital prácticas y acciones poco usuales o inéditas. Dada su artificialidad, el ciberespacio solo puede ser operado por quienes tienen los medios para hacerlo. La "democratización" cibernética choca con la exclusión digital. El aislamiento social actual destaca los desafíos técnicos y socioeconómicos derivados de la transposición del aparato de la administración pública al ciberespacio.
Palabras clave: COVID-19; administración; ciberespacio; *e-government*; exclusión digital.

DOI: http://dx.doi.org/10.1590/0034-761220200207x
ISSN: 1982-3134
Article received on April 24, 2020 and accepted on June 19, 2020.
[Translated version] Note: All quotes in English translated by this article's translator.
The article is part of the effort of the Science, Technology and Innovation in Defense: Cybernetics and National Defense research project, approved by the public notice 27/2018, and the Program to Support Teaching and Scientific and Technological Research in National Defense - PRÓ-DEFESA.
The authors would like to thank Prof. Dr. Karina Rodrigues and the contributions of the RAP reviewers for their critical reading and, of course, exempt them from any mistake that may have been stated in the article.

1. INTRODUCTION

Just as times of war and need drive innovation (Freeman & Soete, 2008), the social isolation imposed by COVID-19 prompts virtual solutions and platforms to assist in the digitalization of social life, driven by the political rhetoric of "War on COVID- 19" (Bennet & Berenson, 2020; Nienaber & Carrel, 2020). The need to transpose the administrative apparatus into cyberspace generates vulnerabilities and challenges rising from the dynamics and logic of the cyber domain that affect possible strategies to combat SARS-CoV-2. Based on paradigmatic cases, this article investigates administrative implications of the transposition of the state apparatus into cyberspace, a practice that started in the 1990s and that gained new contours with the advent of the current pandemic. The text presents a diagnosis of the vulnerabilities and challenges related to the increasing operationalization of cyberspace by the public administration.

Originally, the article demonstrates that when elaborating public policies, the digital divide must be considered a cyberspace vulnerability, alongside traditional technical problems. This work indicates that COVID-19 has highlighted the effects of digital exclusion and that it was not properly considered by the Brazilian authorities when elaborating policies to mitigate the effects of the pandemic.

Structurally, the article elucidates the transposition of the administrative apparatus into the cyber domain and the history of e-government. Thereafter, it examines the challenges arising from the nature of cyberspace regarding the virtualization of government administration. Finally, it analyzes the implications of such transposition with regard to technical and socioeconomic vulnerabilities, focusing on actions triggered by the new coronavirus.

2. TECHNICAL-SCIENTIFIC-INFORMATIONAL DOMAIN AND E-GOVERNMENT

The administrative virtualization is carried out through the technical-scientific-informational framework of globalization processes, which, according to Santos (2009), culminates in cyberspace. In this case, it is viewed as a domain of artificial human interaction, equipped with unique peculiarities (Cohen, 2007; Rattray, 2009; Kuehl, 2009; Medeiros, 2019), developed through the interconnection of physical layers (people and hardware) and digital layers (software and information) (Libicki, 2009; Ventre, 2012).

Given its artificiality, cyberspace only exists through its operation by individuals and institutions. Since access to technology is a limiting factor for cyberspace, the asymmetry of this access results in increasing socioeconomic disparities (Ruediger, 2003).

The most evident manifestation of cyberspace is the Internet. It was conceived during the Cold War by the American public administration as a network of computers interconnected between universities and research centers that then extended to the private sector, originating the universe known today (Castells, 2003). With the popularization of the Internet in the 1990s, portions of the public administration were progressively digitized in order to use Information and Communication Technologies (ICTs) as vectors of efficiency and agility for information flows between governments and their citizens (Chadwick & May, 2003).

At the beginning of the 21st century, ICTs were considered a mere extension of public administration, with potential benefits of speed, accessibility and convenience (Jaeger, 2002). The

most recent views, however, envision e-government as the combination of ICTs and the public administrative apparatus, with repercussions for areas that include improvement in public services, political frameworks, high quality and efficiency of government operations, civil engagement in democratic processes and institutional reforms (Dawes, 2008; Choi & Chandler, 2019).

E-government processes consist of capitalizing on the peculiarities of cyberspace by the public administration. In other words, the use of deterritorialization and interconnection of cyberspace (Medeiros, 2019) to reach connected portions of society, while computational speed and connections accelerate administrative processes. Hence, e-government can effectively be characterized as a facilitator of relations between State and society (Ruediger, 2003) through innovation, rationalization and adoption of management models that prioritize the provision of information and services to citizens. At the same time, e-government opens public administration to participation and social control and encourages the exercise of citizenship (Rampelotto et al., 2015) in accordance with the Brazilian constitutional principle of advertising, provided for in Article 37, caput, of the Federal Constitution (1988), and elucidated by Oliveira (1996).

Because it demands means for its operationalization such as electronic devices and infrastructure networks, e-government has the potential to be excluding, contrary to the intrinsic universality of the public good. Governments often resort to using mixed methods of online and face-to-face processes to mitigate the digital divide (Sampaio, 2016).

In a way, Brazil demonstrates its concern with digital inclusion by the paradigmatic change from the term "electronic government", which refers to the computerization of internal management processes, to the term "digital government", "whose focus centers on the relationship with society (citizen's view), in order to become more user friendly, more accessible and more efficient in offering services to citizens by means of digital technologies" (Digital Government, 2020).

The reality imposed by COVID-19 heightens the operationalization of cyberspace through the administrative apparatus, requiring that employees work remotely (Hern, 2020), banks prioritize digital services (Almeida, 2020), stores adapt to online shopping models (Meyersohn, 2020) and face-to-face education is modified so as to continue at a distance (Star, 2020). Regarding the existing socioeconomic differences, the responsibility for taking further measures of e-government and adapt their communications and practices to the virtual environment rests with the government apparatus. Nevertheless, social insertion in cyberspace is open to exploitation by a myriad of actors capable of operationalizing the logics and peculiarities of the digital universe according to their personal agendas.

3. THE OPERATIONALIZATION OF CYBERSPACE, TECHNICAL VULNERABILITIES AND CHALLENGES

In view of the digitalization of the administrative apparatus and the intensification of e-government, the conservation of political frameworks and the efficiency of government operations are essential focal points for public administration. Maintaining government communications and services in cyberspace is imperative in today's context of social isolation. However, as today's society resorts to cyberspace, in addition to aggravating social differences, this becomes a vector for the dissemination of disinformation and criminal attacks (Batista et al., 2020).

Part of the government's actions in the current pandemic scenario is aimed at combating "infodemics", i.e., the proliferation of false information about SARS-CoV-2 by social networks (Cinelli

et al., 2020). The Oswaldo Cruz Foundation (Fiocruz), for example, recently had to deny information falsely attributed to the entity (Fiocruz, 2020).

One way of spreading false news and cyber-attack is by sending malicious links via email or communication applications (apps). In Brazil, links and sites improperly attributed to health authorities give rise to scams, encouraging downloads of files that supposedly could contain data on SARS-CoV-2 (Mazzi, 2020). After opening the link or the file sent, the device becomes infected. Hence, the attacker can obtain various data from the victim, such as banking (Kaspersky, 2020).

Public administration is also challenged by ransomware: malicious software that encrypts the contents of a device and only releases them after a payment in cryptocurrencies. The university hospital in Brno, Czech Republic, testing center for the new coronavirus, has suffered a ransomware attack (Newman, 2020) where criminals gained access to the hospital system and encrypted the databases (Arbulu, 2020). The hospital did not pay the ransom and, as a result, activities were temporarily suspended and patients were relocated (Schwartz, 2020).

Another recent example of a ransomware attack occurred in the Champaign-Urbana Public Health District in Illinois, USA. As the institution had data backup, its services were not severely affected by the non-payment of ransom (Nichols, 2020). The billions of dollars of damage caused by the 2017 WannaCry ransomware left valuable lessons in digital literacy for administrative entities, among them, ensuring continuous system backups (Coughlin, 2017).

Public websites are targets for cybercriminals who seek advantages by creating clones that simulate official websites. Recently, the US Department of Health and Human Services suffered a DDoS (Distributed Deny of Service) attack that aimed to make the institution's website unavailable. As a result, people lost the official reference and had to search for other sources of data on the pandemic that might not be "legitimate", or be infected with codes to "steal" user data (Morrison, 2020).

It is worth noticing that the digitally excluded are already permanently "denied access" to electronic information systems. Thus, in practice, digital exclusion has social similarities to one of the "traditional" technical vulnerabilities of cyberspace.

4. TRANSPOSING THE SOCIAL ENVIRONMENT TO CYBERSPACE: INNOVATIONS, CHALLENGES, VULNERABILITIES AND LESSONS FOR PUBLIC ADMINISTRATION

The increasing operationalization of cyberspace by the public administration driven by COVID-19 gives rise to innovations, challenges, vulnerabilities and lessons.

In recent weeks, television newscasts have been showing virtual meetings of national authorities, in which videoconferencing platforms are used (Behnke, 2020; Matsuura, 2020; O Estado de S. Paulo, 2020). In order to respond to the demands imposed by the pandemic, public and private entities have transferred activities to cyberspace. However, the use of this alternative for professional and educational activities and for the coordination of public policies reveals technical and social vulnerabilities of cyberspace. According to Sampaio (2016), while it is necessary to admit the advantages of society's participation in cyberspace, it is necessary to recognize the existing limitations.

The transposition of face-to-face work activities into cyberspace creates a type of social exclusion, since only part of society is able to maintain its employment and income. To mitigate the socioeconomic effects of the pandemic, the Federal Government has launched an emergency aid program (Decree

10.316, of April 7, 2020) for the universe of citizens who have drastically lost their livelihood. This action brings to light the technical and social vulnerabilities of cyberspace.

In order to comply with the Government's determinations, the Caixa Econômica Federal (CEF) launched the "Caixa Auxílio Emergencial" website and app by which citizens, covered by the previously mentioned Decree, can request emergency aid. The bank provided a call center to clarify doubts, albeit accessing it poses problems (UOL, 2020). The way it was designed to work is that the 'Bolsa Família' beneficiaries, who are already registered at the CEF, would automatically receive the extra assistance through a deposit made in the same bank account as the regular government program.

Other interested citizens, who fulfill the criteria of the Decree, must register on the CEF website or app to receive emergency assistance, provided they are holders of a regularized Cadastro de Pessoa Física (CPF). A major problem since the many "invisible" Brazilians do not have a CPF (Kerber, 2020). With this requirement, plus the lack of information, technical problems and the precariousness of non-face-to-face information channels, the system did not work as expected and many took to the streets outside the CEFs, forming lines and agglomerations, forcing them to go against the recommendations to combat the pandemic (Lara, 2020).

When the online registration is completed, the interested party awaits analysis by Dataprev (Larghi, 2020). Once approved, the beneficiary should receive the deposit in a CEF or Banco do Brasil account. Those who do not have an account with these banks receive a code to access the Social Savings Account, managed by the "Caixa TEM" software (CEF, 2020). This last alternative presents another problem: the code is only valid for two hours (Branco, 2020), which makes it difficult for those with mobility or internet access problems and / or those who need to use borrowed devices to access the CEF app or website. Technical problems, delays and misinformation again took many people back to the streets unnecessarily (G1, 2020).

The main problems faced by the population are not related to the design of the CEF systems itself, but in the requirements for their use. Initially, data from 2019 show that 6.8% of the Brazilian population over 15 years of age is composed of illiterates (Gazeta do Povo, 2020). These, consequently, are excluded from the digital universe. Inequality of access is another problem: 50% of the population in rural areas and peripheral regions and 16.2% in urban areas do not have access to the Internet (Brazilian Institute of Geography and Statistics [IBGE], 2018); altogether, only 70.07% of the population is active on the Internet (Internet World Stats [IWS], 2020c). In addition, those interested in the aid could still suffer from problems related to the rules imposed on registration (GooglePlay, 2020) and / or have old devices that are unable to install the software.

The digital divide is also present in education during the pandemic. According to data from the National High School Examination (Enem) board of 2018, 34% of students in the public school system did not have access to the Internet and 55% did not have a computer (Saldaña et al., 2020). Despite these numbers, after schools were closed across the nation due to COVID-19, the Ministry of Education (MEC) authorized the use of ICTs as an alternative for continuing education (MEC, 2020).

It took strong pressure from the society for the Government to agree to postpone this year's Enem exams (Betim, 2020). When it comes to inequalities, the Minister of Education allegedly stated in a meeting with senators, "Enem was not designed to correct injustices" (Lemos, 2020). Only time will tell whether the historic inequality in the performance of students from public and private schools in the Enem (G1, 2016) will be exacerbated by the current pandemic.

Both classes and work activities were transferred to the virtual environment via videoconferencing platforms. The operationalization of cyberspace through these tools, including by the public administration, raises questions about privacy and security.

When analyzing the videoconferencing app, Citizen Lab[1] pointed out that calls go through the company's central server so that it can have access to communications, files and videos shared through the platform. In addition, the group identified that encryption keys were transmitted by servers located in countries other than those that host the company (Marczak & Scott-Railton, 2020). These findings gain relevance because Brazilian public entities use the platform in question for work meetings. Therefore, potentially sensitive data could be accessed by private entities located outside the national territory. It is important to emphasize that no communication app is 100% secure and that similar problems can also occur with the storage of information and files "in the cloud", which are actually physical servers located in different countries. Furthermore, the Snowden case has already exposed vulnerabilities related to the traffic of digital information (Greenwald & MacAskill, 2013).

Another vulnerability of video call apps arises from the expedient the cyber-attackers use to enter public meetings or discover the identification code of a private meeting. After entering, they can listen to the communications or try to end meetings or classes, embarrassing participants with racist and / or pornographic messages (O'Flaherty, 2020). Such an issue becomes more prominent as users post photos of meetings on social networks, displaying the call identification code, such as the British Prime Minister Boris Johnson did at the end of March (Corera, 2020).

Despite the aforementioned vulnerabilities, as shown on television news, Brazilian institutions such as the Federal Supreme Court, the Chamber of Deputies and the Federal Senate continue to use videoconferencing platforms to hold ordinary sessions and voting (Brígido, 2020). It is noteworthy that the trials are transmitted over the Internet and TV Justiça, and that no vote in Congress was secret (Ladeira, 2020).

The Snowden case left important lessons. With regard to the initiatives promoted by the Brazilian Government in cyberspace, the topics "budget control" (Normative Instruction No. 01, 2019), "information security" (National Information Security Policy, Decree No. 9.637, 2018) and "confidentiality and transparency" (General Data Protection Law - LGPD) stand out.

5. FINAL CONSIDERATIONS

The operationalization of cyberspace by the public administration faces challenges inherent to the cyber domain. It is imperative that public sectors consider the technical and social vulnerabilities of that environment and take measures to combat them.

Running training courses and developing platforms and personal solutions should be part of broader digital inclusion measures. This challenge is not unprecedented; it synthesizes historical processes of social exclusion.

The problems related to education through digital platforms and the difficulties in accessing the Federal Government's emergency benefit leave significant lessons for the public administration:

[1] Interdisciplinary group based at the University of Toronto, specialized in research and development of policies related to ICTs, human rights and security (The Citizen Lab, 2020).

digital exclusion is a nefarious face of the operationalization of cyberspace. As seen, only 70% of the Brazilian population is active on the Internet (Pop.AI).

Regarding emergency aid, the experiences of countries with digital and / or social reality similar to Brazil offer little as an alternative. According to Ozili (2020), in the African continent, only Nigeria (Pop.AI 61.2%, IWS, 2020a) and Malawi (Pop.AI 14.2%, IWS, 2020a) have emergency income assistance programs. The Nigerian government distributes approximately USD 52.00 to families registered with the 'National Social Register of Poor and Vulnerable Households' via bank transfer (Human Rights Watch [HRW], 2020). India (Pop.AI 40.6%, IWS, 2020d) adopts a similar model, distributing USD 6.60 to women registered in the *Jan Dhan* Program, through deposit in bank accounts (The Economic Times, 2020). Both programs are similar to the transfer that takes place in Brazil for Bolsa Família beneficiaries. Argentina, which has 93% of Pop.AI (IWS, 2020c), adopted measures similar to the Brazilian one: fully online registration of beneficiaries and direct payment in bank accounts (Argentina, 2020).

Brazil could have adopted mixed solutions practiced by States equally affected by the pandemic, as summarized in the following box:

BOX 1 DISTRIBUTION OF EMERGENCY AID

Country	Population active on Internet (Pop.AI) (a)	Registration	Aid Payment
USA	95,6%	Automatic, based on data from the Internal Revenue Service (IRS) statement (b).	The IRS decides whether the beneficiary will receive the subsidy by depositing in a checking account or by making a nominal check using the postal service (b).
UK	94,9%	Through the government website or at the workplace (c).	Credit in bank account or through the worker's company payroll (c).
Spain	92,5%	Demands centralized in companies responsible for requesting emergency aid from the government (d).	Directly in the payroll from companies to workers (d).
Italy	92,5%	Filling in request forms on the Instituto *Nazionale Previdenza Sociale's* website (e).	Beneficiary's bank account. If they do not have an account, the beneficiary chooses an agency to collect the money (e).

Source: Elaborated by the authors, based on (a) IWS (2020b, 2020c); (b) IRS (2020); (c) The United Kingdom (UK, 2020); (d) Spain (2020); (e) Italy (2020).

Despite having a high percentage of Pop.AI, none of the countries listed relied so much on cyberspace for the payment of emergency aid as Brazil. Registration via the workplace (UK and Spain), Federal Revenue (USA) or Social Security (Italy) database, and distribution via the Post Office (USA), payroll (UK and Spain) or deposit in the beneficiary's preferred account (USA, UK and Italy)

could all minimize the problems faced by many Brazilians. Having said that, social issues, such as informality, would hinder the full reproduction of these measures in the country.

The vulnerabilities of cyberspace for public administration are technical and social; and countries with high social inequality are more difficult to remedy. Although it is impossible to predict the world after social isolation, comparable to combating this contagious disease, it is possible to see that a greater exposure of the administrative apparatus to cyber reality engenders practices and habits that will lead to the creation of "cyber antibodies". As a result, government sectors would not only become more aware of the vulnerabilities emanating from the cyber domain, but could also counter back and avoid them in their daily work.

REFERENCES

Almeida, M. (2020, March 24). Bancos restringem atendimento e têm horários diferenciados. *EXAME*. Retrieved from https://exame.abril.com.br/seu-dinheiro/bancos-restringem-atendimento-e-tem-horarios-diferenciados/

Arbulu, R. (2020, March 16). Ciberataque faz hospital que tratava pacientes do coronavírus fechar as portas. *Canal Tech*. Retrieved from https://canaltech.com.br/seguranca/ciberataque-faz-hospital-que-tratava-pacientes-do-coronavirus-fechar-as-portas-161881/

Argentina. (2020). *Ingreso familiar de emergencia*. Buenos Aires, AR: Autor. Retrieved from https://www.argentina.gob.ar/economia/medidas-economicas-COVID19/ingresofamiliardeemergencia

Batista, E., Jr., Medeiros, B., Rocha, H., & Goldoni, L. (2020). *Vetores Cibernéticos da Pandemia de Covid-19*. Rio de Janeiro, RJ: Observatório Militar da Praia Vermelha. Retrieved from http://ompv.eceme.eb.mil.br/masterpage_assunto.php?id=194

Behnke, E. (2020, April 13). Bolsonaro acompanha videoconferência das Forças Armadas sobre covid-19. *Estadão*. Retrieved from https://politica.estadao.com.br/noticias/geral,bolsonaro-acompanha-videoconferencia-das-forcas-armadas-sobre-covid-19,70003269846

Bennet, B., & Berenson, T. (2020, March 19). As Coronavirus Spreads, Trump Refashions Himself as a Wartime President. *Time*. Retrieved from https://time.com/5806657/donald-trump-coronavirus-war-china/

Betim, F. (2020). Governo adia Enem após pressão que trouxe à tona o fosso entre ensino público e privado. *El País Brasil*. Retrieved from https://brasil.elpais.com/sociedade/2020-05-20/governo-adia-enem-apos-pressao-que-trouxe-a-tona-o-fosso-entre-ensino-publico-e-privado.html

Branco, A. (2020, June 02). Beneficiário tem até 2 horas para sacar o auxílio emergencial na Caixa após gerar código. *Agora São Paulo*. Retrieved from https://agora.folha.uol.com.br/grana/2020/04/beneficiario-tem-ate-2-horas-para-sacar-o-auxilio-emergencial-na-caixa-apos-gerar-codigo.shtml

Brígido, Carolina (2020, March 30). STF vai realizar primeira sessão por videoconferência dia 15. *O Globo*. Retrieved from https://oglobo.globo.com/brasil/stf-vai-realizar-primeira-sessao-por-videoconferencia-dia-15-24339078

Caixa Econômica Federal. (2020). *Auxílio Emergencial*. Retrieved from http://www.caixa.gov.br/auxilio/Paginas/default2.aspx

Castells, M. (2003). *A Galáxia da Internet*. Rio de Janeiro, RJ: Jorge Zahar.

Chadwick, A., & May, C. (2003, March 21). Interaction between states and citizens in the age of the internet: "e-government" in the United States, Britain, and the European Union. *Governance, 16*(2), 271-300.

Choi, T., & Chandler, S. M. (2020, January). Knowledge vacuum: An organizational learning dynamic of how e-government innovations fail. *Government Information Quarterly, 37*(1). Retrieved from https://www.sciencedirect.com/science/article/pii/S0740624X17301296

Cinelli, M., Quattrociocchi, W., Galeazzi, A., Valensise, C.M., Brugnoli, E., Schmidt, A.L., Zola, P., Zollo, F., & Scala, A. (2020). The COVID-19 Social Media Infodemic. *ArXiv, abs/2003.05004v1*, 1-18.

Cohen, J. E. (2007). Cyberspace as/and space. *Columbia Law Review, 107*(1), 210-256.

Constituição da República Federativa do Brasil, de 5 de outubro de 1988. (1988). Brasília, DF.

Coughlin, T. (2017, May 14). WannaCry ransomware demonstrates the value of better security and backups. *Forbes*. Retrieved from https://www.forbes.com/sites/tomcoughlin/2017/05/14/wannacry-ransomware-demonstrations-the-value-of-better-security-and-backups/#2532d2d170b8

Corera, G. (2020, April 01). UK government defends PM's use of Zoom. *BBC News*. Retrieved from https://www.bbc.com/news/technology-52126534

Dawes, S. S. (2008). The evolution and continuing challenges of e-governance. *Public Administration Review*, *68*(s1), s86-s102.

Decreto n. 9.637, de 26 de dezembro de 2018. (2018). Dispõe sobre a governança da segurança da informação e institui a Política Nacional de Segurança da Informação. Brasília, DF.

Decreto nº 10.316, de 07 de abril de 2020. (2020). Regulamenta a Lei nº 13.982, de 2 de abril de

2020, que estabelece medidas excepcionais de proteção a serem adotadas durante o período de enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus (COVID-19). Brasília, DF.

Espanha. (2020). *Ministerio del trabajo y economia social. Preguntas frecuentes: información sobre la presentación de expedientes de regulación temporal de empleo por fuerza mayor por causa del COVID-19 en el Ministerio Trabajo y Economía Social*. Madrid, España: Ministerio de Trabajo y Economía Social. Retrieved from http://www.mitramiss.gob.es/ficheros/ministerio/contacto_ministerio/FAQ_ERTES_derivados_coronavirus.pdf

Fundação Oswaldo Cruz. (2019, March 17) *Fiocruz esclarece informações falsas*. Retrieved from https://portal.fiocruz.br/noticia/fiocruz-esclarece-informacoes-falsas

Freeman, C., & Soete, L. (2008). *A Economia da inovação industrial*. Campinas, SP: Editora da UNICAMP.

G1. (2016, October 04). *Enem mostra desigualdade entre ensino público e privado.* Retrieved from http://g1.globo.com/jornal-nacional/noticia/2016/10/enem-mostra-desigualdade-entre-ensino-publico-e-privado.html

G1. (2020, April 13). *Agências da Caixa registram filas e aglomerações no Grande Recife*. Retrieved from https://g1.globo.com/pe/pernambuco/noticia/2020/04/13/agencias-da-caixa-registram-filas-e-aglomeracoes-no-grande-recife.ghtml

GaúchaZH. (2020, March 24). *Famílias afetadas economicamente pela quarentena na Argentina receberão auxílio do governo*. Retrieved from https://gauchazh.clicrbs.com.br/mundo/noticia/2020/03/familias-afetadas-economicamente-pela-quarentena-na-argentina-receberao-auxilio-do-governo-ck869qo4u07ep01pq5prbwgdh.html

Gazeta do Povo. (2020). *Taxa de analfabetismo no Brasil | Infográficos | Gazeta do Povo*. Retrieved from https://infograficos.gazetadopovo.com.br/educacao/taxa-de-analfabetismo-no-brasil/

Greenwald, G., & MacAskill, E. (2013, June 06). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

GooglePlay (2020). Caixa | Auxílio Emergencial. Retrieved from https://play.google.com/store/apps/details?id=br.gov.caixa.auxilio&hl=pt_BR&showAllReviews=true

Governo Digital. (2020). *Do Eletrônico ao Digital*. Retrieved from https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital

Hern, A. (2020, March 13). Covid-19 could cause permanent shift towards home working. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2020/mar/13/covid-19-could-cause-permanent-shift-towards-home-working

Human Rights Watch. (2020, April 14). *Nigeria: Protect Most Vulnerable in COVID-19 Response*. Retrieved from https://www.hrw.org/news/2020/04/14/nigeria-protect-most-vulnerable-covid-19-response

Instituto Brasileiro de Geografia e Estatistica. (2018). *Pesquisa Nacional por Amostra de Domicílios Contínua - PNAD Contínua*. Rio de Janeiro, RJ: Autor. Retrieved from https://www.ibge.gov.br/estatisticas/sociais/trabalho/17270-pnad-continua.html?=&t=downloads

Instrução Normativa n. 01, de 04 de abril de 2019. (2019). Dispõe sobre processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. Brasília, DF.

Internal Revenue Service. (2020, April 01). *Economic impact payments: What you need to know*. Retrieved from_https://www.irs.gov/newsroom/economic-impact-payments-what-you-need-to-know

Internet World Stats (2020a). *Internet Penetration in Africa*. Retrieved from https://www.internetworldstats.com/stats1.htm

Internet World Stats (2020b). *Internet Stats and Facebook Usage in Europe: June 2019 Statistics*. Retrieved from https://www.internetworldstats.com/stats4.htm#europe

Internet World Stats (2020c). *Internet Usage, Facebook Subscribers and Population Statistics for all the Americas World Region Countries: June 30, 2019*. Retrieved from https://www.internetworldstats.com/stats2.htm

Internet World Stats (2020d). *Internet Usage in Asia*. Retrieved from https://www.internetworldstats.com/stats3.htm

Itália. *Decreto-legge 19 maggio 2020, n. 34.* (2020, May 19). Misure urgenti in matéria di salute, sostegno al lavoro e all'economia, nonche' di politiche sociali connesse all' emergenza epidemiologica da COVID-19. Roma, Italia. Retrieved from_https://www.lavoro.gov.it/documenti-e-norme/normative/Documents/2020/D-L-19-maggio-2020.pdf

Jaeger, P. T. (2002). Constitutional principles and e-government: An opinion about possible effects of federalism and the separation of powers on e-government policies. *Government Information Quarterly*, *19*(4), 357-368.

Kaspersky (2020, February 13). *Coronavírus chega ao Brasil: Kaspersky identifica disseminação de malware usando a epidemia como isca.* Retrieved from https://www.kaspersky.com.br/about/press-releases/2020_coronavirus-chega-ao-brasi

Kerber, D. (2020, April 08). O que significa 'CPF em situação inválida' no auxílio emergencial? *Estadão*. Retrieved from https://economia.estadao.com.br/noticias/geral,o-que-significa-cpf-em-situacao-invalida-no-auxilio-emergencial,70003264940

Kuehl, D. T. (2009). *From Cyberspace to Cyberpower: Defining the Problem*. Washington, DC: National Defense University Press.

Ladeira, P. (2020, March 18). Com ministros em idade de risco, Supremo supera resistências e prepara sessão por videoconferência. *Folha de S. Paulo*. Retrieved from https://www1.folha.uol.com.br/poder/2020/04/com-ministros-em-idade-de-risco-supremo-supera-resistencias-e-prepara-sessao-por-videoconferencia.shtml

Lara, M. (2020, April 15). Pará alega aglomerações e pede fim da exigência de regularização de CPF para auxílio emergencial. *Estadão*. Retrieved from https://politica.estadao.com.br/noticias/geral,para-alega-aglomeracoes-e-pede-fim-da-exigencia-de-regularizacao-de-cpf-para-auxilio-emergencial,70003271592

Larghi, N. (2020, April 22). Caixa possui dois aplicativos para auxílio emergencial; entenda a diferença. *Valor Investe*. Retrieved from https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/04/22/caixa-possui-dois-aplicativos-para-auxilio-emergencial-entenda-a-diferenca.ghtml

Lei n. 13.709, de 14 de agosto de 2018. (2018). Dispõe sobre Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF.

Lemos, I. (2020). Em reunião com senadores, Weintraub diz que Enem não foi feito para corrigir injustiças. *Folha de S. Paulo*. Retrieved from https://www1.folha.uol.com.br/educacao/2020/05/em-reuniao-com-senadores-weintraub-diz-que-enem-nao-foi-feito-para-corrigir-injusticas.shtml?aff_source=56d95533a8284936a374e3a6da3d7996

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: Rand Corporation.

Marczak, B., & Scott-Railton, J. (2020, April 03). Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

Matsuura, S. (2020, April 07). Populares com a quarentena, aplicativos para reuniões virtuais viram alvo de hackers. *O Globo*. Retrieved from https://oglobo.globo.com/economia/tecnologia/populares-com-quarentena-aplicativos-para-reunioes-virtuais-viram-alvo-de-hackers-24357276

Mazzi, C. (2020, March 30). Como reconhecer e fugir dos golpes na internet sobre coronavírus. *O Globo*. Retrieved from https://oglobo.globo.com/sociedade/coronavirus-servico/como-reconhecer-fugir-dos-golpes-na-internet-sobre-coronavirus-24337658

Medeiros, B. (2019). *Ciberespaço e Relações Internacionais: Rumo a Construção de um novo Paradigma?* (Master Thesis). Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, RJ. Retrieved from http://bdex.eb.mil.br/jspui/bitstream/123456789/4175/1/MO%205928.pdf

Meyersohn, N. (2020, March 19). Coronavirus will change the grocery industry forever. *CNN Business*. Retrieved from https://edition.cnn.com/2020/03/19/business/grocery-shopping-online-coronavirus/index.html

Ministério da Educação. (2020, 18 de março). *MEC autoriza ensino a distância em cursos presenciais*.

Retrieved from http://portal.mec.gov.br/component/content/article?id=86441

Morrison, S. (2020, March 16). What we know about the Health Department website cyberattack. *Vox*. Retrieved from https://www.vox.com/recode/2020/3/16/21181825/health-human-services-coronavirus-website-ddos-cyber-attack

Newman, L. H. (2020, March 19). Coronavirus Sets the Stage for Hacking Mayhem. *Wired*. Retrieved from https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/

Nichols, S. (2020, Março 12). Fresh virus misery for Illinois: Public health agency taken down by… web ransomware. Great timing, scumbags. *The Register*. Retrieved from https://www.theregister.com/2020/03/12/ransomware_illinois_health/

Nienaber, M., & Carrel, P. (2020, March 18). Merkel tells Germans: Fighting virus demands war-time solidarity. *Reuters*. Retrieved from https://www.reuters.com/article/us-health-coronavirus-germany/merkel-tells-germans-fighting-virus-demands-war-time-solidarity-idUSKBN2153GX

O Estado de S. Paulo. (2020, April 14). *Trump convoca líderes do G7 para videoconferência sobre pandemia*. Retrieved from https://internacional.estadao.com.br/noticias/geral,trump-convoca-lideres-do-g7-para-videoconferencia-sobre-pandemia,70003270865

O'Flaherty, K. (2020, March 27). Beware Zoom Users: Here's How People Can 'Zoom-Bomb' Your Chat. Forbes. Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2020/03/27/beware-zoom-users-heres-how-people-can-zoom-bomb-your-chat/#1124167a618e

Oliveira, F. (1996). A Administração Pública na Constituição de 1988 (2ª Parte). *Revista De Direito Administrativo*, *206*, 43-87. Retrieved from http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/46856/45829

Ozili, P. (2020). COVID-19 in Africa: socio-economic impact, policy response and opportunities, *International Journal of Sociology and Social Policy*, *ahead-of-print*, 1-24. Retrieved from https://doi.org/10.1108/IJSSP-05-2020-0171

Rattray, G. J. (2009). An environmental approach to understanding cyberpower. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (Chap. 10, pp. 253-274). Washington, DC: National Defense University Press.

Rampelotto, A., Löbler, M. L., & Visentini, M. S. (2015). Avaliação do sítio da Receita Federal do Brasil como medida da efetividade do governo eletrônico para o cidadão. *Revista de Administração Pública*, *49*(4), 959-984.

Ruediger, M. A. (2003). Governança democrática na era da informação. *Revista de Administração Pública*, *37*(6), 1257-1280.

Saldaña, P., Mariani, D., Yukari, D., & Sant'Anna, E. (2020, May 28). Internet não chega a 34% dos alunos da rede pública que fizeram Enem. *Folha S. de Paulo*. Retrieved from https://www1.folha.uol.com.br/cotidiano/2020/05/internet-nao-chega-a-34-dos-alunos-da-rede-publica-que-fizeram-enem.shtml?aff_source=56d95533a8284936a374e3a6da3d7996

Santos, M. (2009). *A Natureza do Espaço* (4a ed.). São Paulo, SP: Edusp.

Schwartz, M. (2020, March 16). COVID-19 Complication: Ransomware Keeps Hitting Healthcare. Bankinfosecurity. *Bank Info Security*. Retrieved from https://www.bankinfosecurity.com/covid-19-complication-ransomware-keeps-hitting-hospitals-a-13941

Sampaio, R. C. (2016). e-Orçamentos Participativos como iniciativas de e-solicitação: uma prospecção dos principais casos e reflexões sobre a e-Participação. *Revista de Administração Pública*, *50*(6), 937-958.

Star, M. (2020, March 20). Online Education Becomes Teacher's Pet In COVID-19 Crisis. *Forbes*. Retrieved from https://www.forbes.com/sites/mergermarket/2020/03/20/online-education-becomes-teachers-pet-in-covid-19-crisis/#46c07aec1aa1

The Citizen Lab. (2020). *About the Citizen Lab - The Citizen Lab*. Retrieved from https://citizenlab.ca/about/

The Economic Times. (2020). *Covid-19: Govt to transfer financial assistance only through DBT mechanism*. Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/covid-19-govt-to-transfer-financial-assistance-only-through-dbt-mechanism/articleshow/75185835.cms

The United Kingdom. (2020). *Universal Credit*. London, UK: Autor. Retrieved from_https://www.gov.uk/universal-credit/how-to-claim

UOL. (2020, April 22). *Telefone 111 da Caixa, para auxílio emergencial, continua tendo problemas*. Retrieved from https://economia.uol.com.br/noticias/redacao/2020/04/22/telefone-111-da-caixa-para-auxilio-emergencial-continua-tendo-problemas.htm

Ventre, D. (2012). Ciberguerra. In Academia General Militar. In La Academia General Militar, & Universidad de Zaragoza (Eds.), *Seguridad global y potencias emergentes en un mundo multipolar*. Madrid, España: Autor. Retrieved from https://publicaciones.defensa.gob.es/seguridad-global-y-potencias-emergentes-en-un-mundo-multipolar-4267.html

Breno Pauli Medeiros

https://orcid.org/0000-0002-9839-5252
Ph.D. candidate and MSc. in Military Sciences in the Graduate Program in Military Sciences of the Brazilian Army Command and General Staff School. E-mail: breno.pauli@gmail.com

Luiz Rogério Franco Goldoni

https://orcid.org/0000-0001-5257-9470
Ph.D. in Political Science and Professor of the Graduate Program in Military Sciences of the Brazilian Army Command and General Staff School. E-mail: luizrfgoldoni@gmail.com

Eliezer de Souza Batista Junior

https://orcid.org/0000-0003-4954-2153
Ph.D. candidate in Military Sciences in the Graduate Program in Military Sciences of the Brazilian Army Command and General Staff School; Major of the Brazilian Army. E-mail: junhor82@gmail.com

Henrique Ribeiro da Rocha

https://orcid.org/0000-0002-6286-6219
M.Sc. candidate in Military Sciences in the Graduate Program in Military Sciences of the Brazilian Army Command and General Staff School. E-mail: riques.ribeiro@gmail.com