X Encontro Brasileiro de Administração Pública.
ISSN: 2594-5688
secretaria@sbap.org.br
Sociedade Brasileira de Administração Pública

A segurança está offline: a Subfunção Informação e Inteligência e os crimes cibernéticos nos estados brasileiros

Laura Angélica Moreira Silva, João Paulo Moreira Silva

[ARTIGO] GT 9 Planejamento, Controle e Finanças no Setor Público

A segurança está offline: a Subfunção Informação e Inteligência e os crimes cibernéticos nos estados brasileiros

Resumo

Este estudo analisa as despesas governamentais alocadas na Subfunção 183 - Informação e Inteligência, registradas pelas 27 unidades federativas, e detalha os tipos de crimes cibernéticos no Brasil. Investimentos em inteligência, em nível estadual, são uma premissa fundamental para a elucidação dos crimes que ocorrem no ambiente virtual. A análise ocorre a partir do ano de 2007, marco da telefonia móvel conectada a internet. Apesar do crescente número de crimes cibernéticos, o orçamento para a inteligência não é transparente e não necessariamente volumoso. Os resultados também apresentam cenário complexo para a gestão da segurança cibernética: a alocação de recursos é insignificante, tendo em vista a quantidade significativa de crimes registrados.

Palavras-chave

Crimes cibernéticos. Orçamento público. Investigação. Inteligência

1 INTRODUÇÃO

O ambiente puramente virtual adquire conexões cada vez maiores com o mundo físico (STALANS; FINN, 2016). Essa nova dinâmica é responsável por expandir o número de crimes cibernéticos (CC), atualmente um tema crítico em segurança pública (SARRE; LAU; CHANG, 2018; WEISS; JANKAUSKAS, 2019).

Os CC são de difícil definição (SARRE; LAU; CHANG, 2018; WALL, 1997) e mantêm comportamento distinto dos crimes comuns, perpetrados no mundo real: são extramuros ou transfronteiriços e criminosos beneficiam-se do anonimato e da facilidade para exercer o delito (STALANS; FINN, 2016; WALL, 1999). Devido a sua característica local e transnacional concomitante, países alvos ou "exportadores" de CC se especializam em crimes ou alvo particulares (KSHETRI, 2010) tornando-se perigos globais (HALL et al., 2021). Soma-se às características citadas um processo de vitimização ímpar, em que os indivíduos sequer tomam conhecimento de tornarem-se vítimas (KSHETRI, 2010; WALL, 1997), o que impacta em sua notificação pelos agentes públicos.

O Brasil é reconhecidamente território onde criminosos executam CC, principalmente disseminação de links maliciosos (KSHETRI, 2010), tornando-se um país "exportador" dos referidos crimes (KASPERSKY, 2020). As polícias, por sua vez, são responsáveis por dissuadir e reduzir crimes, incluso os cibernéticos. Dessa forma, em um país de abrangência continental, a pergunta que se apresenta é: uma vez necessária a atuação de inteligência para a investigação e solução de crimes cibernéticos, há orçamento público, em âmbito estadual, disponível para tal?

Para compreender o cenário apresentado, dois esforços foram realizados. Primeiro, buscou-se delimitar o conceito e as tipologias de CC executados (DINIZ; MUGGAH; GLENNY, 2014), optando-se pelos *cyber-trespass* e *cyber-theft* (WALL, 1997), tal qual acesso à dados pessoais e fraudes financeiras no ambiente virtual. Posteriormente, levantou-se a despesa alocada na Subfunção 183 - Informação e Inteligência entre os anos 2007 a 2018, além do quantitativo de CC ocorridos no país. Para tanto, as justificativas para observar esses dados perpassam as extensas possibilidades de atuação de criminosos cibernéticos no país; a concorrência do orçamento da polícia investigativa com outros crimes e pela classificação orçamentária nacional, pouco transparente e funcional (SILVA, 2020). Utilizando-se o advento do iPhone como marco da telefonia móvel conectada a internet, a série histórica para os gastos públicos analisada considera 2007 como ano-base.

A partir das análises, os CC mostraram-se numerosos, com destaque para os estados da região Sudeste. A região Nordeste, segunda região com maior concentração de casos de CC, registra o menor volume de recursos para combatê-los em nível estadual. No geral, os investimentos em Informação e Inteligência mostraram-se difusos e de difícil mensuração. A partir do ano de 2013, houve aumento na ocorrência de estados que passaram a não vincular recursos orçamentários identificados como Informação e Inteligência, ou realizaram lançamentos iguais a zero, o que dificulta a transparência e torna o controle e prevenção ainda mais desafiador.

2 CRIMES CIBERNÉTICOS: DA DEFINIÇÃO AO POLICIAMENTO

Crimes cibernéticos são reconhecidos como um conjunto de ações criminosas que utilizam computador ou redes digitais como ferramentas, alvo ou locais da ação (DINIZ; MUGGAH; GLENNY, 2014), podendo ser economicamente motivadas (HALL et al., 2021) ou não (WALL, 1999). Enquanto uma definição inequívoca para CC ainda está por surgir (SARRE; LAU; CHANG, 2018), há pouca discussão sobre a disseminação da internet e sua maior incidência (DINIZ; MUGGAH; GLENNY, 2014; STALANS; FINN, 2016). A preocupação acerca da amplitude dos CC se justifica também pela dificuldade em se rastrear, mapear e punir tais crimes (HALL et al., 2021; SARRE; LAU; CHANG, 2018), assim como pela ubiquidade das tecnologias (STALANS; FINN, 2016).

Wall (1997) destaca uma tipologia ampla que abarca 4 categorias de CC: (i) *cyber-trespass*, como invasão de espaços delimitados no ambiente virtual; (ii) *cyber-theft*, ou formas de apropriação naturais do ambiente virtual; (iii) *cyber-obscenity* ou a troca de

materiais obscenos online e, por fim, (iv) *cyber-violence*, atividades violentas no ambiente virtual, como práticas de ódio. Os CC comumente transitam entre as categorias e subcategorias que os compõem. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) (CERT.BR, 2020), grupo que busca mapear incidentes que afetam a segurança digital em nível nacional, computa mais de 6 milhões de incidentes ocorridos entre 2007 e 2018 no Brasil, incluindo crimes cibernéticos de maior e menor complexidade (DINIZ; MUGGAH; GLENNY, 2014).

Entretanto, a ausência de barreiras físicas, a possibilidade em conferir anonimato aos criminosos, a facilidade para exercer o delito (STALANS; FINN, 2016; WALL, 1999) e um processo de vitimização único – em que um indivíduo pode sequer reconhecer ter se tornado vítima (SARRE; LAU; CHANG, 2018) – impõem inúmeros desafios às forças de segurança. Tais características tornam o estado reconhecidamente incapaz de prover segurança no ambiente virtual (WEISS; JANKAUSKAS, 2019), e a aplicação da lei "quase impossível" (SARRE et al., 2018, p.516), possibilitando, assim, considerável subnotificação.

A popularização e constante adaptação dos meios para articulação dos CC aumentam as dificuldades das polícias (DAVIS, 2012; KSHETRI, 2010), impactando diretamente nas investigações, incluindo as delegacias especializadas em crimes cibernéticos (HARKIN; WHELAN; CHANG, 2018), presentes também em diversos estados brasileiros. Em relação às equipes policiais que combatem crimes cibernéticos, dificuldades são mencionadas em relação ao treinamento das forças policiais (WILLITS; NOWACKI, 2016), falta de reconhecimento por superiores hierárquicos (HARKIN; WHELAN; CHANG, 2018), falta de clareza na legislação pertinente e até mesmo falta de equipamentos necessários para investigação de crimes cibernéticos (BOSSLER; HOLT, 2012).

3 DISTRIBUIÇÃO ORÇAMENTÁRIA PARA A SEGURANÇA PÚBLICA: UM PANORAMA

A organização do orçamento público no Brasil foi institucionalizada por meio da Lei nº 4.320, de 1964. Posteriormente, a Portaria nº 42, de 1999, atualizou o modelo de classificação em Funções, Subfunções, Programas, Projetos e Atividades. É por meio dessa classificação que se tem níveis de agregação da despesa.

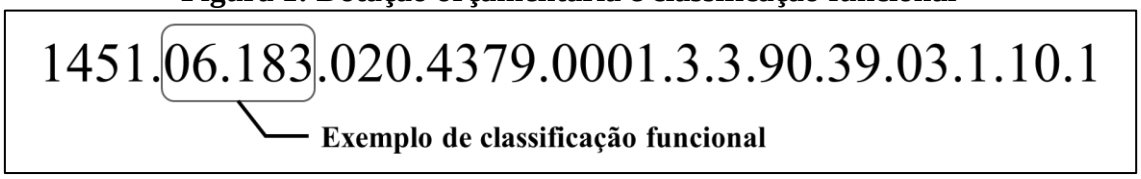
O primeiro agrupamento – Unidade Orçamentária – "compreende uma repartição do órgão ou um agrupamento de serviços que se subordinam a determinado órgão"

(GIACOMONI, 2017, p.91). Na Figura 1, a sequência 1451 simboliza a classificação institucional da Administração Direta (1). Na sequência o código (451) representa a antiga Secretaria de Estado de Defesa Social do Estado de Minas Gerais.

O segundo agrupamento – Funções de Governo – é o maior nível de agregação da despesa (GIACOMONI, 2017). O conjunto numérico 06 representa a Função Segurança Pública. O terceiro agrupamento – Subfunção de Governo – representa "uma partição da Função, visando agregar determinado subconjunto de despesas do setor público" (GIACOMONI, 2017, p. 96). As Subfunções de Governo vinculadas a Função de Governo Segurança Pública são: Policiamento (06.181); Defesa Civil (06.182) e Informação e Inteligência (06.183).

A dotação orçamentária é o resultado da organização desses algarismos em uma sequência na qual cada conjunto de algarismos define o planejamento e a destinação do recurso público. A Figura 1 apresenta uma dotação orçamentária completa.

Figura 1: Dotação orçamentária e classificação funcional



Fonte: autores, 2022

A Subfunção de Governo 183 – Informação e Inteligência é utilizada pela Polícia Civil, dada sua atribuição para investigar crimes. Essa é a Subfunção selecionada por este estudo para detalhar as despesas vinculadas a polícia investigativa, conforme será argumentado a seguir.

4 METODOLOGIA

Este estudo realizou dois movimentos complementares: (i) descrição longitudinal da despesa empenhada nos 27 estados brasileiros para a Subfunção 183 - Informação e Inteligência e (ii) levantamento dos crimes cibernéticos registrados nos 27 estados brasileiros. Os marcos temporais para despesa e registro dos crimes foram tratados de forma distinta devido à ausência de dados.

Sobre o primeiro movimento, ressalta-se que a escolha da Subfunção 183 resguarda correlação com a Constituição Federal (1988), que delimita a segurança pública. Enquanto a Carta Magna apresenta três organizações de segurança em nível estadual, a saber, Polícia Militar, Corpo de Bombeiros Militar e Polícia Civil, as

subfunções também apresentam três classificadores: 06.181 – Policiamento; 06.182 – Defesa Civil e; 06.183 – Informação e Inteligência (BRASIL, 1999).

A Subfunção 181 – Policiamento é comumente utilizada pela Polícia Militar e a Subfunção 183 – Informação e Inteligência é normalmente utilizada pela Polícia Civil, sendo essa a principal razão para a seleção da Subfunção 183 na execução deste estudo, tendo como finalidade o agrupamento do orçamento da Polícia Civil para suas atividades-fim. De forma objetiva, reforça-se a compreensão de que crimes cibernéticos podem ser uma das inúmeras atividades previstas dentro da Subfunção 183 – Informação e Inteligência. Sendo assim, a escolha pela utilização da Subfunção 183 – Informação e Inteligência foi motivada também pela aproximação entre as competências dos atores estaduais responsáveis pela segurança pública e a aderência às legislações de planejamento orçamentário confeccionadas pelo poder executivo.

Dessa forma, excluiu-se da análise a União e, por consequência, a Polícia Federal, que, reconhece-se, também pode atuar em crimes cibernéticos. Nesse momento, destaca-se dois pontos principais: (i) desde o ano de 2017, a União realiza um esforço de adequar a distribuição do orçamento federal seguindo as normas *Classifications of Fuctions of Government* (COFOG) – desenvolvida pelas Nações Unidas –, adequação não utilizada atualmente pelos estados, além de não absorver todos os anos do estudo; (ii) a denúncia de um ato criminoso de natureza cibernética pode ser realizado pelo indivíduo em Delegacias da Polícia Civil Especializadas em Crimes Cibernéticos, cuja investigação pode ser iniciada pela Polícia Civil e, a depender da complexidade, em conjunto com todo o sistema de justiça criminal estadual e, em determinadas circunstâncias, em conjunto com a Justiça Federal. Nesse caso, reforça-se que os recursos vinculados a esse último não foram computados.

Para compilar os recursos da Subfunção mencionada e evitar inconsistências naturais ao registro dos gastos públicos, utilizou-se dos dados oficiais oriundos da Secretaria do Tesouro Nacional (STN). Em consonância com os indicadores fiscais, a métrica selecionada foi a "Despesa Empenhada". Para contornar as influências da inflação, aplicaram-se índices de ajuste aos valores correntes com base no Índice Geral de Preços-Disponibilidade Interna (IGP-DI) (FUNDAÇÃO GETÚLIO VARGAS, 2022). O índice foi ajustado para ter como base os preços de dezembro de 2018 (697,446), permitindo a comparação intertemporal.

Para controlar o efeito do crescimento da população sobre as contas públicas, foram realizadas análises considerando valores per capita. Os dados de população foram

extraídos do Departamento de Informática do Sistema Único de Saúde (DATASUS) (MINISTÉRIO DA SAÚDE, 2020). Ao consolidar a base de dados, notou-se a presença de considerável quantidade de lançamentos igual a zero ou campo de preenchimento vazio. De forma a não alterar a base de dados, os campos vazios foram mantidos de forma a registrar não execução da despesa na Subfunção analisada. Ademais, os dados iguais a zero ou vazios foram analisados de maneira a observá-los como possível indicador de falta de transparência por parte das unidades federativas em que tal fenômeno foi observado, como será argumentado durante a análise dos resultados.

Em relação ao segundo movimento - levantamento dos crimes cibernéticos registrados nos 27 estados brasileiros - não foi possível levantar base de dados que representasse o período temporal estipulado e, concomitantemente, fornecesse informações subdivididas por estado. Tal fato não é surpresa na literatura sobre o tema e pode ser justificado pela dificuldade em se mapear CC (DAVIS, 2012; SARRE; LAU; CHANG, 2018), sendo reconhecido também como uma das limitações deste estudo.

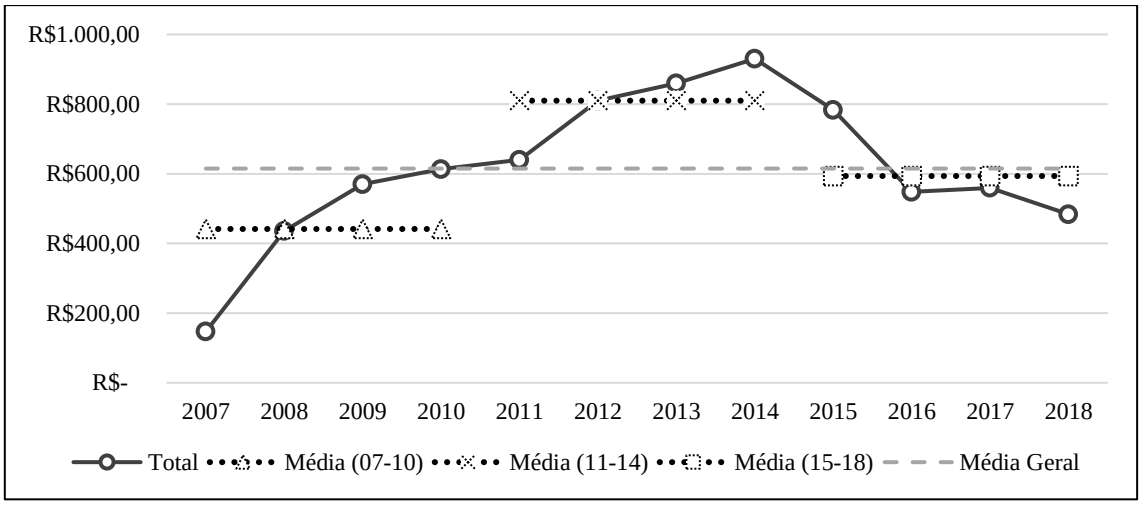
Em busca de números satisfatórios, recorreu-se à bases de dados de empresas que atuam no setor de segurança digital para conhecer dados relativos à links maliciosos – *cyber-trespass* – durante três trimestres de 2018 e tentativas de fraudes eletrônicas – *cyber-theft* – ocorridas em 2018, detalhados por estado. Por este motivo, as análises acerca dos CC e suas relações com a subfunção Informação e Inteligência estiveram delimitadas a 2018.

5 APRESENTAÇÃO DOS RESULTADOS

5.1 Gastos orçamentários com Informação e Inteligência

Considerando a série histórica, o Brasil aloca, em média, R$ 600 milhões por ano em Informação e Inteligência, com evolução crescente no período 2007-2014. A partir de 2014, há redução nos gastos até 2016, alcançando, em 2018, valor próximo ao registrado há uma década.

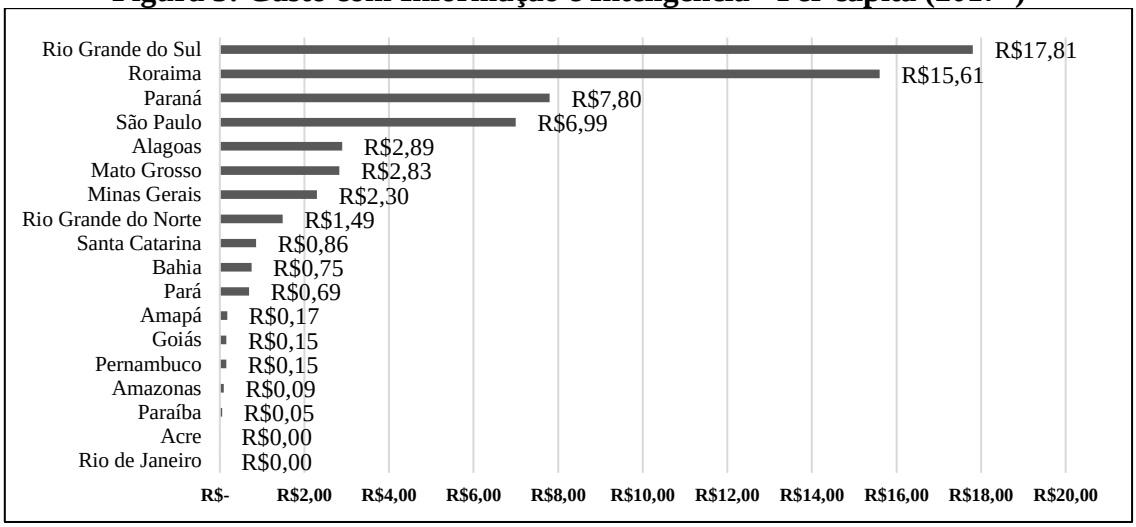
Figura 2: Gasto com Informação e Inteligência (em milhões de reais) - 2007-2018



Fonte: Elaborado a partir de dados da STN.

Também é possível identificar ausência de padrão de gastos. Em relação ao gasto per capita, em 2017, apenas três estados se destacam, mas Roraima – 2º maior gasto per capita -, registra 0,3% da população geral (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2022). Ademais, ressalta-se que durante o ano de 2017, estados como o Acre e Rio de Janeiro não registraram gastos na subfunção analisada.

Figura 3: Gasto com Informação e Inteligência - Per capita (2017*)



Fonte: Elaborado a partir de dados da STN.

*Dado o quantitativo de registros ‘zero’ ou ‘vazios’ no ano de 2018, coube aos autores selecionarem o ano anterior.

Tabela 1 – Gastos em Informação e Inteligência por Estado (em milhões de reais) – 2007-2018

Estados	07	08	09	10	11	12	13	14	15	16	17	18	Média
Espírito Santo - ES	1,33	10,15	2,12	3,71	3,51	3,76	2,99	2,20	2,56				3,23
Minas Gerais - MG	34,69	81,24	62,40	64,94	34,49	109,31	116,28	139,72	142,05	50,46	48,53	39,61	76,98
Rio de Janeiro - RJ	0,30	0,13	0,05	0,03		0,03	0,02	0,05	0,03				0,06
São Paulo - SP	10,17	228,43	348,06	332,57	419,22	392,38	434,13	377,46	405,18	319,52	315,40	263,49	320,50
Total Região Sudeste	**46,48**	**319,95**	**412,63**	**401,25**	**457,22**	**505,47**	**553,43**	**519,43**	**549,81**	**369,98**	**363,93**	**303,10**	**400,22**
Paraná - PR	35,53	35,73	34,36	43,35	35,68	44,66	81,15	73,52	85,29	86,37	88,25	76,89	60,06
Rio Grande do Sul - RS	32,84	36,10	39,05	41,16	33,50	49,27	5,03	51,69	48,80	34,06	48,32	62,12	40,16
Santa Catarina - SC	1,73					0,19	1,05			3,99	6,02	6,84	1,98
Total Região Sul	**70,10**	**71,83**	**73,41**	**84,51**	**69,18**	**94,12**	**87,23**	**125,21**	**134,08**	**124,42**	**142,58**	**145,85**	**101,88**
Alagoas - AL		0,03		0,15	0,39	8,48	6,28	3,05	4,96	1,98	9,77	0,01	2,92
Bahia - BA	0,86	2,78	9,63	20,38	17,78	18,80	7,72	18,25	17,97	22,08	11,49	9,21	13,08
Ceará - CE		4,33	7,64	10,11	10,77	6,53	2,91	0,84	4,79				4,79
Maranhão - MA													0,00
Paraíba - PB	0,80	0,98	0,73	0,77	0,30	0,58	0,92	1,36	0,41	0,22	0,21	0,16	0,62
Pernambuco - PE	2,29	3,54	2,77	2,76	3,44	5,25	1,38	1,15	1,19	0,71	1,43	0,51	2,20
Piauí - PI							0,42						0,05
Rio Grande do Norte - RN											5,22		0,65
Sergipe - SE		0,99											0,14
Total Região Nordeste	**3,95**	**12,65**	**20,78**	**34,17**	**32,68**	**39,64**	**19,64**	**24,64**	**29,34**	**24,99**	**28,12**	**9,89**	**23,37**
Distrito Federal - DF													0,00
Goiás - GO		1,97	1,06	0,27	0,35	0,04	0,30	3,95	1,72	0,25	1,04	0,91	0,99
Mato Grosso - MT	0,99	1,08	0,17	13,49	11,03	7,54	8,02	7,78	8,47	11,37	9,45	9,85	7,44
Mato Grosso do Sul - MS	1,66	7,01	22,72	22,63	31,95	127,83	154,66	191,82					62,25
Total Região Centro-Oeste	**2,65**	**10,06**	**23,95**	**36,39**	**43,33**	**135,42**	**162,98**	**203,55**	**10,18**	**11,62**	**10,49**	**10,76**	**55,11**
Acre - AC	1,65	0,62	0,27	0,18	0,38		1,85	1,64	1,25	0,02			0,66
Amapá - AP	0,24	2,78	9,63	20,38	17,78	18,80			0,11	0,13	0,14	0,11	7,01
Amazonas - AM	12,18	11,74	14,94	11,12	9,77	0,29	0,50	0,45	0,36	0,34	0,36	0,17	5,19
Pará - PA	6,86	3,21	10,69	17,42	5,26	11,00	23,60	38,13	47,00	7,17	5,78	6,12	15,19
Rondônia - RO													0,00
Roraima - RR	2,77	2,67	3,08	3,08	4,29	4,39	6,00	12,81	11,01	9,30	8,16	7,70	6,27
Tocantins - TO		0,44	0,78	4,90	0,19	0,96	4,19	4,46	0,06				1,60
Total Região Norte	**23,69**	**21,46**	**39,40**	**57,09**	**37,66**	**35,44**	**36,15**	**57,49**	**59,79**	**16,95**	**14,44**	**14,11**	**34,47**

Fonte: Elaborado a partir de dados da STN.

A dificuldade em realizar o levantamento de gastos públicos é, também, uma consequência da forma como o orçamento é instituído e computado pelos atores públicos, como observa-se pelos lançamentos de valores R$ 0,00 ou vazios na Tabela 1. O Quadro 2 abaixo detalha o número de lançamentos de R$ 0,00 e vazios no período analisado. Lançamentos faltantes são identificados pelo símbolo (•).

Ressalta-se que R$ 0,00 tende a indicar uma escolha de não realização de empenho, enquanto o lançamento vazio prejudica a análise da qualidade das escolhas realizadas pelos poderes executivos.

Quadro 1 – Lançamentos R$ 0,00 ou faltantes (2007-2018)

Estados	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
AC						0						0
AL	0											
AP							•	•				
AM												
BA												
CE	0									•	•	0
DF	0	0	0	0	0	0	•	•	•	•	•	0
ES										•	•	0
GO	0											
MA	0	0	0	0	0	0	•	•	•	•	•	0
MT												
MS									•	•	•	0
MG												
PA												
PB												
PR												
PE												
PI	0	0	0	0	0	0		•	•	•	•	0
RJ					0					•		
RN	0	0	0	0	0	0	•	•	•	•		0
RS												
RO	0	0	0	0	0	0	•	•	•	•	•	0
RR												
SC		0	0	0	0			•	•			
SP												
SE	0		0	0	0	0	•	•	•	•	•	0
TO	0									•	•	0

Fonte: Elaborado a partir de dados da STN.

5.2 Crimes cibernéticos no Brasil

Os crimes cibernéticos são naturalmente complexos (WEISS; JANKAUSKAS, 2019). Assim, tem-se a expectativa de que gastos com Informação e Inteligência sejam

ampliados. Nesse momento, serão destacados CC que ocorreram por meio de links maliciosos –*cyber trespass* – e tentativas de fraudes em compras online – *cyber theft* – em âmbito estadual. O número de ataques via links maliciosos é considerável – 147.934.485 – e reforça a posição de destaque do país nesse quesito. Ademais, os ataques via links maliciosos podem assumir diferentes formas, como aponta a Tabela 2. Dentre os principais tipos de ataques, destacam-se as variações de *phishing* – ato em que o usuário revela informações sensíveis, que podem ser utilizadas de forma ilícita posteriormente. Ainda em relação ao *phishing*, destaca-se também a sua capacidade de ser utilizado em conjunto a operações financeiras, como o *phising* via premiação falsa, *phishi*ng bancário ou *phishing* via criptomoeda.

Tabela 2 – Tipos de links maliciosos no Brasil – 1º, 2º e 3º trimestres (2018)

Links maliciosos	**1º Tri.**	**2º Tri.**	**3º Tri.**
Phishing (app de mensagens)	65,5%	57,4%	38,2%
Publicidade suspeita	14,3%	19,2%	29,5%
Notícias falsas	5,3%	7,0%	11,0%
Phishing (premiação falsa)	4,3%	3,0%	2,6%
Golpe do SMS pago	4,1%	3,1%	0,0%
Phishing bancário	3,1%	3,8%	4,8%
Site com malware	1,3%	1,6%	2,4%
Phishing (e-mail)	1,0%	3,9%	4,7%
Phishing (perfil falso)	0,9%	0,0%	0,0%
Phishing (serviços falsos)	0,0%	0,0%	3,1%
Phishing (criptomoeda)	0,0%	0,0%	1,6%
Outros (genérico, *phishing* de redes sociais)	0,1%	0,9%	2,1%

Fonte: Elaborado a partir de (DFNDR LAB, 2018a, 2018b, 2018c)

Em conjunto com os links maliciosos, as fraudes online em *e-commerce* – (KONDUTO, 2020) – formam a segunda categoria de crime alvo deste estudo registrada na Tabela 3.

Tabela 3 – Links maliciosos e tentativas de fraudes registrados em 15 estados

Links maliciosos (1º, 2º e 3º Trimestres de 2018)			Fraudes (2018)		
	Estado	**% Ataques**		**Estado**	**% Fraudes**
1	SP	25,78%	1	SP	40,68%
2	RJ	11,51%	2	RJ	9,77%
3	MG	10,86%	3	MG	8,15%
4	BA	7,49%	4	BA	5,36%
5	PE	4,87%	5	CE	4,40%
6	CE	4,82%	6	PR	3,80%
7	RS	4,11%	7	GO	3,77%
8	PR	3,79%	8	DF	3,63%
9	PA	2,95%	9	RS	3,14%
10	GO	2,66%	10	SC	2,70%
11	SC	2,34%	11	PE	2,07%
12	AM	2,18%	12	MA	1,46%
13	MA	2,11%	13	MT	1,46%
14	DF	2,06%	14	PA	1,44%
15	PB	1,71%	15	ES	1,43%

Fonte: Elaborado a partir de (DFNDR LAB, 2018c, 2018a, 2018b; KONDUTO, 2020)

Observa-se a predominância de ataques via links maliciosos e tentativas de fraudes em *e-commerce* nos estados mais populosos do país, como SP, MG, RJ e BA (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2022). Analisando as fraudes em *e-commerce*, os estados da região Nordeste possuem parcela significativa de fraudes, enquanto o registro de compras online é inferior aos estados da região Sul, por exemplo.

Nos estados da região Nordeste, a proporção de tentativas de fraude registradas é superior ao *share* de *e-commerce*. Ou seja, os estados possuem parcela superior na tentativa de fraudes em relação a sua parcela de mercado. O inverso se aplica à região Sul (Konduto, 2019). A Tabela 4 demonstra a proporção de *fraud share* e links maliciosos por regiões do país, além da proporção de população com acesso à internet.

Tabela 4 – *Fraud Share*, ataques via links maliciosos e população conectada

Região	***Fraud Share* (2018)**	**Ataques (1º, 2º, 3º Trimestres de 2018)**	**Pessoas com mais de 10 anos que utilizam a internet (2018)**
Sudeste	60,03%	49,61%	76,5%
Nordeste	17,16%	26,31%	58,4%
Sul	9,64%	10,24%	73,2%
Centro-Oeste	9,59%	6,99%	76,6%
Norte	3,58%	6,85%	60,1%

Fonte: Elaborado a partir de (DFNDR LAB, 2018c, 2018a, 2018b; IBGE-TIC, 2019; KONDUTO, 2020)

A região Nordeste possui a menor proporção de população com acesso à internet, tornando possível cogitar que a região tenha potencial para florescimento ainda maior de CC. A preocupação se eleva quando os dados são sobrepostos aos estados e regiões que declararam gastos com Informação e Inteligência como zero ou inexistentes: a região Nordeste é o local em que esse comportamento mais prevaleceu, com cerca de 50 lançamentos. Além disso, é seguida pela região Norte – segunda menor proporção de população conectada à internet – em que os gastos foram declarados como zero em 11 oportunidades e faltantes em outras 9.

6 CONSIDERAÇÕES FINAIS

Este estudo buscou analisar os recursos financeiros disponíveis para investigar e elucidar CC no Brasil, crimes complexos (SARRE; LAU; CHANG, 2018; WALL, 1997) e ameaça latente em escala nacional e internacional (HALL et al., 2021). Para tanto, foi utilizada a Subfunção 183 - Informação e Inteligência entre 2007 e 2018, assim como dados secundários de CC ocorridos no país, com enfoque em links maliciosos e tentativas de fraudes em *e-commerce*. O levantamento tornou-se um esforço hercúleo devido à falta de padronização dos gastos na referida Subfunção.

Ressaltou-se, durante a análise, a singularidade no orçamento público nacional em se distinguir os lançamentos sem valor real e os dados vazios ou faltantes. Ambos se mostraram presentes em diversos momentos, sendo registrados pelo menos uma vez por 16 estados. Tal fato torna possível sugerir falta de transparência por parte dos entes públicos, além de demonstrar a necessidade de se estabelecer uma sistemática de controle e fiscalização, com o objetivo de se certificar que os estados registrem de forma clara os seus gastos na Subfunção 183 - Informação e Inteligência. Dada a estrutura de segurança nacional, conjuntamente às constantes inovações tecnológicas, torna-se questionável um estado não possuir gastos na área pelos últimos 12 anos. Ressalta-se ainda que a falta de investimentos públicos na área, como investimentos em infraestrutura digital e treinamento de agentes públicos que participam da elucidação de crimes cibernéticos, são aspectos que dificultam a plena condução de atividades investigativas dos referidos crimes (BOSSLER; HOLT, 2012; WILLITS; NOWACKI, 2016).

Ao unir os gastos com o volume de crimes cibernéticos perpetrados no Brasil, a situação se revela ainda mais urgente. Ao se negligenciar a importância de manter-se um registro apurado dos gastos necessários para investigar e elucidar crimes cibernéticos, o país, que já é reconhecido como gerador de *cyber-spy* (KASPERSKY, 2020; KSHETRI,

2010), pode tornar-se premente em outros tipos de crimes cibernéticos. Além disso, elevada preocupação volta-se para a Região Nordeste, que conta com a menor proporção de indivíduos que possuem acesso à internet, mas responde por um elevado número de CC. Ao se demonstrar as dificuldades no combate ao crime cibernético, teme-se que o país possa se tornar um celeiro de criminosos cibernéticos, gerando uma ameaça global.

Espera-se que o estudo contribua para que novas discussões acerca da alocação de recursos no Brasil surjam, assim como o combate aos CC. Para tanto, ressalta-se as limitações deste estudo. Como principal limitação, destaca-se a acessibilidade aos dados de CC, atualmente ofertada apenas por empresas privadas, em período e escopo específicos, estando ausente base de dados específica que mensure o quantitativo de crimes cibernéticos reportados aos entes responsáveis pela investigação dos mesmos. Dessa forma, recomenda-se fortemente a condução de novos estudos que analisem os CC a partir de séries históricas, assim como estudos que analisem casos comparados, em nível internacional, entre países, utilizando de métodos quantitativos que possam descortinar novas compreensões acerca dos crimes cibernéticos em nível nacional e internacional.

Referências

BOSSLER, A. M.; HOLT, T. J. Patrol officers' perceived role in responding to cybercrime. **Policing**, v. 35, n. 1, p. 165–181, mar. 2012.

BRASIL. **Portaria 42 de 14 de abril de 1999**. Brasília. Atualiza a discriminação da despesa por funções de que tratam o inciso I do § 1o do art. 2o e § 2o do art. 8o, ambos da Lei no 4.320, de 17 de março de 1964, estabelece os conceitos de função, subfunção, programa, projeto, atividade, operações..., , 14 abr. 1999. Disponível em: <http://www.orcamentofederal.gov.br/orcamentos-anuais/orcamento-1999/Portaria_Ministerial_42_de_140499.pdf/>. Acesso em: 22 ago. 2022

CERT.BR. **Estatísticas do CERT.br - Incidentes**. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 22 ago. 2022.

DAVIS, J. T. Examining perceptions of local law enforcement in the fight against crimes with a cyber component. **Policing**, v. 35, n. 2, p. 272–284, maio 2012.

DFNDR LAB. **Relatório da Segurança Digital no Brasil: segundo trimestre - 2018**. [s.l: s.n.].

DFNDR LAB. **Relatório da Segurança Digital no Brasil: terceiro trimestre - 2018**. [s.l: s.n.]. Disponível em: <https://www.psafe.com/dfndr-lab/pt-br/relatorio-da-seguranca-digital/>. Acesso em: 22 ago. 2022b.

DFNDR LAB. **Relatório da Segurança Digital no Brasil: primeiro trimestre - 2018**. [s.l: s.n.]. Disponível em: <https://www.psafe.com/dfndr-lab/wp-

content/uploads/2018/05/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-Primeiro-trimestre-de-2018-1.pdf>. Acesso em: 22 ago. 2022c.

DINIZ, G.; MUGGAH, R.; GLENNY, M. **Deconstructing cyber security in brazil: Threats and Responses**. [s.l: s.n.]. Disponível em: <https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf>. Acesso em: 22 ago. 2022.

FUNDAÇÃO GETÚLIO VARGAS. **IGP | IBRE**. Disponível em: <https://portalibre.fgv.br/igp>. Acesso em: 22 ago. 2022.

GIACOMONI, J. **Orçamento público**. 17. ed. São Paulo: Atlas, 2017.

HALL, T. et al. Economic geographies of the illegal: the multiscalar production of cybercrime. **Trends in Organized Crime**, v. 24, n. 2, p. 282–307, 1 jun. 2021.

HARKIN, D.; WHELAN, C.; CHANG, L. The challenges facing specialist police cyber-crime units: an empirical analysis. **Police Practice and Research**, v. 19, n. 6, p. 519–536, 2 nov. 2018.

IBGE-TIC. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2018 - Pesquisa Nacional por Amostra de Domicílios Contínua 2017-2018.IBGE-TIC**. [s.l: s.n.]. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101705_informativo.pdf>. Acesso em: 22 ago. 2022.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **IBGE | Cidades@ | Brasil | Panorama**. Disponível em: <https://cidades.ibge.gov.br/brasil/panorama>. Acesso em: 22 ago. 2022.

KASPERSKY. **Kaspersky Security Bulletin 2020. Statistics**. Disponível em: <https://securelist.com/kaspersky-security-bulletin-2020-statistics/99804/>. Acesso em: 22 ago. 2022.

KONDUTO. **Raio-X da Fraude 2019: veja dados sobre a fraude no e-commerce**. [s.l: s.n.]. Disponível em: <https://blog.konduto.com/pt/2019/02/indice-cai-mas-e-commerce-ainda-sofre-553-tentativas-de-fraude-por-hora/>. Acesso em: 22 ago. 2022.

KSHETRI, N. Diffusion and effects of cyber-crime in developing economies. **Third World Quarterly**, v. 31, n. 7, p. 1057–1079, out. 2010.

MINISTÉRIO DA SAÚDE. **TabNet Win32 3.0: População Residente - Estimativas para o TCU - Brasil**. Disponível em: <http://tabnet.datasus.gov.br/cgi/tabcgi.exe?ibge/cnv/poptuf.def>. Acesso em: 22 ago. 2022.

SARRE, R.; LAU, L. Y. C.; CHANG, L. Y. C. **Responding to cybercrime: current trends**. **Police Practice and Research**Routledge, , 2 nov. 2018.

SILVA, L. A. M. **CAPACIDADES ESTATAIS APLICADAS À SEGURANÇA PÚBLICA: Análise da Execução orçamentária na Política de Segurança Pública no Estado de Minas**. São Paulo: Fundação Getulio Vargas, 2020.

STALANS, L. J.; FINN, M. A. **Understanding How the Internet Facilitates Crime and Deviance**. **Victims and Offenders**Routledge, , 1 out. 2016.

WALL, D. Policing the Virtual Community: The Internet, Cyberspace and Cyber-Crime. Em: **Policing Futures**. London: Palgrave Macmillan UK, 1997. p. 208–236.

WALL, D. Cybercrimes: New Wine, No Bottles? Em: **Invisible Crimes**. London: Palgrave Macmillan UK, 1999. p. 105–139.

WEISS, M.; JANKAUSKAS, V. Securing cyberspace: how states design governance arrangements. **Governance**, v. 32, n. 2, p. 259–275, 2019.

WILLITS, D.; NOWACKI, J. The use of specialized cybercrime policing units: an organizational analysis. **Criminal Justice Studies**, v. 29, n. 2, p. 105–124, 2 abr. 2016.

AGRADECIMENTOS

Os autores agradecem à Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) pelo suporte financeiro para a pesquisa deste artigo.