revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

O Ransomware como ameaça à cibersegurança da gestão pública de dados no Brasil[1]

Ransomware as a threat to cybersecurity in public data management in Brazil

Luciano Vaz-Ferreira
Doutor em Estudos Estratégicos Internacionais pela Universidade Federal do Rio Grande do Sul (UFRGS), com período de pesquisa na *American University* (Washington, D.C.). Realizou estágio de pós-doutorado na Universidade da Força Aérea (UNIFA). Professor da Universidade Federal do Rio Grande (FURG). E-mail: lvazferreira@gmail.com.

Filipe Bach Rodrigues
Mestrando em Direito e Justiça Social (FURG). E-mail: bachfilipe@gmail.com.

Resumo

Com o aumento da digitalização da sociedade e da Administração Pública, emergiram novas discussões a respeito da utilização de dados digitais, regulada pela recente Lei de Proteção de Dados brasileira (LGPD). Uma preocupação importante diz respeito à vulnerabilidade na segurança destes dados, ameaçada por crimes cibernéticos como o *ransomware*. Diante disto, a presente pesquisa busca analisar as possibilidades de responsabilização da Administração Pública no tratamento de dados, focando-se no aspecto preventivo da cibersegurança. A metodologia utilizada neste artigo será baseada em revisão bibliográfica. Como conclusão, verificou-se que o *ransomware* é uma ameaça à cibersegurança brasileira e que exige a adoção de instrumentos de cooperação internacional. É preciso estar atento às possíveis implicações do *ransomware* na LGPD, especialmente em relação à gestão pública de dados. O investimento preventivo em cibersegurança é um dos pilares da LGPD, podendo acarretar sanções direcionadas também para entes públicos em caso de descumprimento da legislação.
Palavras-chave: Ransomware, Cibersegurança, Gestão Pública de Dados, Lei Geral de Proteção de Dados Pessoais. Brasil.

Abstract

With the increasing digitization of society and Public Administration, new discussions emerged regarding the use of digital data, regulated by the recent Brazilian Data Protection Law (LGPD). A current concern is the security vulnerability of this data, threatened by cybercrimes such as ransomware. Given this, this research seeks to analyze the possibilities of accountability of the Public Administration in data processing, focusing on the preventive aspect of cybersecurity. The methodology is based on a literature review. In conclusion, it was found that ransomware is a threat to Brazilian cybersecurity and requires the adoption of instruments of international cooperation. It is necessary to be aware of the possible implications of ransomware on the LGPD, especially concerning public data management. Preventive investment in cybersecurity is one of the pillars of the LGPD, which may also lead to sanctions directed at public entities in case of non-compliance with the law.
Key words: Ransomware, Cybersecurity, Public Data Management, Brazilian Data Protection Law, Brazil.

[1] Recebido para Publicação em 22/07/2021. Aprovado para Publicação em 15/08/2021.
DOI https://doi.org /10.5281/zenodo.5515726

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

Introdução

Com o aumento das atividades realizadas no ambiente virtual, especialmente em virtude da situação pandêmica instaurada em 2020, emergiram novas discussões a respeito da utilização de dados digitais, regulada pela recente Lei de Proteção de Dados brasileira (LGPD). Uma preocupação importante diz respeito à vulnerabilidade na segurança destes dados, ameaçada pelo crescimento da ocorrência de crimes cibernéticos, como o *ransomware*. Diante disto, a presente pesquisa busca analisar as possibilidades de responsabilização da Administração Pública no tratamento de dados, focando-se no aspecto preventivo da cibersegurança. O artigo possui como base metodológica a revisão bibliográfica, envolvendo, além da análise da produção acadêmica, a consulta em documentos oficiais (inclusive instrumentos legais brasileiros e internacionais) e matérias jornalísticas.

No primeiro capítulo serão discutidos o processo de digitalização da sociedade, por meio dos avanços da tecnologia de informação e comunicação, e o papel do poder público na gestão de dados. O segundo capítulo será dedicado ao estudo do *ransomware* enquanto ameaça global à cibersegurança. Serão analisados os aspectos conceituais, o papel da Convenção de Budapeste e o contexto brasileiro. Por fim, no terceiro capítulo o foco será na LGPD e seus reflexos na esfera pública. Neste cenário, serão demonstrados os limites no tratamento de dados realizado por ente público e os mecanismos de responsabilização dispostos na regulação brasileira.

Digitalização da Sociedade e da Administração Pública

Com a eclosão da pandemia de covid-19, muitos gestores, em diferentes esferas de governo, tiveram que rapidamente se adaptar às novas circunstâncias. Como consequência das medidas de contenção de propagação do vírus, acelerou-se o uso de tecnologias de informação e comunicação, desenvolvendo uma crescente dependência desse meio em diferentes segmentos da sociedade, como trabalho (*home office*), compras (*e-commerce*), finanças (*e-banking*) e ensino à distância (*EAD*).

Na esfera pública, há também um redimensionamento destas interações, que passam a ser realizadas no ambiente virtual. Já são termos correntes as cidades inteligentes (*smart cities*) e os governos eletrônicos (*e-government*), que conectam cidadãos e empresas com a Administração Pública utilizando-se de plataformas digitais. Em um estudo recente do Departamento de Assuntos Econômicos e Sociais das Nações Unidas (UNITED NATIONS, 2020, p. 215-220), no contexto pandêmico, o governo eletrônico e as cidades tecnológicas mostram-se como ferramentas importantes em duas frentes: a transmissão de informações sobre a pandemia à população (como, por exemplo, orientações de medidas de saúde e busca por locais de atendimento em telefones móveis); e o controle da mobilidade humana e vigilância epidemiológica (como no caso de monitoramento de infecção e mobilidade por meio de aplicativos e *GPS* de *smartphones*).

De acordo com West (2004, p. 16), *e-government* refere-se à "entrega de informações e serviços governamentais on-line por meio da internet ou outros meios digitais". O "governo eletrônico para cidadãos" (*G2C*) é um tipo de *e-government* que possui como objetivo facilitar a interação entre os cidadãos e a informação pública, tornando-a mais acessível (ALSHEHRI; DREW, 2010, p. 36). Neste sentido,

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

Fana (2002, p. 4) discorre que o governo eletrônico "aumenta o acesso às informações governamentais e promove melhores oportunidades de o cidadão participar em instituições de maneira democrática".

No contexto pandêmico, a experiência do governo eletrônico pelo mundo foi responsável por alertar a população por meio de portais públicos, fornecendo "informações transparentes e confiáveis", e conectando "pessoas com os recursos apropriados" (UNITED NATIONS, 2020, p.219). Além disso, auxiliou na vigilância epidemiológica, permitindo os governos tomarem decisões políticas rápidas com base em dados e análises em tempo real (UNITED NATIONS, 2020, p. 215).

As *smart cities* podem ser traduzidas como "cidades tecnológicas" ou "inteligentes". Segundo Washburne Sindhu (2010) trata-se "do uso de tecnologias de computação inteligente que visa tornar os serviços essenciais de infraestrutura de uma cidade mais inteligente, interconectados e eficientes". O seu objetivo é fomentar o desenvolvimento social, educacional, econômico e ecológico do ambiente urbano (REMÉDIO, 2017, p. 673). As *smart cities* têm demonstrado vantagem na gestão da pandemia, devido à colocação em prática de avançadas ferramentas de governo eletrônico (UNITED NATIONS, 2020).

A tecnologia do *big data* é fundamental para o funcionamento das cidades inteligentes (ALDAIRI; TAWALBETH, 2017, p. 1090). De acordo com Remédio (2017, p. 673), o *big data* "possibilita o acompanhamento de comportamentos humanos em tempo real e de maneira massificada, proporcionando inteligência às cidades, quando devidamente processados e analisados os dados que o integram". Uma cidade que constrói suas políticas públicas com base neste mecanismo possui "um poderoso trunfo para resolver os vários problemas enfrentados (...) incluindo crescimento da população urbana, envelhecimento da sociedade, congestionamento de trânsito e segurança" (TOKORO, 2016, p. 2).

Estas ferramentas tecnológicas devem ser utilizadas com cautela, pois podem ser transformadas em "poderosas armas de controle social" (LYON, 1994, p. 04), na forma de vigilância (*surveillance*). Apesar do uso de mecanismos de vigilância pelo Estado não ser uma novidade, a tecnológica é capaz de potencializá-los de maneira inimaginável, visto que atualmente as interações sociais dependem cada vez mais do relacionamento com bases de dados digitais (LYON, 1994, p. 06).

Dados compartilhados permitem a análise do perfil do indivíduo, o direcionamento de informações e o oferecimento de serviços de acordo com o seu comportamento na rede, tanto pelo poder público quanto pelo setor privado. A mineração de dados tem sido conhecida como o "novo petróleo" por conta de seu potencial econômico. Contudo, ao contrário deste recurso energético, não são protegidos por barreiras físicas de segurança. Dados envolvendo cartão de crédito ou contas privadas de e-mail, por exemplo, encontram-se em bases de segurança frágil (GOODMAN, 2015, p. 241). Existe sempre o risco que tais dados possam ser apropriados indevidamente não apenas pelo Estado e empresas, mas também por criminosos, utilizando-se de fraudes e invasões cibernéticas.

O grande desafio para as cidades tecnológicas e para o governo eletrônico é preservar a segurança e a privacidade destes dados. Em virtude do rápido aumento das tecnologias de utilização de dados nas cidades pelo mundo **(**ALDAIRI; TAWALBEH, p. 1088) é necessário aumentar as estratégias que preservem a cibersegurança. Com a dependência do meio digital, "diversificam as possibilidades de aplicação destas tecnologias para fins lícitos e ilícitos, intensifica-se o debate em torno dos desafios que a era digital apresenta à segurança nacional e internacional" (CEPIK et al, 2014, p. 161).

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

Ransomware como ameaça digital ao Brasil

Primeiramente, é necessário discutir os conceitos de crimes cibernéticos e ciberespaço. Marion e Twede (2020, p. 12) definem os crimes cibernéticos (digitais ou virtuais) como sendo "qualquer crime que envolva um computador ou uma rede". Singer e Friedman (2014, p. 94) entendem ser o "uso de ferramentas digitais por criminosos para roubar ou realizar outras formas de atividades ilegais". Solis (2014, p. 02) inclui como crimes cibernéticos "ofensas de acesso, comprometimento de dados, uso indevido de dispositivos e interceptação de dados".

É preciso entender que o ambiente do ciberespaço, onde são praticados estes crimes, é mais amplo que noção comum de internet ou "rede mundiais de computadores". Conforme Canabarro et al (2014, p. 132), o ciberespaço constituiu-se, além da internet, em "redes de telégrafo, de rádio amador, de telefonia fixa/móvel e de televisão via satélite, sistemas de controle de tráfego aéreo e de navegação marítima". Da mesma forma, Nye (2012, p. 163) destaca que não se restringe "somente a internet dos computadores ligados a rede, mas também intranets, tecnologias de telefonia celular e comunicações via satélite".

Nos últimos anos, um crime que tem ganhado destaque é o *ransomware*. De acordo com Marion e Twede (2020, p. 351), trata-se da utilização de um tipo de código ou software nocivo (*malware*) para extorquir dinheiro (*ransom*) de outros usuários. Primeiramente, o criminoso invade e controla os dispositivos de um usuário, impedindo o acesso aos seus arquivos, como fotos, planilhas e outros documentos. Em troca da liberação do acesso da vítima, o criminoso solicita que seja pago uma determinada quantia e concede um prazo. Caso o pagamento não seja realizado, o delinquente poderá aumentar a quantia solicitada ou destruir os dados. O primeiro crime cibernético por *ransomware* difundiu-se por meio do disquete, no ano de 1989, conhecido como *PC Cyborg*. Com o passar das décadas, novas formas de disseminação foram desenvolvidas, aumentando a sua incidência (POPOOLA et al, 2017, p. 01-02).

Na maioria das vezes este pagamento é realizado por meio de *bitcoins* ou outra forma de criptomoeda, ao invés de dinheiro (MARION; TWEDE, 2020, p. 351). A preferência pelas criptomoedas diz respeito à possibilidade de transferência segura e secreta para contas em que há dificuldade de rastreamento (FORNASIER et al, 2020, p. 213). As vítimas costumam pagar o resgate para tentar minimizar os potenciais danos causados (HOLT et al, 2018, p. 157). Porém, o usuário não costuma ficar totalmente seguro mesmo após a transferência dos valores, visto que o criminoso provavelmente possui informações suficientes para roubar a sua identidade ou acessar suas contas bancárias (MARION; TWEDE, 2020, p. 352), podendo ser alvo de outros crimes virtuais.

Nos EUA, o Município de *Lake City,* na Flórida, decidiu pagar 460 mil de dólares em *bitcoin*, pois concluiu ser mais barato cumprir a exigência do que reconstruir seus bancos de dados (NEW YORK TIMES, 2019). Em *Riviera Beach*, na Flórida, do mesmo modo, o poder público entendeu por pagar 600 mil dólares a cibercriminosos que deixaram os sistemas eletrônicos da cidade inacessíveis (CNN, 2019).

Recentemente, outro caso ganhou destaque internacional: o ataque de *ransomware* a empresa *Colonial Pipeline*, que deixou inoperante o maior oleoduto dos EUA. Para recuperar o acesso ao sistema, a companhia pagou aproximadamente 5 milhões de dólares (BLOOMBERG, 2021). Em razão destes exemplos, o governo dos EUA agora enfrenta o *ransomware* como um assunto de segurança nacional, por ser capaz de interferir em serviços essenciais para a sociedade norte-americana (CNN,2021). Já se discute a

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

possibilidade de voltar a usar os registros em papel em algumas cidades, tentando minimizar os possíveis prejuízos (NEW YORK TIMES, 2019).

No Brasil, recentemente, alguns casos de *ransomware* envolvendo o poder público ganharam notoriedade durante a pandemia. O mais conhecido ocorreu em 2020,contra a rede cibernética do Superior Tribunal de Justiça (STJ), deixando os seus sistemas inacessíveis. Como consequência, milhares de processos tiveram seus prazos suspensos, o que resultou em atrasos no serviço jurisdicional (BRASIL, 2021). Outro caso semelhante envolveu o ataque de 2021 contra o Tribunal de Justiça do Estado do Rio Grande do Sul (TJ-RS) (LIMA, 2021), acarretando transtornos aos jurisdicionados. O Porto de Fortaleza, operado pela empresa pública Companhia Docas do Ceará, também foi vítima de *ransomware* em 2020. Os sistemas da companhia ficaram fora do ar durante vários dias, causando graves prejuízos, visto que as operações que eram eletrônicas passaram a ser realizadas de maneira manual, como o controle de entrada e saída de cargas (BRITO, 2019).

O Brasil ocupa a nona posição entre os países que mais enfrentaram problemas de *ransomware*, estimando-se 3.800.000 ataques (SONIC WALL).Por ser um crime ainda de prática recente, não existe a descrição de uma conduta específica de *ransomware* no Direito Penal Brasileiro. Tais ações podem compreender: a) "invasão de dispositivo informático" (Art. 154-A do Código Penal), pelo acesso indevido ao sistema; b) "fraude eletrônica" (Art. 171, § 2-A do Código Penal), pela indução ao erro; c) "extorsão" (Art. 158 do Código Penal), pelo pedido de resgate; d) "atentado contra a segurança de utilidade pública" (Art. 265 do Código Penal) ou "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade" (Art. 266 do Código Penal), se envolver serviços essenciais (WENDT; MASSENO, 2017, p. 11).

Recentemente, em maio de 2021, por meio da Lei Federal nº 14.155, o Brasil criou o crime de "fraude eletrônica" e aumentou os parâmetros de pena para o delito de "invasão de dispositivo de informática". Apesar dos tipos penais não descreverem exatamente o *ransomware,* as recentes modificações parecem ter como alvo o endurecimento de crimes desta natureza.

A Convenção contra a Criminalidade Cibernética, elaborada em 2001 no âmbito do Conselho da Europa, também conhecida como Convenção de Budapeste, exemplifica que ocorrem crimes cibernéticos quando o dispositivo eletrônico é alvo de invasão, como acesso ilegítimo (Art. 2º), interceptação ilegítima (Art. 3º), interferência em dados e em sistemas (Art. 4º e 5º) e uso abusivo (Art. 6º). O dispositivo eletrônico também pode servir como um facilitador para crimes tradicionais, como falsificação (Art. 7º) e fraude (Art. 8º). São também mencionados crimes cibernéticos vinculados à pornografia infantil (Art. 9º) e à violação de propriedade intelectual (Art. 10º).

O *ransomware* constitui-se como uma ameaça de amplitude global, o que torna a persecução criminal muito complexa. Um dos principais problemas está relacionado à sua autoria, pois é muito difícil determinar a identidade, a nacionalidade, a procedência ou a organização do criminoso (SINGER; FRIEDMAN, 2014, p. 74). Por se tratar geralmente de um crime transnacional (WALL, 2001, p. 09), há dificuldades impostas pelos limites da soberania e pela virtualização destas condutas (HOLT et al, 2018, p. 27). Um país que é alvo de um crime cibernético não pode exercer atividade policial ou judiciária em país estrangeiro sob pena de violação de soberania. Neste contexto, é necessário que haja consentimento do Estado estrangeiro ou instrumentos internacionais, como acordos bilaterais de cooperação jurídica, capazes de compelir a cooperação entre as autoridades.

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

Uma alternativa é a participação em tratados internacionais como a Convenção de Budapeste, já mencionada. Em seu preâmbulo, a Convenção reconhece a preocupação "com o risco de que as redes informáticas e a informação eletrônica sejam utilizadas para cometer infrações criminais" (COUNCIL OF EUROPE, 2001). O objetivo é fomentar a cooperação internacional entre os Estados Membros para o combate à cibercriminalidade, estabelecendo ações comuns (MARION; TWEDE, 2020, p. 76-78). A Convenção cria a obrigação de criminalizar certas condutas e harmonizar as legislações dos Estados participantes. Também permite a manutenção de canais de comunicação entre os sistemas de justiça, como polícias e poder judiciário, envolvendo, por exemplo, troca de informações, compartilhamento de provas e operações conjuntas.

De acordo com Clough (2012, p. 370), é importante que os países declarem jurisdição sobre os crimes cibernéticos da maneira mais ampla possível, pois existe perigo na manutenção de portos seguros para estas atividades. Países como Rússia, Irã, Coreia do Norte e China, potenciais locais de origem de operações cibernéticas, não assinam a Convenção, o que pode implicar barreiras para cooperação. Segundo o *Cyber Operations Tracker* do *Council of Foreign Relations* (2021), um *think tank* sobre política externa, entre 2005 e 2020, 77% de todas as operações suspeitas ao redor do mundo advêm possivelmente destes países.

A Convenção de Budapeste também é objeto de críticas. A linguagem do tratado internacional não teria acompanhado os avanços tecnológicos, dispondo sobre dispositivos e sistemas que na época de sua redação eram comumente utilizados e hoje encontram-se obsoletos (CLOUGH, 2012, p. 375; MARION; TWEDE, 2020, p. 78). Observa-se que o *ransomware* não se encontra tipificado na Convenção de Budapeste, o que impede a harmonização das legislações de Direito Penal Material nesta área. Porém, como o delito envolve a invasão de dispositivo eletrônico, entende-se ser possível utilizar os mecanismos de cooperação internacional previstos neste tratado, auxiliando a investigação e o processamento destes crimes.

Em 2019, o Brasil foi convidado a aderir à Convenção pelo Conselho da Europa. Em memorando ao Congresso Nacional, o Ministério Público Federal (2020) opinou favoravelmente à adesão ao instrumento, por uma série de razões que merecem ser apresentadas. A assinatura da Convenção cria a obrigação para o Brasil de introduzir tipos penais específicos, que poderiam preencher lacunas e auxiliar a persecução penal mais efetiva de delitos cibernéticos. Esse processo também permite a harmonização da legislação brasileira com a dos outros países, o que pode incrementar o diálogo e cooperação na área.

De acordo com o MPF, o instrumento representa um avanço na cooperação internacional em investigações, obtenções de provas e extradições envolvendo crimes cibernéticos em geral. A Convenção impõe a colaboração entre todos os signatários, o que possibilita a ampliação da cooperação com países que não possuem ainda acordo bilateral em matéria penal com o Brasil. O tratado internacional mantém pontos de contato direto entre autoridades, o que possibilita a existência de canais de comunicação que podem ser acessados de forma rápida e disponíveis 24 horas por dia. É possível inclusive o acesso direto a bancos de dados e provas digitais hospedados em outros países, havendo seu consentimento.

O MPF também observa a adesão de outros países latino-americanos à Convenção, como Argentina, Chile, Costa Rica, República Dominicana, Panamá, Paraguai e Colômbia. A participação do Brasil e a estreita colaboração com os países da região incrementaria o controle destes crimes.

A possível desatualização do tratado é minimizada, visto que é indicado que os Estados Partes costumam manter comissões de trabalho em que há avaliação mútua dos esforços colocados em prática

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

nos sistemas jurídicos nacionais e troca contínua de experiências. Por fim, menciona que a participação do país, aliada à recente promulgação da Lei de Proteção de Dados (LGPD), "completará a introdução do Brasil no cenário mundial da era digital, em que as trocas financeiras e comerciais estarão dentro do padrão internacional também do ponto de vista da segurança, permitindo um melhor combate aos delitos".

Impactos na gestão pública de dados

Apesar das dificuldades enfrentadas na persecução do *ransomware*, entende-se que a incidência de tal delito tendo como vítima a Administração Pública (como nos recentes casos relatados) pode resultar em reflexos importantes para regulação e gestão de dados digitais no Brasil.

De acordo com Wimmer (2019, p. 30), antes da legislação atual, o Brasil já possuía "uma série de direitos e garantias com o objetivo de oferecer salvaguardas ao cidadão quanto ao uso de seus dados pelo poder público". A Lei do *Habeas Data* (Lei Federal nº 9.507/97) e a Lei de Acesso à Informação (Lei Federal nº 12.257/2011) são exemplos de regulações previstas no ordenamento pátrio.

Influenciado pelo Regulamento Geral de Proteção de Dados Europeu, o Brasil criou em 2018 a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Federal nº 13.709/2018). Seu objetivo é "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Art. 1º). A LGPD estabeleceu um novo paradigma para o tratamento de dados do cidadão pelo poder público e privado, instituindo novos direitos adicionais àqueles consagrados no ordenamento jurídico brasileiro (WIMMER, 2019, p. 31).

Visando melhorar a proteção no tratamento de seus dados, grandes empresas estão investindo milhões em *softwares* mais sofisticados, contratando *data protection officers* (DPO), até mesmo oferecendo quantias para especialistas em tecnologia descobrirem falhas em seus sistemas. Apesar da proeminência das *Big Techs*, observa-se que a esfera pública é uma grande produtora e coletora de dados, possuindo um "gigantesco acervo, que é um recurso valioso que pode ser usado pelas partes interessadas para uma infinidade de propósitos" (UNITED NATIONS, 2020, p. 150). Neste contexto, é essencial que exista um arcabouço jurídico efetivo que proteja os dados pessoais.

A LGPD é taxativa ao estabelecer que seu regulamento deve ser aplicado em qualquer operação de tratamento de dados realizado por pessoa natural ou pessoa jurídica de direito privado ou *público* (Art. 3º). Neste contexto, o controlador, a quem compete às decisões referentes ao tratamento de dados pessoais, e o operador, que realiza o tratamento de dados pessoais em nome do controlador, podem ser entes públicos. O tratamento de dados pelo poder público deve ser realizado em observância do interesse público, com o objetivo de executar competências legais ou cumprir as atribuições legais do serviço público (Art. 23).

A legislação estabelece o chamado "princípio da segurança" (Art. 6, VII). Conforme Masseno et al (2020, p. 08-09), os agentes de tratamento devem minimizar a exposição a ameaças utilizando-se de "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Autoridade Nacional de Proteção de Dados (ANPD) pode "sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público" (Art.32). Portanto, "os sistemas utilizados para o tratamento de dados pessoais devem ser

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança (...)" (Art. 49).

Como exemplo de medidas preventivas técnicas, a esfera pública deve assegurar que a sua defesa eletrônica seja tão impenetrável quanto possível, por meio da utilização de antivírus, *firewalls*, *intrusion prevention systems (IPS)*, filtragem de e-mail, entre outros recursos tecnológicos. Além de uma política e de processos robustos de cibersegurança, deve-se investir em um sistema de educação para que os utilizadores possam saber como prevenir e lidar com os ataques (POPOOLA et al, 2017, p. 04).

Algumas medidas preventivas estão sendo tomadas pelo Estado brasileiro, que incluem a criação do Comitê de Segurança Cibernético pelo Conselho Nacional de Justiça (CNJ) (Portaria nº 242/2020), o Comitê Central de Governança de Dados da Administração Pública Federal (Decreto Federal nº 10.046/2019) e a Rede Federal de Gestão de Incidentes Cibernéticos (Decreto Federal n° 10.748/2021). O Poder Executivo Federal tem tentado estabelecer uma política de governança no compartilhamento de dados, além do lançamento de um Guia de Boas Práticas.

Neste cenário, parece salutar que as entidades e órgãos públicos de todas as esferas administrativas devem investir de maneira preventiva em sua cibersegurança e no cumprimento da LGPD. Isto significa que a manutenção de sistemas vulneráveis a crimes cibernéticos, como *ransomware*, cuja ocorrência já foi registrada em órgãos públicos brasileiros, pode resultar em sanções com base na LGPD.

O agente de tratamento de dados (controlador ou operador) ligado ao poder público pode ser responsabilizado se causar dano patrimonial, moral, individual ou coletivo, sendo obrigado a repará-lo (Art. 42). Neste contexto, a captura indevida de informações dos usuários do serviço em uma situação de *ransomware*, a eliminação destes dados ou até mesmo a indisponibilidade do oferecimento do serviço, podem ser caracterizados como possíveis danos. As sanções podem ser de natureza cível, como, por exemplo, a condenação em ação de indenização proposta no Poder Judiciário, ou administrativa (Art. 52), aplicada pela ANPD.

Na esfera administrativa, os entes públicos podem sofrer advertência, publicização da infração, bloqueio dos dados pessoais a que se refere a infração, eliminação destes mesmos dados, suspensão parcial do funcionamento dos bancos de dados, suspensão do exercício de atividade de tratamento de dados pessoais e proibição parcial ou total das atividades voltadas ao tratamento de dados (Art. 52).

A LGPD brasileira não prevê pena de multa para Administração Pública (Art. 52, § 3º). Apesar de não haver o fator dissuasório financeiro como no setor privado[2], a LGPD faz referência expressa à possibilidade de aplicação de outras legislações com conteúdo sancionatório, que incluem o Estatuto do Servidor Público Federal (Lei nº 8.112/90), Lei de Improbidade Administrativa (Lei nº 8.429/92) e Lei de Acesso à Informação (Lei nº 12.527/2011). Neste contexto, servidor público que viola a LGPD pode sofrer sanções que incluem, por exemplo, a perda dos direitos políticos, a perda da função pública e o ressarcimento ao Erário.

O comportamento preventivo, como investimento em sistemas robustos de cibersegurança e realização de treinamentos poderá auxiliar na minimização das sanções da LGPD (art. 52, § 1º). Exige-se, neste ponto, a adoção reiterada de mecanismos e procedimentos internos capazes de minimizar os danos.

[2] A LGPD prevê que entidades privadas podem ser sancionadas em valores partindo de 2% do faturamento do último exercício até 50 milhões de reais por infração.

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XVII | Volume XVIII | Nº 35| Janeiro/Junho 2021 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellector.cenegri.org.br

Conclusão

Observa-se que a adaptação às novas circunstâncias impostas pela pandemia de covid-19 acelerou a digitalização da sociedade. A esfera pública intensificou as ferramentas tecnológicas de captura de dados, com o interesse de informar cidadãos, vigiá-los e oferecer serviços. Tal processo, contudo, pode contribuir para o aumento da vulnerabilidade aos crimes digitais. O grande desafio é preservar a segurança e a privacidade dos dados pessoais.

O *ransomware* é um tipo de crime cibernético voltado à extorsão de valores dos usuários, representando uma ameaça à cibersegurança brasileira. Trata-se de um crime de amplitude global, o que necessita de estratégias que envolvam a cooperação internacional, como a Convenção de Budapeste. Uma futura vinculação do Brasil a este instrumento internacional parece ser uma decisão acertada.

É preciso estar atento às possíveis relações entre os crimes cibernéticos e a aplicação da nova regulação de dados no Brasil, a LGPD. Os aspectos específicos que envolvem a gestão pública de dados também merecem atenção, especialmente após os recentes casos de *ransomware* envolvendo o poder público brasileiro. O investimento preventivo em cibersegurança é um dos pilares da LGPD, podendo acarretar sanções direcionadas também para entes públicos em caso de descumprimento da legislação.

Referências

ALDAIRI, Anwar & TAWALBEH, Loai. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. Procedia Computer Science. v.109, 2017, p.1086-1091.

ALSHEHRI, Mohammed, DREW, Steve. E-Government Fundamentals, 2010. Disponível em: <https://researchrepository.griffith.edu.au/bitstream/handle/10072/37709/67525_1.pdf?sequence=1&isAllowed=y>. Acesso em: 10 jan. 2021

BLOOMBERG. Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom, 2021. Disponível em : https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom?sref=WJKVI5nK. Acesso em: 25 jun. 2021.

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

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

CANABARRO, Diego; BORNE, Thiago; LEAL, Marcelo. A Era Digital e os Estudos de Segurança: conceitos e práticas. In: PIMENTA, Marcelo; CANABARRO, Diego (Org). Governança Digital. Porto Alegre-RS, Editora UFRGS, 2014. p.130-150. <https://www.ufrgs.br/cegov/files/livros/gtdigital.pdf>.Acesso em: 13 jun. 2020.

CEPIK, M. A. C. ; CANABARRO, Diego. ; BORNE, Thiago . A Securitização do Ciberespaço e o Terrorismo: uma Abordagem Crítica. In: André de Mello e Souza; Reginaldo Mattar Nasser; Rodrigo Fracalossi de Moraes. (Org.). Do 11 de Setembro de 2001 à Guerra ao Terror: Reflexões sobre o Terrorismo no Século XX. 1ed.Brasília: Ipea, 2014, v. 1, p. 161-186.

CLOUGH, Jonathan. The Council of Europe Convention on Cybercrime: Defining 'crime' in a digital world. Criminal Law Forum, 2012. Disponível em: <https://doi.org/10.1007/s10609-012-9183-3>. Acesso em: 13 jan. 2021.

CNN. Florida city to pay $600K ransom to hacker who seized computer systems weeks, 2019. Disponível em:<https://edition.cnn.com/2019/06/20/us/riviera-beach-to-pay-hacker/index.html>. Acessoem: 10 jan. 2021.

CNN. Ransomware attacks saddle Biden with grave national security crisis, 2021. Disponível em:<https://edition.cnn.com/2021/06/07/politics/president-joe-biden-cyber-attacks-russiaputin-trump-economy/index.html>. Acessoem: 25 jun. 2021.

COUNCIL OF EUROPE. Convention on Cybercrime. Budapest, 2001. Disponível em: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Acesso em: 10 jan. 2021.

COUNCIL OF FOREIGN RELATIONS. *Cyber Operations Tracker*. Disponível em: <https://www.cfr.org/cyber-operations/>. Acesso em: 21 jul. 2021.

FANG, Z. E-Government in Digital Era: Concept, Practice, and Development. International journal of the Computer, the internet and Management. Thailand, v.10, 2002.

FORNASIER, Mateus de Oliveira; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. Revista Thesis Juris – RTJ, São Paulo, v. 9, n. 1, p. 208-236, jan./jun. 2020.

GOODMAN, Marc. Future Crimes. São Paulo: HMS, 2015.

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

LIMA, Lilian. TJ-RS diz que sistema de informática do tribunal foi alvo de ataque cibernético. Disponível em:<https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/29/tj-rs-diz-que-sistema-de-informatica-do-tribunal-foi-alvo-de-ataque-hacker-e-muito-grave.ghtml>. Acesso em: 21 jul, 2021.

LYON, D. The electronic eye: The rise of surveillance society. Minneapolis: University of Minnesota Press, 1994.

MARION, Nancy E, TWEDE, Jason. Cybercrime: an encyclopedia of digital crime. 1ed. 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, 2020, p. 1-28.

MINISTÉRIO PÚBLICO FEDERAL. Ministério Público Federal. Nota técnica PR-SP-00095455/2018. 2018, p.5-10. Disponível em :http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf; Acesso em: 18 jan. 2021

NEW YORK TIMES. Ransomware Attacks Are Testing Resolve of Cities Across America, 2019. Disponível em:< https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html>. Acesso em: 10 jan. 2021.

NYE, Joseph S. O futuro do poder. São Paulo, Benvirá, 2012.

POPOOLA, Segun I; IYEKEKPOLO, Ujioghosa B.; OJEWANDE, Samuel O; SWEETWILLIAMS, Faith O.; JOHN, S. N; ATAYERO, A. A. Ransomware: Current Trend, Challenges, and Research Directions. In: Proceedings of the World Congress on Engineering and Computer Science, v. 2, 2017.

REMÉDIO, José Antonio; SILVA, Marcelo Rodrigues da. O Uso Monopolista do Big Data por Empresas de Aplicativos: Políticas Públicas para um Desenvolvimento Sustentável em Cidades Inteligentes e Um Cenário de Economia Criativa e Livre Concorrência. Revista Brasileira de Políticas Públicas, Brasília, v. 7, n. 3, 2017, p. 671-693.

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

SOLIS, Gary D. Cyber Warfare. Military Law Review, v.219, 2014, p.1-52.

SONIC WALL. Cyber Threat Report, 2021. Disponível em :<https://www.sonicwall.com/2021-cyber-threat-report/>. Acesso em: 25 jun. 2021.

TOKORO, Nobuyuki. The smart city and the co-creation of value*:* a source of new competitiveness in a Low-carbon society. Japan: Springer, 2016.

UNITED NATIONS. United Nations E-government Survey 2020. Department of Economic and Social Affairs. Digital government in the decade of action for sustainable development, 2020. Disponível em: <https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf>. Acesso em: 10 jan. 2021.

WALL, David. S. Cybercrimes and the Internet. Crime and the Internet. New York: Routledge, 2001, p.1-17.

WASHBURN, D e SINDHU, U. Helping CIOs Understand “Smart City” Initiatives. Forrester Research, 2010.

WENDT, E.; MASSENO, M. D. O ransomware na Lei: apontamentos breves de Direito Português e Brasileiro. REVISTA ELETRÔNICA DIREITO &TI , v. 1, 2017, p. 1-13.

WEST, Darrell. E-Government and the Transformation of Service Delivery and Citizen Attitudes. Public Administration Review, 2004.

WIMMER, Miriam. Cidadania, Tecnologia e Governo Digital: Proteção de Dados Pessoais no Estado Movido a Dados. In: BARBOSA, Alexandre F. (org). TIC Governo Eletrônico 2019. Pesquisa Sobre uso das Tecnologias de informação e comunicação no setor público brasileiro. São Paulo: Comitê Gestor da Internet no Brasil,v.1, 2020, p.27-36.