REVISTA BRASILEIRA DE SEGURANÇA PÚBLICA

ARTIGO

AS (POSSÍVEIS) REGRAS E DIRETRIZES PARA USO DE SOFTWARE INVASORES PELO ESTADO BRASILEIRO: UMA ANÁLISE A PARTIR DA TENTATIVA DE CONTRATAÇÃO DO SOFTWARE DE ESPIONAGEM PEGASUS

DEVILSON DA ROCHA SOUZA

Doutor em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR) com bolsa CAPES. Mestre em Direito Constitucional Contemporâneo pela Universidade de Santa Cruz do Sul (UNISC) com bolsa CAPES, modalidade II e Mestre em Direito da União Europeia pela Universidade do Minho (UMINHO) - Portugal. Especialista em Direito Constitucional e em Direito Público. Graduado pelo Centro Universitário Franciscano do Paraná (FAE) em 2017. Pesquisador nas áreas de Ciência Política, Direito Constitucional e Novas Tecnologias.

País: Brasil **Estado:** Paraná **Cidade:** Curitiba

E-mail: devilsonsousa@hotmail.com **ORCID:** https://orcid.org/0000-0002-1261-6019

CINTHIA OBLADEN DE ALMENDRA FREITAS

Doutora em Informática, Mestre em Engenharia Elétrica e Informática Industrial, Engenheira Civil. Professora Titular do Programa de Pós-Graduação em Direito (PPGD) da Escola de Direito da Pontifícia Universidade Católica do Paraná (PUCPR). Membro Consultivo da Comissão de Direito Digital e Proteção de Dados da OAB/PR.

País: Brasil **Estado:** Paraná **Cidade:** Curitiba

E-mail: almendracinthia@gmail.com **ORCID:** https://orcid.org/0000-0002-7015-094X

BIANCA AMORIM BULZICO

Advogada, mestre em Direito pela Pontifícia Universdade Católica do Paraná em 2022, com atuação profissional nas áreas do Direito Digital e Direito da Saúde, professora convidada da UNINTER para a disciplina de Propriedade Intelectual. Entusiasta a pesquisa de novos temas relacionados a inserção do direito digital.

País: Brasil **Estado:** Paraná **Cidade:** Curitiba

E-mail: biancabulzico@gmail.com **ORCID:** https://orcid.org/0000-0002-8272-5499

Contribuições dos autores: Os três autores participaram ativamente da elaboração do presente artigo. Sob a orientação da Profª. Dra. Cinthia Freitas, os orientandos Dr. Devilson da Rocha Sousa e Me. Bianca Bulzico realizaram o levantamento bibliográfico a partir das pesquisas desenvolvidas no âmbito de seus respectivos projetos no Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Os orientandos, sob a orientação da Profª. Dra. Cinthia Freitas, foram responsáveis pela definição da estrutura do artigo, organização do referencial teórico e redação inicial do texto. Todas essas etapas foram desenvolvidas de forma colaborativa, com discussões contínuas, revisões críticas e aprimoramentos sucessivos realizados em conjunto com a orientadora. A Profª. Dra. Cinthia Freitas contribuiu de maneira decisiva na orientação metodológica, no aprofundamento e refinamento teórico-crítico, na revisão final e na consolidação dos argumentos apresentados, assegurando a coerência científica e a qualidade acadêmica do trabalho.

RESUMO

Apesar de *prima facie* representarem um risco considerável a direitos e garantias fundamentais, *softwares* invasores são corriqueiramente alardeados como fundamentais para o Estado manter o controle e exercer seu poder de polícia. Exemplo dessa categoria de *software* é o *malware* de espionagem Pegasus, que foi objeto de interesse do governo brasileiro e que é capaz de acessar dispositivos e sistemas que contêm dados e informações sigilosas sem maiores dificuldades e sem deixar rastros. Diante desse cenário, e considerando que as discussões acerca dos riscos e da legalidade do uso dessas ferramentas têm sido cada vez mais acaloradas, o presente trabalho busca jogar luz sobre essa temática. Para enfrentar o tema se faz uso do método hipotético-dedutivo e de pesquisa legislativa e bibliográfica. Os resultados apontam para a existência de um arcabouço normativo significativo ainda incapaz de orientar satisfatoriamente o Estado e seus agentes no emprego dessas novas tecnologias.
Palavras-chave: Brasil. Cibersegurança. Dados pessoais. Novas tecnologias. Segurança pública. Software.

THE (POSSIBLES) RULES AND GUIDELINES FOR THE USE OF INVADER SOFTWARE BY THE BRAZILIAN STATE: AN ANALYSIS FROM THE ATTEMPT TO CONTRACT THE PEGASUS ESPIONAGE SOFTWARE

ABSTRACT

Despite prima facie representing a considerable risk to fundamental rights and guarantees, invading software is routinely heralded as essential for the State to maintain control and exercise its police power. An example of this category of software is the spy malware Pegasus, which was the object of interest of the Brazilian government and which is capable of accessing devices and systems that contain data and confidential information without major difficulties and without leaving any traces. In this scenario and considering that discussions about the risks and the legality of using these tools have been increasingly heated, the present work aimed to shed light on this topic. To tackle the issue, the hypothetical-deductive method and legislative and bibliographical research are used. The results point to the existence of a significant normative framework still incapable of satisfactorily guiding the State and its agents in the use of these new technologies.
Keywords: Brazil. Cybersecurity. Personal data. New technologies. Public security. Software.

Data de Recebimento: 08/04/2024 **Data de Aprovação:** 24/07/2024
DOI: 10.31060/rbsp.2026.v20.n1.2166

INTRODUÇÃO

Em decorrência da familiaridade e facilidade do dia a dia proporcionadas pelo uso da internet e das novas tecnologias, tem sido cada vez mais comum a ocorrência de incidentes de segurança em sistemas e dispositivos privados e públicos; incidentes que focam especialmente na violação de mecanismos e *softwares* de segurança. Isso se dá pelo fato de que em um contexto de ciberespaço[1], no qual todos os indivíduos

1 Por ciberespaço se entende um ambiente artificialmente criado onde as relações sociais se desenvolvem e em que trafega uma quantidade avassaladora de dados, conforme definição feita por Willian Gibson em 1984, no livro *Neuromancer*. Contudo, vale destacar que o termo já havia sido utilizado anteriormente, pelo próprio autor em sua obra *Burning Chrome*, publicada em 1982.

em alguma medida estão inseridos, a coleta, o armazenamento e o tratamento de dados são manipulados em escala crescente. Fato é que, diante de tantas informações disponibilizadas nesse espaço virtual, a vulnerabilidade dos dados é elemento de preocupação, uma vez que tanto rede pública como rede privada pode ser acessada indiscriminadamente através de diversos *malwares*.

A proteção e segurança em ambiente digital é assunto urgente aos agentes particulares e entes públicos. Iniciativas políticas, técnicas e jurídicas têm despertado o interesse do Estado para a aquisição de mecanismos e ferramentas com capacidade de atacar sistemas de segurança.

Prova disso, o Estado brasileiro buscou pela aquisição do *spyware* Pegasus, propriedade de uma empresa de tecnologia israelense, a NSO Group Technologies, e também referenciado como *malware*. O *spyware* é considerado uma ferramenta de espionagem remota que realiza sofisticados ataques para acesso a dados e informações de localização e comunicação (SMS, voz e vídeo).

O Pregão Eletrônico nº 3/2021 chegou a ser aberto pelo Ministério da Justiça com valor de R$ 25,4 milhões, direcionado para a aquisição dessa ferramenta[2]. A participação da NSO Group foi confirmada no pregão eletrônico, mas, posteriormente, rumores confirmaram que a empresa havia desistido da licitação por motivos não justificados[3].

Esse cenário duvidoso abriu brecha para questionamentos e críticas a respeito da conduta na administração pública, na defesa e proteção dos direitos à liberdade e privacidade dos cidadãos brasileiros, além de inseguranças acerca da legalidade e da falta de critérios claros e bem definidos no que concerne ao uso de sistemas com as características do sistema Pegasus.

Nesse contexto, o artigo aponta diretrizes, regras e condições que, por um lado, devem nortear o agir estatal no que se refere à proteção dos indivíduos, identificados por seus dados no ciberespaço e, por outro, são fundamentais para o respeito e a proteção dos direitos e dos dados dos indivíduos. Nesse contexto, qual abordagem protetiva seria a prevalente?

A presente pesquisa apresenta probabilidades de resultados, favoráveis e não favoráveis, à solução da indagação. Para isso, se fez uso da legislação pátria e de bibliografia especializada na abordagem do tema, em especial, artigos científicos dedicados à temática de proteção e privacidade de dados e à cibersegurança.

O presente artigo está estruturado em três seções principais, seguidas pelas considerações finais. Na primeira seção, discute-se o contexto da segurança digital no Brasil, com ênfase no aumento das vulnerabilidades dos sistemas e dos dados, tanto no setor público quanto no privado. Abordam-se as noções e perspectivas sobre cibersegurança no cenário brasileiro, destacando-se a relevância das ferramentas tecnológicas na proteção e no combate a crimes cibernéticos.

A segunda seção trata da atuação do Estado na proteção de dados pessoais e na prevenção de ataques cibernéticos, com uma análise detalhada da legislação vigente e dos desafios enfrentados em sua aplicação.

2 A íntegra do processo licitatório não está mais disponível no site do Ministério da Justiça, contudo as informações quanto à sua abertura podem ser encontradas disponíveis em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/19/briga-entre-militares-e-carlos-bolsonaro-racha-orgaos-de-inteligencia.htm; https://www.conectas.org/noticias/tcu-mantem-veto-a-compra-de-sistema-espiao-pelo-governo-bolsonaro/. Acesso em: 21 jan. 2026.

3 Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/25/empresa-de-software-espiaopegasus-deixa-edital-que-e-rodeado-de-incertezas.htm. Acesso em: 21 jan. 2026.

Já na terceira e última seção, examina-se a polêmica em torno do uso do *software* Pegasus, explorando o equilíbrio entre a autonomia do poder estatal e a proteção dos direitos fundamentais dos cidadãos. Nas considerações finais, são retomados os principais pontos discutidos no artigo, reforçando a necessidade de um arcabouço normativo mais robusto para enfrentar os desafios impostos pelas novas tecnologias, visando à proteção efetiva dos dados pessoais e à garantia da segurança cibernética no Brasil. O artigo é resultado de projeto de pesquisa financiado pelo Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses (Procad/SPCF), da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes).

CIBERSEGURANÇA: NOÇÕES E PERSPECTIVAS NO CENÁRIO BRASILEIRO

A segurança em ambiente digital é uma preocupação crescente, não apenas para indivíduos e empresas, que investem cada vez mais em sistemas e mecanismos que sejam capazes de garantir maior proteção no que se refere à garantia da sua intimidade e privacidade e à inviolabilidade de seus equipamentos e ativos, como também ao Estado, historicamente alvo de ataques cibernéticos e que continua vulnerável a essas ameaças[4].

O tema da segurança digital não faz referência apenas ao campo da cibersegurança, entendida como um conjunto de práticas que visa proteger ativos de informação, sistemas, computadores e servidores, entre outros, contra ameaças cibernéticas ou ataques maliciosos (Bravo, 2021). A segurança digital inclui práticas e condutas que têm por objetivo combater e prevenir crimes praticados no ciberespaço.

É por isso que, diferentemente dos particulares, ao Estado também interessa adquirir mecanismos e ferramentas que sejam capazes de não apenas conferir segurança e proteção a seus ativos, mas também que lhes possibilite superar, ou mesmo burlar, sistemas de segurança quando estes forem um entrave à sua autoridade. Esse interesse advém da necessidade de o Estado fazer valer sua força coercitiva e seu poder de polícia em um ambiente onde o tempo e o espaço têm novas dimensões e onde o exercício das liberdades individuais e da cidadania se dá em novos formatos e com novas extensões e reflexos (Lévy, 1999).

Nesse sentido, conforme observam Mendes e Fernandes (2020, p. 12), em que pese esse espaço não ser um universo apartado e desconectado do mundo material, onde a força normativa da Constituição e das leis não produzem seus efeitos ou onde são deliberadamente desconsideradas, para que haja a sua territorialização e a, consequente, expansão do Estado de Direito para tais fronteiras, o agir estatal deverá, em certa medida, se ressignificar e ampliar. Essa ressignificação é fundamental para garantir a prevalência, o respeito e a efetividade dos direitos no ciberespaço.

E não se quer aqui fazer supor que com uma maior atuação estatal o mundo digital e virtual se tornará um local amplamente seguro e isento de condutas criminosas, visto que o ambiente físico, próprio do Estado, está longe de refletir essa realidade.

Busca-se tão somente jogar luz ao fato de que, por se desenvolver de modo muito mais intenso e multifacetado e por apresentar riscos que até pouco tempo sequer faziam parte das preocupações sociais[5], para que

4 Vários foram os ataques cibernéticos sofridos por órgãos e estruturas do governo brasileiro, os mais graves e que chamaram mais atenção na mídia foram os ataques suportados pelo Superior Tribunal de Justiça, em novembro de 2020, e pelo Tribunal de Justiça do Rio Grande do Sul, em junho de 2021.

5 Para um governo no final da década de 1990 ou no início dos anos 2000, era impensável ou mesmo considerado fantasia que sua estrutura social, financeira ou física pudesse ser posta em risco por uma ação conduzida e executada através de uma rede virtual de comunicação.

mantenha sua autoridade e supremacia, e mesmo para que se garanta sua continuidade, o Estado deverá lançar mão de novos instrumentos e mecanismos, sejam eles legais ou tecnológicos, ou mesmo, tecno-legais.

Não bastando essa complexidade própria do ambiente digital, a carência por uma atuação mais ampla e eficiente também se dá pelo fato de a sociedade digital deixar mais expostos e vulneráveis os cidadãos, exposição essa que advém do fato de que toda atividade que de alguma forma perpassa ou interage com o ambiente virtual apresenta fragilidades e expõe seus participantes a riscos[6] (Cavedon; Ferreira; Freitas, 2015).

Tal exposição pode ser justificada por vários motivos, mas especialmente pela sempre possível violação dos sistemas e mecanismos de segurança cibernética, pelo fato daquelas ações ocorrerem a partir da conexão de uma rede aberta e conectada mundialmente, que pode ser acessada por agentes não autorizados e pelo intenso fluxo de informações e dados que produzem e fazem trafegar em nível transnacional.

Não fossem suficientemente problemáticos esses fatores, em decorrência da transnacionalidade das ações, ainda que executadas unicamente em determinado território, não há como se falar em segurança e proteção em ambiente digital em nível nacional sem cooperação e *accountability* em nível internacional[7].

Tendo em vista que não apenas os cidadãos estão inseridos na teia do mundo digital, uma vez que sistemas e *softwares* são cada vez mais responsáveis por auxiliarem ou efetivamente fazerem a gestão da infraestrutura física e lógica (virtual) do Estado e de seus órgãos, intervenção essa que vai desde uma simples organização para a prestação de determinado serviço público até a operação de sistemas de segurança e de defesa aeroespacial, vê-se que o Estado, suas instituições e seus agentes estão também expostos. De outro lado, considerando que instrumentos tradicionais essenciais para o combate ao crime, tais como escutas telefônicas, quebras de sigilo telemático, entre outros, não são, em ambiente digital, suficientes para outorgar ao Estado a capacidade e a superioridade necessárias ao exercício pleno de seu poder de polícia e de sua autoridade.

Em decorrência disso e buscando garantir a segurança de seus ativos e de suas infraestruturas, o Brasil tem caminhado no sentido de modernizar e melhorar sua atuação, não apenas com a adoção de novas ferramentas tecnológicas, como discutido mais à frente neste artigo, mas também por meio de sua legislação.

A partir de uma normatização baseada não somente na segurança, mas também na defesa cibernética[8] e, em certa medida, na militarização do espaço virtual, o Estado brasileiro tem buscado inserir novos instrumentos tecnológicos, tais como a Aprendizagem de Máquina (*Machine Learning*) e o uso da inteligência artificial. Tais ferramentais são tratadas inclusive como fundamentais para a efetividade da Estratégia Nacional de Segurança Cibernética e das políticas públicas de segurança do ciberespaço, conforme Decreto nº 10.222, de 2020:

> Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais. Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incen-

6 Apesar de Mário Quintana, desde há muito, poetizar que viver, por si só, é um risco, não poderia imaginar o gaúcho que, em ambiente digital, mesmo as tarefas mais simples efetivamente são capazes de expor seus participantes a riscos, situações estas que de fato não acontecem no mundo físico.

7 Foi atenta a esta necessidade, que a Convenção de Budapeste (Conselho da Europa, 2001) veio reforçar e possibilitar a cooperação internacional na prevenção e punição dos crimes ocorridos no ambiente digital.

8 Segundo o Ministério da Defesa do Brasil, por defesa cibernética se compreende o "Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação" (Brasil, 2010).

> tivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão. [...]
> As ameaças cibernéticas [...] têm o escopo de alcançar grande número de organizações, inclusive as representantes das infraestruturas críticas, que, por prestarem serviços essenciais à sociedade, possuem elevado nível de criticidade. Por isso, essas organizações necessitam de meios para identificar, proteger, detectar, avaliar, responder, recuperar e assim gerenciar o risco das ameaças cibernéticas, e também de ferramentas de automação de segurança que usam inteligência artificial e aprendizado de máquina, que permitam analisar, identificar e conter os ataques cibernéticos. (Brasil, 2020).

Essa forma de agir do Estado conecta-se diretamente com o conceito de Estado enquanto ente detentor do monopólio sobre administração da força, desenvolvido por Weber (1985), na medida em que, para manter sua autoridade e legitimidade, o Estado moderno deve fazer uso do ordenamento legal para autorizar e legitimar o uso de novas ferramentas coercitivas que sejam capazes de lhe possibilitar a superação de obstáculos ou que possibilitem a limitação ou extinção de agentes que podem pôr em risco sua autoridade.

Outrossim, ao agir com vias a introduzir modernas ferramentas de tecnologia no arcabouço e na estrutural do Estado brasileiro e alçar a cibersegurança à política de Estado, o legislador acabou por transformá-la em política pública interdisciplinar que invariavelmente deverá congregar diversas áreas do conhecimento, tais como a Tecnologia da Informação (TI), a Matemática e o Direito público.

Apesar dessa conduta aparentemente atenta à evolução social e da análise sistemática das principais leis brasileiras que, em alguma medida, abordam a questão dos crimes cibernéticos, pode-se verificar que essas, na maioria das vezes, têm seu foco direcionado unicamente ao combate de crimes cibernéticos específicos, não focando no fenômeno do cibercrime propriamente dito.

Assim, a Lei nº 11.829/2008 (Brasil, 2008), que trata da pedofilia na Internet, a Lei nº 12.735/2012 (Brasil, 2012), que buscou determinar a criação de setores e equipes especializadas no combate aos delitos praticados nesse ambiente, a Lei nº 12.737/2012 (Brasil, 2012), popularmente conhecida como Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos, e o próprio Marco Civil da Internet – Lei nº 12.965/2014 (Brasil, 2014), quando analisadas conjuntamente não são suficientes para direcionar o Estado e suas instituições no que concerne a proteção do ciberespaço.

Resta observar ainda que tais estatutos buscam unicamente oferecer uma resposta aos incidentes já ocorridos, não dispondo acerca de quaisquer ações de prevenção de incidentes ou mesmo não trazendo diretrizes próprias de uma estratégia nacional para a defesa cibernética.

Nessa perspectiva, as normativas que mais detidamente abordam a temática do cibercrime e de sua prevenção são aquelas expressas por órgãos de segurança e de defesa, a exemplo do Ministério da Defesa e do Ministro de Estado da Justiça e Segurança Pública. A Portaria GSIPR nº 45, do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República[9], e a Estratégia Nacional de Defesa (END) do Brasil[10], aprovada pela primeira vez em 18 de dezembro de 2008, são exemplos nítidos dessa realidade.

9 A portaria do Gabinete de Segurança Institucional veio, entre outras coisas, instituir um Grupo de trabalho cujo objetivo é "propor diretrizes e estratégias para a Segurança Cibernética no âmbito da Administração Pública Federal" (Brasil, 2008).

10 A Estratégia Nacional de Defesa (END), além de estabelecer as diretrizes para a preparação e capacitação das Forças Armadas, com vias a garantir a segurança do Estado brasileiro em períodos de paz ou de guerra, também se detém em estabelecer as premissas e condições para a defesa cibernética.

Essa forma de agir se dá pelo fato de que muito embora o ambiente digital não tenha sido criado com fins militares, nem mesmo com o objetivo de interferir na infraestrutura e na segurança interna dos estados, atualmente é o foco das atenções e tem a capacidade de assim favorecer tais interferências; dessa forma, possuir as competências necessárias para proteger seu espaço cibernético torna-se questão de interesse especial dos órgãos encarregados da defesa e segurança nacional.

Apesar de toda essa preocupação, e como observam Cavedon, Ferreira e Freitas (2015), para a garantia de um ambiente digital seguro e para o combate aos crimes e ataques cibernéticos, não basta apenas garantir o uso de novos mecanismos e sistemas de tecnologia, nem mesmo alçar a ciência que cuida desse campo (cibersegurança) à condição de política pública; se faz necessário, sobretudo, a criação, o domínio e a manutenção de sistemas de segurança de informática, de investimento em recursos físicos e intelectuais e de implantação de estruturas de segurança computacional relativas aos sistemas e dados.

Na mesma medida, não basta que o ordenamento jurídico introduza novos conceitos ou ferramentas à prática judicial, se fazendo mesmo necessário a adoção de certa dinamicidade capaz de possibilitar uma abordagem multifacetada, inovadora e que inclua outros ramos do conhecimento (Cavedon; Ferreira; Freitas, 2015).

A ATUAÇÃO DO ESTADO NA PROTEÇÃO DE DADOS E NO COMBATE A ATAQUES CIBERNÉTICOS

Historicamente, o Brasil vem ganhando espaço na constante busca pela proteção aos dados pessoais em consequência da velocidade avassaladora e, por vezes, incontrolável que a evolução tecnológica alimenta o cotidiano social com diversos aplicativos, sites e redes sociais, evidenciando, ainda mais, a necessidade em reforçar a tutela de dados perante essa atual conjuntura.

Quando se ressalta a importância na tutela aos dados pessoais, refere-se igualmente à preservação da privacidade dos titulares de dados. Esse direito personalíssimo, ligado ao direito à intimidade e ao princípio da dignidade da pessoa humana, ressoa em diversos tratados e convenções internacionais, como a Declaração dos Direitos do Homem e do Cidadão (Assembleia Nacional Constituinte Francesa, 1789), a Declaração Universal dos Direitos do Homem (ONU, 1948) e a Convenção Europeia dos Direitos do Homem (Conselho da Europa, 1950), bem como se faz presente no Código Civil Brasileiro (Brasil, 2002) e, principalmente, na Constituição Federal do Brasil de 1988, que prevê no art. 5º, inciso X, que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material decorrente de sua violação" (Brasil, 1988).

A imersão populacional na chamada "sociedade da informação", ao mesmo passo que informatizou determinadas ações, facilitando a dinâmica na coleta e transmissão de dados, também colocou em risco a violação de direitos e garantias fundamentais, ameaçando a manutenção da democracia.

E quando se refere à democracia, Saldanha, Brum e Mello (2016) a relacionam diretamente com a informação, sob o argumento de que a informação é elemento essencial e indispensável para o controle democrático das instituições e está diretamente ligada ao direito de acesso à informação (Brasil, 2011) e ao respeito aos direitos fundamentais.

Ocorre que os instrumentos de tecnologia, atualmente, são considerados pontes de acesso à informação e, por consequência, uma condição para a garantia dos direitos individuais de liberdade (Saldanha; Brum; Mello, 2016).

Convém lembrar que, a partir da visão de Bobbio e Bovero (2000), inexiste a possibilidade do exercício da democracia se o poder for exercido de forma oculta, ou seja, para que o governo consiga estabelecer uma relação democrática entre os cidadãos deve tornar seus atos e decisões públicos, de forma que nada seja feito sem passar pela aprovação dos maiores interessados, isto é, daqueles que os elegeram.

Esse pensamento se aproxima da descrição da Lei nº 12.527 de 2011, Lei de Acesso à Informação (LAI), tendo em vista que objetiva fazer com que o Poder Público informe e seja transparente quanto aos seus atos, prestando contas sobre suas decisões à população (Brasil, 2011).

A LAI trouxe significativo avanço democrático no fomento ao acesso à informação e à transparência da Administração Pública, mas Carvalho (2014) indica uma tensão perante a utilização de dados considerados públicos. Isso porque, mesmo com a autorizada utilização desses dados, tais dados continuam na esfera privada do titular. Desse modo, torna-se frágil a relação entre os dois polos (público e privado), uma vez que a própria LAI, na redação dos art. 3º e 4º, enfatiza a prevalência ao direito à informação sobre o direito à intimidade (Brasil, 2011).

Em análise do conflito apresentado de informação *versus* privacidade, no que diz respeito aos dados pessoais, principalmente ao se levar em conta os princípios que norteiam a Administração Pública, Flôres e Silva (2020) apontam um problema central: a falta de previsão legislativa específica que proteja dados e imponha ao Poder Público limites quanto à sua coleta e divulgação.

No ímpeto de haver transparência com relação ao tratamento de dados, entrou em vigor a Lei Federal nº 13.709, de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que dispõe sobre o "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural" (art. 1º), devendo ser observada pela União, pelos estados, pelo Distrito Federal e pelos municípios. Ou seja, ela regula o tratamento de dados pessoais realizado por pessoa jurídica de direito público ou privado, aí incluídos a Administração direta e indireta, inclusive fundações, empresas públicas e sociedades de economia mista (Brasil, 2018).

Ao analisar o texto da LGPD, na disposição do seu art. 2º, é possível visualizar os fundamentos que inspiram e sustentam a proteção de dados, a saber: i) a autodeterminação informativa; ii) a liberdade de expressão, de informação, de comunicação e de opinião; iii) a inviolabilidade da intimidade, da honra e da imagem; iv) o desenvolvimento econômico e tecnológico e a inovação; v) a livre iniciativa, a livre concorrência e a defesa do consumidor; e por fim, vi) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas (Brasil, 2018).

Em seu art. 7º, a LGPD apresenta as hipóteses autorizadoras para o tratamento de dados pessoais, assim como prevê os requisitos para a sua execução (Brasil, 2018). No entanto, ainda que a situação fática ora discutida se enquadre nas expressões dos incisos III e VII do referido artigo, é imprescindível ter em mente que, além de existirem limites para a coleta e o tratamento desses dados, o princípio da boa-fé e da razoabilidade devem nortear esse tratamento.

A validade da operação de tratamento de dados depende, em especial: a) do enquadramento da situação fática em um dos incisos do art. 7º; b) da observância dos princípios de proteção listados no art. 6º; e c) do respeito ao princípio da boa-fé objetiva.

Especificamente no caso do setor público, o tratamento de dados pessoais, além do dever de obediência aos princípios do art. 6º e da boa-fé, somente poderá ser realizado se estiver relacionado à "execução de políticas públicas revistas em lei, regulamentos, convênios, contratos administrativos e instrumentos congêneres" (art. 7º, inciso III) ou para cumprimento de obrigação legal ou regulatória pelo controlador, no caso pela Administração Pública (art. 7º, inciso II) (Brasil, 2018).

Além dos critérios para coletar dados dos titulares, a legislação impõe à rigor um dos elementos de extrema importância: o consentimento fornecido pelo titular de dados (art. 7º, inciso I). Em regra, a LGPD estabelece que as operações de tratamento somente poderão ocorrer mediante o consentimento[11] do titular de dados, entretanto algumas peculiaridades envolvem essa regra de ouro da legislação.

Para ser válido, é necessário que o consentimento fornecido pelo titular seja de forma inequívoca, livre, desembaraçada e sem vícios, no bojo do qual ele manifesta sua concordância com o tratamento de seus dados pessoais com finalidade e prazo determinados (art. 5º, inciso XII) (Brasil, 2018).

Apesar de existir essa previsão, que, em regra, deve ser sempre observada, a LGPD normatiza que, em casos excepcionais e necessários, será dispensada a exigência do consentimento expresso do titular. Neste caso, o § 4º do art. 7º anuncia a dispensa do consentimento nos casos em que os dados coletados sejam manifestamente públicos, pela atuação do próprio titular e quando houver necessidade de disponibilizá-los, devendo se levar em conta a finalidade, a boa-fé e o interesse público (Brasil, 2018).

Até pouco tempo, o ente estatal era visto como o detentor de posição proeminente, devido ao fato do interesse público possuir superioridade hierárquica em relação ao interesse individual. No entanto, soa o alerta para a necessidade de se implementar mecanismos de ação adequados a conferir poder ao titular de dados na autodeterminação de fornecer, fiscalizar, questionar, solicitar e requerer a finalidade da coleta e a exclusão do banco de dados (Bioni, 2019).

Outro ponto importante no estudo é a exploração do aspecto de segurança como fator obrigatório disposto pela LGPD no armazenamento de dados. Quando se trata acerca de sistemas no qual ocorre o compartilhamento de dados, em especial dados pessoais, é essencial elevar o entendimento aos protocolos de segurança aos quais esses sistemas deverão submeter-se, para garantir ao titular a privacidade e a integridade na guarda, no armazenamento e no compartilhamento de dados e informações.

Algumas técnicas baseadas em tecnologia computacionais, ciências forenses, computação forense e engenharia social podem ampliar o arquétipo de segurança da informação de uma organização, a partir da implementação de: uma política de segurança adequada, utilização de mecanismos de proteção físicos e lógicos, incentivo ao uso de sistemas de detecção de intrusão, criptografia, segurança física, dentre outros mecanismos (Velho, 2016).

11 No que tange à aplicação do poder de polícia ou à realização de atividades relacionadas à defesa ou à segurança pública, o consentimento do indivíduo envolvido não é necessário. Nessas situações, o poder estatal prevalece em razão do interesse público. Entretanto, fora desses contextos específicos, a necessidade de consentimento pode variar conforme a natureza da atividade ou o tratamento de dados em questão, especialmente em ambientes que envolvem a proteção de direitos fundamentais, como a privacidade e a intimidade dos cidadãos.

Merece destaque a área de Segurança da Informação, a qual, de acordo com a Norma ABNT NBR ISO/IEC 17799[12], Segurança da Informação é:

> A proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio. (ABNT NBR ISO/IEC 17799, 2005).

E, por sua vez, a Segurança da Informação tem por base algumas propriedades, a saber: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas[13].

Para garantir adequada proteção aos seus ativos de informação, é necessário que a organização empresarial e seus principais gestores levantem e selecionem soluções específicas adequadas ao modelo de negócio específico. O mesmo deve ocorrer com o setor público, principalmente frente às necessidades e exigências de Serviços de Inteligência, Inteligência Analítica, Cibersegurança e Policiamento Preditivo, sendo esses alguns exemplos de aplicação que requerem a Segurança da Informação como objeto e foco central.

Grande parte dos dados que compreendem a estrutura informacional de uma organização, pública ou privada, é armazenado em computadores, o que evidencia a preocupação na confiabilidade de sistemas baseados em tecnologias da informação (TI). Silva Netto e Silveira (2007) afirmam que na medida em que essa confiança no armazenamento de dados for destruída, o impacto pode ser comparável à destruição do próprio sistema.

Para Peron (2019, p. 1): "A Segurança Preditiva vem sendo entendida como um novo paradigma de segurança pública frente aos aspectos de vigilância dos Estudos sociais, da Ciência e da Tecnologia e, também, em certa medida da Sociologia da Punição". O autor discute a Segurança Preditiva apoiada em dispositivos de vigilância associados às técnicas de automatização do processamento de dados e às Tecnologias de Informação e Comunicação (TIC). O trabalho de Peron (2019) é atual e discute também o uso dos dados e a aplicação de técnicas de Mineração de Dados (*Data Mining*), a qual, por sua vez, está inserida na área de Inteligência Artificial e Aprendizagem de Máquina (*Machine Learning*). O autor explica que vazamento de dados, tal qual o apontado pela agência de jornalismo investigativo *The Intercept*, em 2015, "revelou que um sistema desenvolvido para o cruzamento de dados obtidos pelos Drones, Skynet, é capaz de angariar dados para a construção de padrões de vida a partir de dados produzidos por redes sociais" (Peron, 2019, p. 5). Essa construção de padrões que o autor menciona está relacionada com as técnicas de Inteligência Artificial e Aprendizagem de Máquina (*Machine Learning*).

12 A partir de 2007, a norma ISO/IEC 17799 foi incorporada ao novo sistema de numeração de normas, passando a constar como ISO/IEC 27002 (ABNT, 2005, p. ix).

13 A partir de 2007, a norma ISO/IEC 17799 foi incorporada ao novo sistema de numeração de normas, passando a constar como ISO/IEC 27002 (ABNT, 2005, p. ix).

Desse modo, Peron (2019, p. 7) explica que a Segurança Preditiva, por contar com o apoio de tais dispositivos (a exemplo dos drones), assim se caracteriza "por um conjunto heterogêneo de práticas, instrumentos e saberes orientados a detectar comportamentos discrepantes e nocivos". Aqui se deve observar que o comportamento discrepante ou nocivo pode advir de indivíduos ou *softwares*, a exemplo das inúmeras categorias de *malware*.

O risco é eminente. Por isso, tais aplicações podem ser de interesse de Estados quando o tema é terrorismo, guerra urbana ou civil, guerra militar e, também, a guerra cibernética.

Pela capacidade que dados, informação e conhecimento tendem a adicionar valor a processos, produtos e serviços, estes também constituem recursos cada vez mais críticos para o alcance da missão e do objetivo organizacional (Caruso; Steffen, 1999). Assim, para o melhor enfrentamento de vulnerabilidades, redução de ameaças, riscos e exposições, é necessário construir um conjunto adequado de controles, orientado por políticas, processos, procedimentos, estruturas organizacionais e funções de *softwares* e *hardwares* capazes de agir como medidas agregadas à cibersegurança (Hintzbergen *et al.* , 2018).

A cibersegurança, em sentido estrito, é definida como conjunto de atividades que se destinam a proteger sistemas informáticos (tal como definido no art. 2º da Lei do Cibercrime nº 109/09) e os dados informáticos neles contidos, mantendo-se à salvo da ocorrência de dano intencional ou do uso negligente (Bravo, 2021).

Com o objetivo de estabelecer estrutura e modelo de governança para a integração e a coordenação nacional das atividades de Segurança da Informação, em um cenário de crescentes ataques cibernéticos e elevada interdependência das tecnologias da informação e comunicação, assim como evitar superposições, concorrências e redundâncias de ações e tarefas que acabam afetando o cidadão e o Estado brasileiro, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) coordenou uma série de ações.

Dentre elas, por meio do Decreto nº 9.637, de 26 de dezembro de 2018, foi instituída a Política Nacional de Segurança da Informação (PNSI), no âmbito da administração pública federal, que tem a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e autenticidade da informação em âmbito nacional (Brasil, 2018).

A segurança cibernética da informação é elemento em destaque na implementação da PNSI, especialmente em relação à mitigação de riscos e ao combate às ameaças em eminência que podem comprometer a segurança pública, por esse motivo, o Ministério de Defesa torna-se aliado na elaboração de dispositivos e mecanismos que atuem na defesa nacional.

Mesmo com toda a preparação técnica e legal criada para ampliar a segurança dos sistemas nacionais que guardam dados e informações, por vezes sigilosos, estes são e sempre serão alvo de ataques cibernéticos. Os noticiários confirmaram uma sequência de vazamentos, denunciando a vulnerabilidade no acesso aos sistemas do Governo Federal, conforme já exposto.

Motivado por essas razões, o presidente da República editou o Decreto nº 10.748, de 16 de julho de 2021, para instituir a Rede Federal de Gestão de Incidentes Cibernéticos, objetivando a prevenção de ameaças cibernéticas e a elevação do nível de resiliência em segurança cibernética dos ativos de informação que guardam os órgãos e das entidades da administração (Brasil, 2021).

Os primeiros parágrafos mencionam a obrigatoriedade de adesão por parte das entidades da administração pública federal direta, autárquica e fundacional, enquanto para empresas públicas e sociedades de economia mista federal podem optar voluntariamente participar, por meio de adesão (Brasil, 2021)

No delineado dessas circunstâncias, pouco se pode prever sobre o cumprimento dos dispositivos legais apontados, tanto pelo poder público quanto pelo privado. No entanto, o que se sabe é a frequência com que as ferramentas tecnológicas de invasão seguem ultrapassando os limites criados pela segurança cibernética, inclusive pela administração pública.

E é a partir desse ponto que surgem diversos questionamentos a respeito do exercício pleno do dever do Estado em cumprir legalmente com a proteção de direitos fundamentais e individuais, além de manter a transparência em suas ações perante a coletividade.

A FORMA DE ATUAÇÃO DO PEGASUS E A CONTRADIÇÃO ENTRE A AUTONOMIA DO PODER DO ESTADO E OS DIREITOS FUNDAMENTAIS

Ao longo dos anos, diversas ferramentas e mecanismos seguem sendo criados, adquiridos e contratados, quer seja por forças polícias, órgãos de repressão, instituições do Estado, ou mesmo, por outros entes federativos, com vias a melhor capacitar e direcionar o agir estatal. No mesmo sentido, cumpre destacar que ações investigativas baseadas em espionagem ou contra vigilância sempre encontraram lugar no rol de ações praticadas pelo Estado, a exemplo de: interceptações telefônicas, quebras de sigilo telemático e escutas em ambientes.

Isso acontece pelo fato de que dados e informações sempre foram recursos indispensáveis ao exercício do poder por parte dos Estados, sejam eles autoritários ou democráticos. E em um contexto social marcado por uma constante vigilância e intensa produção e compartilhamento de dados, conforme apontam Foucault (1987), Lévy (1999) e Castells (2007), ações que possam conferir ao Estado vantagem nessas circunstâncias ganham dimensões ainda maiores e, por consequência, complexas.

Foi sob a justificativa de melhorar a capacidade investigativa e de prevenção a crimes no espaço cibernético que, em um controverso processo licitatório, o governo brasileiro tentou adquirir o *software* Pegasus, programa de computador classificado como *malware*.

Embora haja diversas categorizações de *malware*, o reconhecimento e a definição de um código malicioso é dado a partir da identificação das formas de atuação desses *softwares* em sistema computacionais desde os sistemas operacionais, a exemplo de: técnicas de ofuscação, ciclos de operação, *download* de arquivos, captura de informações, dentre outras atividades imprescindíveis para essa caracterização (Fernandes Filho *et al.*, 2011). Dentre esses aspectos, o Pegasus se destaca por possuir a quase totalidade dessas capacidades.

Conforme destacado por Ivar Hartmann do Insper[14], ter o Pegasus instalado em um celular é, por exemplo, mais do que uma simples escuta telefônica, significaria ter um policial 24 horas acompanhando as

14 A exemplificação foi feita pelo Prof. Ivar Hartmann no podcast "Big Data Vênia", disponível em: https://www.youtube.com/watch?v=GYwy4mVzUYo. Acesso em: 8 set. 2021.

atividades executadas naquele aparelho, acompanhamento este que incluiria a possibilidade de copiar, baixar e compartilhar todo e qualquer dado armazenado no aparelho.

A possível utilização desse *malware*, ou de outro com características semelhantes, como ferramenta investigativa que se preste à coleta[15] de dados pessoais de indivíduos supostamente ou comprovadamente envolvidos na prática de crimes, se caracteriza, diferentemente das ações investigativas já previstas no arcabouço jurídico brasileiro, como dinâmica operacional com grande capacidade de expor não somente seus destinatários a riscos, mas toda a sociedade, na medida em que tal sistema pode ser utilizado sem qualquer fiscalização por parte dos outros órgãos de controle do Estado.

Ademais, o interesse do Estado em adquirir uma ferramenta que opera a partir de técnicas de constante vigilância e que emprega indiscriminadamente métodos de espionagem, sem qualquer discussão prévia, em um contexto no qual inexiste uma normativa que de forma detida e transparente aborde seu uso, tem o condão de colocar em risco todo o rol de direitos e liberdades individuais consolidados no texto constitucional.

E quando se defende aqui a inexistência de um arcabouço normativo que seja suficiente para direcionar e estabelecer as balizas e os *standards* mínimos que devem ser observados quando do eventual uso dessas ferramentas, menciona-se em decorrência do fato de existirem mesmo questionamentos do ponto de vista dos direitos fundamentais acerca da legalidade e constitucionalidade do uso desses mecanismos, uma vez que se tem como fundamento o fato de que, mesmo a partir de uma análise sistemática de todas as normativas legais expostas no presente trabalho, ainda restariam dúvidas acerca do emprego e dos limites de atuação desses sistemas baseados em programas maliciosos (*malware*).

Ademais, a insuficiência de diretrizes que sejam capazes de direcionar o agir estatal de forma detida e dentro dos limites estabelecidos pela Constituição, invariavelmente, pode acabar outorgando aos membros e às instituições do Estado, tais como as forças policiais, os agentes de segurança e membros do ministério público e do poder judiciário, a faculdade de determinar, conforme o caso, o uso de tais ferramentas. Fato este que fragiliza ainda mais os ideários de liberdade e proteção à intimidade e privacidade dos cidadãos presentes tanto na Constituição quanto nas recentes legislações, a exemplo da Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018) ou da Lei nº 14.155, de 27 de maio de 2021 (Brasil, 2021), a qual torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela Internet (Brasil, 2021).

E mesmo que o judiciário faça uso, ainda que de forma analógica, das regras estabelecidas no Código de Processo Penal – Decreto Lei nº 3.689/1941 (Brasil, 1941), da Lei nº 13.964/2019, que veio aperfeiçoar a legislação penal e processual penal, e é popularmente conhecido como Pacote Anticrime (Brasil, 2019), e da Lei nº 9.296/1996 (Brasil, 1996), que aborda as questões de interceptação de comunicações telefônicas e escuta ambiental, ainda assim, por conta da complexidade e da ampliação técnica dessas novas ferramentas, ao juiz restaria a tarefa hercúlea e por demais expansiva de estabelecer as premissas para o emprego dessas novas tecnologias.

E na medida que a Constituição se preocupou de modo significativo não apenas com a temática da proteção da intimidade e da privacidade dos dados dos cidadãos, mas também com o todo o processamento e com a utilização de dados e informações que pudessem afetar "não apenas os direitos fundamentais

15 Maiores informações acerca do modo de funcionamento do Pegasus disponíveis em: https://portal.fgv.br/artigos/pegasus-cavalo-troia-seguranca-cibernetica. Acesso em: 08 set. 2021.

que expressamente regulam o fenômeno da informação" (Mendes, 2018, p. 193), mas também os demais direitos fundamentais, tal tarefa deverá se dar a partir das premissas presentes no texto constitucional.

Acerca dessas premissas constitucionais, os ensinamentos de Laura Schertel Mendes são norteadores:

> Objeto de proteção constitucional é o processamento e a utilização dos dados e informações pessoais em geral. A relevância jurídica reside menos nos dados em si, mas no processo de coleta, armazenamento, utilização ou transferência, a partir do qual são extraídas informações pessoais a serem utilizadas em um determinado contexto para determinados fins. Assim, entra em ação a proteção constitucional se a informação for usada para uma finalidade que cause riscos aos cidadãos, ou para fins considerados ilícitos a priori (como é o caso, por exemplo, de bancos de dados criados para fins discriminatórios). Assim, somente uma análise do contexto do uso das informações (ou das hipóteses previstas para a sua utilização), do conteúdo da informação, da finalidade de sua utilização e dos riscos envolvidos para o cidadão pode determinar a legitimidade de uma ação de tratamento de dados ou informações pessoais.
>
> O bem jurídico protegido por esse direito é duplo. Ele visa proteger, por um lado, a integridade moral da pessoa, como componente essencial da dignidade humana, e, por outro, as liberdades em sentido amplo (como a liberdade de comunicação, de trabalho, de locomoção, de informação, entre outras). (Mendes, 2018, p. 193).

Percebe-se, a partir dessas considerações, que a questão do acesso e do processamento de dados pessoais a partir da perspectiva constitucional acarretará uma compreensão multifacetada e ambivalente de proteção, na medida em que a garantia e o respeito aos direitos fundamentais comportarão não somente aqueles direitos fundamentais que a esta estão diretamente vinculados.

E, se por um lado, as novas tecnologias emergem como ferramentas capazes de instrumentalizar a realização dos objetivos do constitucionalismo, em especial no que se refere ao exercício, ao controle e à regulação do poder e da autoridade do Estado, por outro, ela também exigirá novas conformações protetivas de direitos fundamentais que estão em jogo no ambiente digital.

CONCLUSÃO

Por todo o exposto, entende-se que a utilização de novos mecanismos e ferramentas tecnológicas já é uma preocupação latente e presente por parte do Estado brasileiro. Esse fato é expresso tanto pela legislação, que nos últimos anos tem se dedicado intensamente em tutelar questões relacionadas à privacidade, à intimidade e aos dados cedidos por cidadãos brasileiros, quanto pela sua intenção em possuir instrumentos que sejam capazes de lhe conferir maior capacidade de vigilância e de controle no ambiente digital perante a sociedade.

Apesar disso, e especificamente em relação ao uso de tecnologias por parte da administração púbica, o arcabouço legislativo nacional tem se mostrado insuficiente para lidar com todas as problemáticas que o emprego desses novos instrumentos enseja, em especial no que se refere ao respeito aos direitos e às garantias fundamentais dos indivíduos que nesse ambiente se apresentam de forma multifacetada.

Ainda que as justificativas apresentadas ao emprego de novos instrumentos tecnológicos por parte do Estado estejam fundamentadas, seu uso deve estar pautado em premissas e questões fundamentais à manutenção do projeto constitucional elegido e adotado pelo constituinte em 1988.

Além disso, ao conferir a capacidade do Estado em operar com mecanismos satisfatórios de fiscalização, tais ferramentas tecnológicas, a exemplo do sistema Pegasus, podem colocar em risco toda a noção de separação de poderes, freios e contrapesos e devido processo legal, na medida em que essa execução é capaz de desequilibrar toda relação de forças até então existente.

Ante a ausência de melhores técnicas normativas, em decidido pelo Estado brasileiro pelo emprego de mecanismos de controle e vigilância mediante a aquisição do Pegasus, é essencial considerar a sistemática das legislações abordadas no presente trabalho à luz da Constituição, responsável por direcionar e impedir eventuais abusos por parte do Estado. Essa análise deverá contar não somente com o cuidado e a proteção aos direitos fundamentais diretamente vinculados à intimidade e privacidade, mas também estender-se aos direitos fundamentais que, em alguma medida, podem ser impactados pela nova realidade digital.

REFERÊNCIAS

ASSEMBLEIA NACIONAL CONSTITUINTE FRANCESA. **Declaração dos Direitos do Homem e do Cidadão**. França, 26 ago. 1789. Disponível em: http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/declaracao-de-direitos-do-homem-e-do-cidadao-1789.html. Acesso em: 28 set 2021.

Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 17799:2005**. Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOBBIO, Norberto; BOVERO, Michelangelo (Orgs.). **Teoria Geral da Política**: a filosofia política e as lições dos clássicos. Tradução: Daniela Beccaccia Versiani. Rio de Janeiro: Campus, 2002.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988.

BRASIL. **Decreto nº 10.748, de 16 de julho de 2021**. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Diário Oficial da União, Brasília, DF, 19 jul. 2021.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação. Diário Oficial da União, Brasília, DF, 27 dez. 2018.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. *Diário Oficial da União*: seção 1, Brasília, DF, 6 fev. 2020.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Diário Oficial da União, Rio de Janeiro, RJ, 13 out. 1941.

BRASIL. Gabinete de Segurança Institucional. Portaria Nº 2, de 8 de fevereiro de 2008. Institui Grupos Técnicos de Segurança de Infra-estruturas Críticas (GTSIC) e dá outras providências. Brasília/DF: **Diário Oficial da União**, ano CXLV, n. 27, Seção 1, 11 fev. 2008.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002.

BRASIL. **Lei nº 11.829, de 25 de novembro de 2008**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar condutas relacionadas à pornografia infantil na internet. *Diário Oficial da União*: seção 1, Brasília, DF, 26 nov. 2008.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º da Constituição Federal. Diário Oficial da União, Brasília, DF, 18 nov. 2011.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal (Pacote Anticrime). Diário Oficial da União, Brasília, DF, 24 dez. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa**. Brasília/DF, 2010.

BRASIL. **Portaria GSIPR nº 45, de 13 de julho de 2009**. Institui diretrizes para a Política de Segurança da Informação e Comunicações da Administração Pública Federal direta e indireta. *Diário Oficial da União*: Brasília, DF, 14 jul. 2009.

BRASIL. Secretaria de Assuntos Estratégicos. **Desafios estratégicos para a segurança e defesa cibernética**. Brasília: SAE, 2011.

BRAVO, Roger. **Segurança da Informação, CiberSegurança e CiberCrime**: contributos para um alinhamento de conceitos. Lisboa, 2021. Disponível em: https://www.academia.edu/40494857/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o_e_ciberseguran%C3%A7a_aspetos_pr%C3%A1ticos_e_legisla%C3%A7%C3%A3o. Acesso em: 31 ago. 2021.

CARUSO, Carlos; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**. São Paulo: Senac São Paulo, 1999.

CARVALHO, Igor Chagas de. A tensão entre o direito à informação e o direito à privacidade e o acesso aos arquivos sensíveis. **Revista de Informação Legislativa**, Brasília/DF, v. 51, n. 202, p. 115-130, 2014. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/503040. Acesso em: 10 ago. 2021.

CASTELLS, Manuel. **A galáxia internet**: reflexões sobre internet, negócios e sociedade. Tradução: Rita Espanha. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007.

CAVEDON, Ricardo; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. O meio ambiente digital sob a ótica da Teoria da Sociedade de Risco: os avanços da informática em debate. **Revista Direito Ambiental e Sociedade**, Caxias do Sul/RS, v. 5, n. 1, 2015.

CONSELHO DA EUROPA. **Convenção Europeia dos Direitos do Homem**: com as modificações introduzidas pelos Protocolos nos 11, 14 e 15, acompanhada do Protocolo adicional e dos Protocolos nos 4, 6, 7, 12, 13 e 16. França: Conselho da Europa, 1950. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf. Acesso em: 28 set. 2021.

CONSELHO DA EUROPA. **Convenção de Budapeste**. Budapeste, 23 nov. 2001. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci-en/rules-and-legislation/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 18 ago. 2021.

FERNANDES FILHO, Dário Simões; AFONSO, Vitor Monte; MARTINS, Victor Furuse Martins; GRÉGIO, André Ricardo Abed Grégio; GEUS, Paulo Lício de Geus; JINO, Mario; SANTOS, Rafael Duarte Coelho dos Santos. Técnicas para análise dinâmica de malware. *In*: **Anais** do XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. São Paulo: Unicamp – Universidade Estadual de Campinas, 2011, p. 104-144. Disponível em: https://www.lasca.ic.unicamp.br/paulo/papers/2011-SBSEG-Minicurso-dario.fernandes-vitor.afonso-victor.martins-andre.gregio-mario.jino-rafael.santos.pdf. Acesso em: 28 set. 2021.

FLÔRES, Flôres; SILVA, Silva. Segurança da informação e sociedade digital. Curitiba: Juruá, 2020.

FUNDAÇÃO GETULIO VARGAS. **Pegasus: o cavalo de Troia da segurança cibernética**. Disponível em: https://portal.fgv.br/artigos/pegasus-cavalo-troia-seguranca-cibernetica. Acesso em: 8 set. 2021.

GIBSON, William Gibson. **Neuromancer**. New York: Ace Books, 1984.

GIBSON, William Gibson. **Burning Chrome**. New York: Ace Books, 1982.

HINTZBERGEN, Jule; SMULDERS, André; BAARS, Hans; HINTZBERGEN, Saskia. **Foundations of information security management**. Cham: Springer, 2018.

QUINTANA, Mário Quintana. **Baú de Espantos**. Porto Alegre: L&PM, 1986.

FOUCAULT, Michel. **Vigiar e Punir**: nascimento da prisão. Tradução: Raquel Ramalhete. Petrópolis: Vozes, 1987.

LÉVY, Pierre. **Cibercultura**. Rio de Janeiro: Editora 34, 1999.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte/MG, ano 12, n. 39, p. 185-216, 2018.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Brasileira de Direito**, Passo Fundo/RS, v. 16, n. 1, p. 1-33, out. 2020. ISSN 2238-0604. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/4103. Acesso em: 12 jul. 2021.

ONU – Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos**. Assembleia Geral das Nações Unidas, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 28 set 2021.

PERON, Alcides Eduardo dos Reis. **Segurança preditiva? A incorporação de técnicas de mineração de dados e perfilização em conflitos internacionais com drones pelos EUA e em práticas de vigilância pela Polícia Militar do Estado de São Paulo**. In: **SIMPÓSIO INTERNACIONAL LAVITS, 4., 2016, Buenos Aires**. *Anais do IV Simpósio Internacional LAVITS: Novos paradigmas da vigilância? Miradas desde América Latina.* Buenos Aires: LAVITS, 2016. p. 1-15.

SALDANHA, Jânia Maria Lopez; BRUM, Márcio Morais; MELLO, Rafaela da Cruz. As novas tecnologias da informação e comunicação entre a promessa de liberdade e o risco de controle total: estudo da jurisprudência do sistema interamericano de direitos humanos. **Anuario Mexicano de Derecho Internacional**, v. 16, p. 461-498, 2016. Disponível em: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542016000100461&lng=es&nrm=iso. Acesso em: 10 ago. 2021.

SILVA NETTO, Abner; SILVEIRA, Marco Antônio Pinheiro. Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão a Tecnologia e Sistemas da Informação**, São Paulo, v. 4, n. 3, p. 375-397, 2007. Disponível em: https://www.scielo.br/j/jistm/a/Vx8Ypv6mDjxdYkKKrfYVgqz/?lang=pt&format=pdf. Acesso em: 26 jul. 2021.

VELHO, Jesus Antonio (Org.). **Tratado de computação forense**. Campinas: Millennium, 2016.

WEBER, Max. **Ciência e Política**. Duas vocações. São Paulo: Cultrix, 1985.

REVISTA BRASILEIRA DE SEGURANÇA PÚBLICA