A PROTEÇÃO DE DADOS PESSOAIS POR AGENTES DE PEQUENO PORTE: A GOVERNANÇA E AS BOAS PRÁTICAS COMO ESTRATÉGIAS DE IMPLEMENTAÇÃO DA LGPD

THE PROTECTION OF PERSONAL DATA BY SMALL AGENTS: GOVERNANCE AND GOOD PRACTICES AS STRATEGIES FOR IMPLEMENTATION OF LGPD

Rosane Leal da Silva[1]
Raonny Canabarro Costa da Silva[2]
Katiele Daiana da Silva Rehbein[3]

REVISTA MERITUM • v.18 • n.1 • p. 35-54 • Jan. - Abr. 2023

RESUMO

Este artigo aborda a proteção de dados pessoais, partindo de sua evolução histórica até a edição da Lei Geral de Proteção de Dados Pessoais Brasileira (LGPD). Neste ponto, concentra-se nos desafios para a sua implementação, sobretudo no que se refere à segurança da informação a ser promovida por agentes de tratamento de pequeno porte. A investigação tem como objetivo identificar e compreender o estado atual da proteção de dados no Brasil, para responder ao seguinte problema de pesquisa: quais os desafios para a efetivação da segurança dos dados pessoais processados por agentes de tratamento de pequeno porte? Para tanto, com apoio no método dedutivo realizou-se abordagem normativa e doutrinária do tema a partir de sua evolução em âmbito europeu, fonte de inspiração para a legislação brasileira. Foram identificados e discutidos os

1 Graduação em Direito pela Universidade da Região da Campanha (1994), mestrado em Integração Latino - Americana pela Universidade Federal de Santa Maria (2000) e doutorado pela Universidade Federal de Santa Catarina, na área de concentração Direito, Estado e Sociedade, com pesquisa sobre criança e adolescente na sociedade informacional (2009). É professora associada da Universidade Federal de Santa Maria, nos cursos de Graduação e Mestrado em Direito. Atua no Curso de Direito do Centro Universitário Franciscano, atual Universidade Franciscana (UFN). É docente pesquisadora na Faculdade Antonio Meneghetti. Atualmente é líder do Grupo de Pesquisa Teoria Jurídica no Novo Milênio (UFN) e do Grupo de Pesquisa Núcleo de Direito Informacional (UFSM), ambos inscritos no CNPq. Integra, na condição de pesquisadora, o Núcleo de Estudos Jurídicos e Sociais da Criança e do Adolescente, da Universidade Federal de Santa Catarina. Coordena o Núcleo de Direito Informacional, na Universidade Federal de Santa Maria. LATTES iD: http://lattes.cnpq.br/1218962383221912. ORCID iD: https://orcid.org/0000-0002-9636-2705.

2 Mestrando em Direito pela Universidade Federal de Santa Maria. Especialista em Direito Médico e da Saúde pela ULBRA. Advogado e Diretor Executivo na Siqueira Cordeiro Advogados. Consultor Sênior de Privacidade na oPrivacy, empresa localizada no estado de Santa Catarina. LATTES iD: http://lattes.cnpq.br/0143203009573511. ORCID iD: https://orcid.org/0000-0001-7336-7661.

3 Mestra em Direito pela Universidade Federal de Santa Maria (UFSM); Mestra em Ciências Ambientais pela Universidade de Passo Fundo (UPF) - Bolsista Capes Prosuc - I; Especialista em Direito Ambiental pelo Centro Universitário Internacional; Especialista em Direito Constitucional Aplicado pela Faculdade Legale; Bacharela em Direito pela Faculdade Antonio Meneghetti; Técnica em Meio Ambiente pelo Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense (IFSul); Membra do Grupo de Estudos e Pesquisas em Democracia e Constituição - GPDECON e do Grupo de Pesquisa em Direitos Animais - GPDA, ambos coordenados pela Prof. Dr Nina Trícia Disconzi Rodrigues Pigato, vinculados ao Curso e Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria (UFSM). LATTES iD: http://lattes.cnpq.br/7362064577211371. ORCID iD: https://orcid.org/0000-0003-4224-8090.

Como citar esse artigo:/*How to cite this article*:
SILVA, Rosane Leal da; SILVA, Raonny Canabarro Costa da; REHBEIN, Katiele Daiana da Silva. A proteção de dados pessoais por agentes de pequeno porte: a governança e as boas práticas como estratégias de implementação da LGPD. **Revista Meritum**, Belo Horizonte, v. 18, n. 1, p. 35-54, 2023. DOI: https://doi.org/10.46560/meritum.v18i1.9249.

principais aspectos que devem ser contemplados em programa de governança e boas práticas com vistas à efetividade segurança dos dados, concluindo-se que a edição da legislação é um passo importante e que coloca o Brasil em nível de adequação se comparado a outros países. No entanto, não é suficiente, pois sua implementação prática depende de variáveis tecnológicas e humanas, mostrando-se essencial a existência de programa de governança que observe boas práticas tanto no uso das tecnologias, quanto nas rotinas diárias sob responsabilidade direta dos colaboradores.

Palavras-chave: dados pessoais; Lei Geral de Proteção de Dados; Marco Civil da *Internet*; segurança.

ABSTRACT

This article addresses the protection of personal data from its historical evolution to the enactment of the Brazilian General Data Protection Law (LGPD). At this point, it focuses on the challenges for its implementation, especially with regard to information security to be promoted by small-scale processing agents. The investigation aims to identify and understand the current state of data protection in Brazil in order to answer the following research question: What are the challenges for the effectiveness of personal data security processed by small-scale processing agents? Therefore, based on the deductive method, a normative and doctrinal approach to the theme was carried out from its evolution in the European scope, which is a source of inspiration for the Brazilian legislation. The main aspects that must be considered in a program of governance and good practices were identified and discussed with a view to the effectiveness of personal data security. It was concluded that the enactment of the legislation is an important step in this scenario, and that it places Brazil at a level of adequacy when compared to other countries. However, this is not enough because its practical implementation depends on technological and human variables, proving to be essential to have a governance program that observes good practices both in the use of technologies and in the daily routine of organizations.

Keywords: *small-scale agents; good habits; personal data; General Data Protection Law; security.*

1. INTRODUÇÃO

A proteção de dados pessoais[4] é um tema que merece atenção na atual sociedade hiperconectada, marcada pela sofisticação dos mecanismos utilizados para a coleta e tratamento de informações. Tal interesse cresce em grande escala, tanto pelo rápido desenvolvimento de novas e invisíveis tecnologias para seu recolhimento e tratamento, quanto pelo poder que o acesso aos dados pessoais confere aos agentes que realizam esse tratamento.

Nesse cenário, dados tornaram-se moeda de troca e têm a capacidade de fornecer informações diversas e sensíveis sobre os seus titulares, formando perfil a partir dos quais é possível aplicar estratégias capazes de modular seu comportamento, predizendo ou mesmo direcionando desejos e ações. Ainda que o debate sobre este tema seja relativamente novo no Brasil, há vários anos os eventuais riscos sobre os direitos fundamentais, derivados do emprego das tecnologias, já constava na pauta de interesses de outros países, como evidenciam os registros oriundos do Continente Europeu.

Desse período até o atual, a evolução tecnológica proporcionou avanços exponenciais e, com o advento da *internet* e, mais recentemente, da inteligência artificial, os dados pessoais

4 De acordo com o art. 5º, da LGPD, há previsão de duas espécies de dados pessoais, a saber: "I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Brasil, 2018a).

foram alçados à condição de ativos ainda mais valiosos. Era preciso, então, avançar na regulação no Brasil, posto que a Lei nº 12.965/2014, denominado Marco Civil da *Internet*, ainda que referisse os dados pessoais ao tratar da privacidade dos registros, não teve o escopo de sistematizar essa matéria. A sistematização veio com o advento da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD).

Muito tem se discutido sobre o tema, desde a edição desta legislação. Não obstante, para além de conhecer seus antecedentes históricos, compreender os valores que nortearam a elaboração dessa lei e seus princípios fundantes, é essencial pensar na sua efetivação. Essa tarefa ganha maior complexidade em razão das inúmeras variáveis que envolvem o tema, desde a ausência de uma cultura de proteção de dados pessoais no Brasil, até as diferenças de porte e funcionamento das diferentes organizações sobre as quais a lei incide, o que é acrescido pela tardia organização da Autoridade Nacional de Proteção de Dados.

Independentemente do perfil e do grau de maturidade que a organização já se encontrava, é certo que novos desafios se apresentam com a LGPD, motivo pelo qual se justifica sua abordagem nesse artigo, cujo propósito é responder ao seguinte problema de pesquisa: considerando os agentes de tratamento[5], em especial os de pequeno porte[6], tais quais as estratégias essenciais para um programa de boas práticas e governança de dados, que prime pela segurança da informação?

Buscando respostas ao problema, utilizou-se o método dedutivo para fins de abordagem, isso porque o estudo partiu de uma investigação mais ampla, passando pelos aspectos históricos sobre a proteção de dados em âmbito internacional, com ênfase para a União Europeia, até seu tratamento em território nacional, o que é feito tanto pelo aporte constitucional quanto infraconstitucional, com ênfase para a LGPD. Pautada nesta legislação, discutem-se os desafios para a sua implementação, com apoio no procedimento monográfico, especialmente em razão da Resolução nº 2, de 27 de janeiro de 2022 da Autoridade Nacional de Proteção de Dados (ANPD) sobre a "*flexibilização*" da Lei 13.709/18 para agentes de tratamento de pequeno porte.

2. ANTECEDENTES HISTÓRICOS DA PROTEÇÃO DE DADOS PESSOAIS: A INFLUÊNCIA EUROPEIA

A proteção de dados pessoais é um tema que se popularizou nos últimos anos, em especial após a promulgação da LGPD. No período de sua *vacatio legis* muitos cursos, treinamentos e *lives* foram realizadas, o que não só movimentou a área jurídica, como também produziu impacto sobre as organizações públicas e privadas, muitas das quais passaram a investir no tema, na tentativa de implementar um novo modelo de tratamento de dados pessoais. Em que pese o tema ter se destacado mais recentemente no Brasil, a proteção de dados pessoais não

5 Neste trabalho será aplicada a definição de termos da LGPD e por agente de tratamento entende-se, a partir do art. 5º: "VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Brasil, 2018).

6 De acordo com o art. 2º, da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, consideram-se agentes de pequeno porte as microempresas, s*tartups,* pessoas jurídicas de direito privado, inclusive sem fins lucrativos, bem como pessoas naturais e entes privados despersonalizados que realizam o tratamento de dados (Brasil, 2022).

consiste em novidade nos Estados mais desenvolvidos tecnologicamente, o que aponta para certo atraso do Brasil quanto ao seu tratamento jurídico.

Os antecedentes históricos da proteção de dados indicam a preocupação com o tema ainda em meados da década de 1970. Usualmente há referência ao pioneirismo da República da Alemanha, mas em realidade a legislação produzida inicialmente limitava-se ao Estado de Hesse, tratando-se de lei estadual que se ocupava, em 17 artigos, dos dados processados e mantidos pelo poder público. Somente mais tarde houve a edição de lei federal, o que ocorreu no ano de 1977 (Doneda, 2006, p. 228). Esta primeira geração de leis preocupava-se basicamente com as questões referentes aos bancos de dados, espelhando o estado da tecnologia e a visão dos juristas da época (Doneda, 2011).

Em termos de legislação federal pode-se dizer que a Suécia se notabilizou ao se antecipar a outros países e editar sua legislação nacional em 1973, demonstrando a preocupação com o avanço tecnológico e seus reflexos sobre os direitos dos titulares. Tal preocupação era igualmente partilhada por outros Estados Europeus e, segundo análise de Doneda (2006, p. 229), naquele ano foi expedida Resolução, na qual os Estados foram incentivados a adotar princípios mínimos, em suas legislações internas, para a salvaguarda de dados pessoais.

Na França, em 1978, foi promulgada a Lei nº 78-17, a Lei *Informatique et Libertés* sobre a proteção de dados, em movimento que avançou para outros países europeus, tais como Dinamarca, Áustria, Noruega, Luxemburgo e Islândia. Este movimento igualmente atingiu Estados que recém ingressavam no bloco, tais como Portugal e Espanha (Doneda, 2006, p. 228-229). Esta Lei originou o que os doutrinadores convencionaram chamar de segunda geração das legislações de dados pessoais, leis que ultrapassavam o âmbito computacional ao apostar na privacidade e proteção de dados de maneira mais ampla.

Não tardou, no entanto, para que se percebesse que as tecnologias imprimiam um ritmo de evolução acelerado e que permitiam a rápida capilarização das informações e dos dados pessoais além das fronteiras estatais. Era necessário, então, intervir de forma mais concertada, transcendendo-se às legislações nacionais e localizadas territorialmente em direção à uniformização legislativa, constatação que norteou estudos no âmbito da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Foi produzido um guia para a proteção da privacidade e dados pessoais (1980), logo substituído pela Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, conhecida como Convenção nº 108 ou *Convenção de Estrasburgo* (1981). Esses documentos contribuíram para o sistema europeu de proteção de dados pessoais, tanto por estender a participação a Estados terceiros não integrantes da União Europeia quanto por considerar os dados pessoais como direitos humanos, importante marco no reconhecimento da natureza dos direitos em questão (Oliveira; Lopes, 2019, p. 58).

A Convenção de Estrasburgo, seguida da Carta de Direitos Fundamentais da União Europeia (ano 2000) elevou a proteção de dados ao status de direito fundamental autônomo, que deveria ser respeitado pelos Estados integrantes da União Europeia, vinculados aos documentos referidos (Sarlet, 2020, p. 183).

Neste período histórico tenta-se aprimorar a tutela dos dados pessoais, ainda centralizada nos cidadãos, reforçando a autodeterminação informativa (Doneda, 2011). Trata-se de reconhecer as assimetrias das relações estabelecidas entre as partes, notadamente do titular

dos dados frente a quem realiza o tratamento, pois sabidamente o primeiro é mais vulnerável. Deve-se, portanto, tutelar sua liberdade e seu poder decisório para eleger para quem e quais dados disponibilizar.

Como ensina Juárez (2003, p. 68-69), o direito à autodeterminação informativa é pessoal, relaciona-se com a dignidade da pessoa e ostenta as seguintes características: a) é originário, pois nasce com o sujeito de direitos; b) é personalíssimo; c) é direito subjetivo privado e relaciona-se com o gozo das faculdades do indivíduo; d) é oponível a todas as demais pessoas, tanto de direito público quanto privado; e) é variável ou contextual, pois comporta sopesamentos; f) é imprescritível.

A preocupação com a autodeterminação informativa caracterizou a denominada terceira geração de leis, que busca o fortalecimento da posição do sujeito em relação às entidades que coletam os dados, passando a existir o reconhecimento do desequilíbrio da relação e levando-se em consideração que algumas modalidades de tratamento de dados precisam de uma proteção especial, como o caso dos dados pessoais sensíveis (Doneda, 2011).

O sistema de proteção de dados pessoais foi complementado pela Diretiva nº 95/46/CE da União Europeia, a qual reconhece os distintos estágios de desenvolvimento tecnológico e níveis de proteção conferidos a cada Estado, e cujo item 2. firma a premissa básica de que as tecnologias devem estar a serviço das pessoas, com resguardo de sua vida privada. Ao longo de seus setenta e três (73) *considerandos,* os signatários explicitam os deveres dos Estados e reiteram, no Artigo 1º, a natureza de direitos fundamentais dos dados pessoais[7], ao estabelecer que "Os Estados-Membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais" (Parlamento Europeu e Conselho, 1995). Como destaca Busatta (2020, p. 33), essa Diretiva, "além de regular a proteção dos dados pessoais, tratou dos elementos, das noções a respeito da livre circulação de dados pessoais."

A autodeterminação informativa também estava prestigiada, pois em diversos dispositivos havia menção aos direitos do titular, a exemplo do art. 10º, no qual se assegurava à pessoa, cujos dados eram tratados, as informações sobre a identidade do responsável pelo tratamento ou seu representante, ter conhecimento sobre a finalidade do tratamento, os eventuais destinatários para os quais os dados seriam repassados, bem como o direito de retificar os dados a seu respeito. Para tanto, revelava-se essencial que o titular tivesse direito de acesso, o que estava contemplado no artigo 12º, da referida Diretiva. Ademais, cada Estado parte União Europeia deveria ter um órgão ou profissional que fosse responsável pela implantação e adequação das leis locais, conforme previsto pela Diretiva nº 95/46/CE (Parlamento Europeu e Conselho, 1995).

A evolução do tema no âmbito europeu não parou nesta importante Diretiva, especialmente no que se refere às transferências de dados pessoais, pois nos anos 2000 originou-se o acordo intitulado de *Safe Harbor,* que se refere a um programa de proteção de dados entre os Estados Unidos da América (EUA) e a União Europeia (UE). Tal acordo foi invalidado no

7 Os dados pessoais são definidos no Artigo 2º: "a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificado ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;" (Parlamento Europeu e Conselho, 1995).

REVISTA MERITUM • v.18 • n.1 • p. 35-54 • Jan. - Abr. 2023

ano de 2015 pela Corte de Justiça da União Europeia, isso porque a UE não considerava que os EUA pudessem certificar a segurança de dados sem esse acordo (Weiss; Archick, 2016). Esta revogação deu-se mediante uma provocação feita por *Maximiliam Schrems,* um cidadão australiano, ao órgão Irlandês que era responsável pelo Acordo de Processamento de Dados, levando o caso à Comissão de Justiça da União Europeia. *Schrems* estava aflito com o fato de que a empresa *Facebook* à época, hoje *Meta,* estaria transferindo dados dos servidores localizados na Irlanda para os Estados Unidos, o que violava o acordo firmado (Weiss; Archick, 2016).

Em 2013 já se sucediam as discussões para a remodelação do *Safe Harbor,* dando origem a formação de um novo acordo intitulado de *Privacy Shield*, como resposta às preocupações frequentes da União Europeia com os programas de vigilância da Agência de Segurança Nacional Americana (NSA), sendo oficializado no ano de 2016 (Weiss; Archick, 2016). Entretanto, *Schrems* ingressou com outra representação sobre o acordo concernente à transferência de dados entre os EUA e a União Europeia, que ficou conhecida como Caso *Schrems* II. Em 16 de julho de 2020, a Corte de Justiça Europeia invalidou novamente o acordo argumentando que ele não teria base jurídica para a transferência de dados entre cidadãos Europeus e os Estados Unidos (DW, 2020).

Em 25 de maio de 2018 houve um grande avanço na proteção de dados com a entrada em vigor da *General Data Protection Regulation* – Regulamento Geral de Proteção de Dados (GDPR), da União Europeia. Este Regulamento abarca os dados pessoais de todos os cidadãos residentes na UE, de forma independente da localização em que os dados sejam processados, primando pela transparência e prestação de contas no seu tratamento. Ademais, trata-se de um marco histórico na proteção de dados, erigidos à condição de direito humano fundamental e passará a ter reflexos em todo o mundo.

O Regulamento Geral de Proteção de Dados está alicerçado em seis princípios gerais de proteção de dados (justiça e legalidade; limitação de finalidade; minimização de dados; precisão; limitação de armazenamento; integridade e confidencialidade) e tem como núcleo central a proteção de dados por *design* e padrão[8]. Isso significa dizer que o cuidado com o titular de dados deve estar presente desde a concepção do serviço ou produto, cuja arquitetura deve ser pautada na privacidade como padrão. As práticas de negócios devem primar pela lisura e transparência, o que importa que as informações sejam fornecidas aos titulares de maneira clara, compreensível e acessível. Há, também, a imposição de responsabilidade para as organizações que realizam o tratamento de dados pessoais, obrigadas à prestação de contas que permitam demonstrar como realizaram o tratamento de dados pessoais (Goddard, 2017, p. 703).

A principal mudança operada com a adoção de um Regulamento, no entanto, é quanto à uniformidade e obrigatoriedade da norma, pois enquanto as Diretivas Europeias davam margem para discussão e aplicação das legislações nacionais, o Regulamento é aplicável diretamente, uniformizando o tratamento de dados o que, segundo Goddard (2017, p. 704), deve contribuir para a redução de disputas sobre a proteção de dados. Ficava claro que a proteção de dados doravante estaria na pauta dos Estados Europeus e que sua observância era impositiva, com

8 De acordo com Busatta (2020, p. 48), o Regulamento Geral de Proteção de Dados Europeu baseou-se no enfoque do risco e na adoção de medidas de prevenção. Para tanto, elegeu o p*rivacy by design* e o p*rivacy by default* como "princípios-chave". Pelo primeiro entende-se que as organizações devem, desde a concepção de seus projetos, incorporar elementos que respeitem a privacidade do titular e valorizem seu poder de escolha ao longo de todo o processo. O privacy by default parte da ideia de que o produto ou serviço deve vir com as restrições de privacidade por padrão e o usuário é que deve liberá-las, caso assim o deseje. A proteção de dados, então, deve estar presente desde a fase inicial do projeto, ser uma conduta pró-ativa e pautada na boa-fé objetiva do agente de tratamento e não meramente reativo.

reflexo também em eventuais países terceiros com os quais as empresas europeias viessem negociar, pois seria desejável que todos desfrutassem de um nível de proteção adequado.

O panorama da evolução da proteção de dados na União Europeia revela movimentos que impactaram a forma como o tema passou a ser tratado em território brasileiro, conforme se verá na sequência.

3. A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: DA LEGISLAÇÃO ESPARSA À LGPD

Ao lançar um olhar sobre o Brasil, constata-se que a evolução do tema foi tímida, isso porque somente no ano de 2022 a proteção de dados foi incorporada aos direitos fundamentais. Mesmo que o texto da Constituição Federal de 1988 tivesse alçado o direito à vida privada e à intimidade à condição de direito fundamental, sua abordagem era mais abrangente e não mencionava especificamente os dados pessoais. Em que pese não haver menção expressa, Sarlet (2020, p. 189) sustentava sua inclusão implícita na Carta Constitucional, aduzindo que

> [...] o direito à proteção de dados pode (e mesmo deve!) ser associado e reconduzido a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam – aqui nos termos da CF – os direitos à privacidade e à intimidade, no sentido do que alguns também chamam de uma "intimidade informática".

Outros autores, em sentido contrário, limitavam-se a mencionar a previsão constitucional do *Habeas Data* e, no setor privado, invocar a Lei nº 8.078, de 11 de setembro de 1990, o Código de Defesa do Consumidor. A legislação consumerista trata dos dados do consumidor em seu artigo 43, que elenca um rol de direitos e garantias frente aos bancos de dados, desde o direito a ter conhecimento sobre a eventual inscrição nos cadastros, o dever de as instituições manterem os registros de maneira clara e compreensível, com informações verdadeiras e que não excedam ao período de cinco anos. Confere o direito de o consumidor exigir a correção de dados inexatos ou incorretos no prazo de cinco dias úteis, o que é algo bastante positivo em razão dos eventuais prejuízos ao crédito que poderão ser suportados pelo titular em razão de eventual registro incorreto (Brasil, 1990).

É incontestável que a evolução tecnológica e os fluxos transnacionais de dados exigiam um passo à frente por parte do Brasil, sobretudo diante da voracidade do "capitalismo de vigilância", expressão desenvolvida por Shoshana Zuboff (2020) e que bem descreve a forma como o mercado e os governos se aproveitam das tecnologias para recolher o maior número de dados pessoais, tratando-os de maneira a compor perfis e predizer comportamentos. Para além da preocupação com os titulares, havia também a necessidade de adequação para que o Brasil não sofresse revés no mercado global, já que países mais desenvolvidos estavam a exigir níveis adequados de proteção de dados por parte dos governos e empresas. Tal impunha atualização normativa, o que começou com a edição da Lei n° 12.965 de 23 de abril de 2014, o Marco Civil da *Internet* (MCI). Esta lei simbolizou um avanço na governança da internet no Brasil, porque deli-

REVISTA MERITUM • v.18 • n.1 • p. 35-54 • Jan. - Abr. 2023

mitou direitos e responsabilidades dos usuários da rede mundial de computadores, ao mesmo tempo que buscou promover a liberdade de expressão, afastando eventuais riscos de censura na *internet* (Bezerra; Waltz, 2014). Para tanto, o legislador tentou harmonizar princípios como liberdade de expressão, neutralidade da rede, inimputabilidade da rede e privacidade dos usuários.

Este último princípio se liga mais diretamente à proteção de dados pessoais. Seu desenvolvimento no MCI, no entanto, foi tímido, limitando-se a tratar do tema ao abordar os registros de acesso e aplicação, não ocupando o lugar que era reservado a uma legislação específica.

O MCI regulou o exercício do Poder Público quanto ao desenvolvimento da *internet* no Brasil, com a definição de aparatos de governança multiparticipativa que englobam o governo, empresas, comunidade acadêmica e sociedade civil, criando-se um sistema de corregulação para a *internet* em âmbito nacional (Tomasevicius Filho, 2016). Assim, se observa que o MCI é uma norma que criou um cenário abrangente e introdutório para a regulamentação das relações que ocorrem na internet, sem se deter de forma aprofundada em temas considerados mais complexos, como a proteção de dados. Restavam, portanto, importantes questões que não estavam abrangidas pelo MCI e que somente foram contempladas pela Lei nº 13.709, de 2018 (LGPD), passando a vigorar a partir de 18 de setembro de 2020.

A LGPD foi claramente inspirada nos princípios norteadores do Regulamento Europeu, ainda que numa versão mais enxuta. Seu artigo 6º concentrou esses princípios de forma mais evidenciada, com especial atenção para a finalidade da coleta de dados, que deve efetivamente corresponder ao que foi informado ao titular, cujo tratamento deve justificar-se em uma das bases legais descritas no art. 7º. Ademais, os dados pessoais que serão tratados devem atender à necessidade declarada, ou seja, não se pode recolher dados com o objetivo de ampliar o banco de dados da empresa ou órgão público.

Esse é um ponto fulcral que precisa ser devidamente compreendido pelos agentes de tratamento de dados pessoais que, independente do segmento em que atuam e do seu porte, terão que organizar seus fluxos de trabalho e treinar seus colaboradores para observar os princípios da LGPD. É preciso que todos estejam apropriados da legislação, revejam suas rotinas e competências, o que deve ser feito a partir da elaboração de um bom diagnóstico do tratamento de dados pessoais realizado naquela organização. As organizações também precisarão elaborar um cuidadoso inventário dos dados pessoais processados, com a clara do escopo do tratamento, identificação da natureza dos dados (se dados cadastrais, sensíveis, especiais por se tratar de sujeitos vulneráveis, como crianças, adolescentes, idosos, pessoas com deficiência, etc), seu fluxo nos setores, níveis de segurança e proteção já existentes, assim como potenciais riscos. Essas são etapas preparatórias, sem as quais não se pode rever os padrões de segurança adotados ou, na ausência dessa sistematização, não se consegue estabelecer fluxos de trabalho que estejam conformes às boas práticas estabelecidas no art. 50, da LGPD[9].

Esses procedimentos não devem estar circunscritos a um setor específico, de gerência ou gestão da organização, pois de nada adiantará que alguns colaboradores observem a legislação e outros, ao revés, a ignorem sob a falsa crença de que os dados pertencem à empresa.

9 Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (Brasil, 2018a)

Ademais, o envolvimento de todos se mostra essencial para a implementação das boas práticas preconizadas na LGPD, as quais integrarão o programa de governança em privacidade[10], previsto no art. 50, §2º, I, da LGPD.

A existência de um programa de governança que esteja atualizado, seja transparente e conforme à LGPD evidenciará a organização do controlador, sua boa-fé em operar no mercado, assim como facilitará o próprio exercício de direitos por parte do titular do dado pessoal, o que facilitará sua autodeterminação informativa. Isso porque o titular deve ter acesso aos seus dados, saber como estão sendo utilizados, solicitar a sua eventual correção em caso de inexatidão, bem como requerer a sua eliminação quando não houver mais razão para a sua manutenção pelo controlador. Esses princípios estão conectados pela ideia de transparência, ou seja, o direito de o titular ser informado sobre o processamento de seus dados, o que, como sustentam Oliveira e Lopes (2019, p. 76), não se limita ao momento do recolhimento dos dados, mas alcança todas as etapas de seu ciclo de vida. Ademais, a LGPD impõe que as organizações estabeleçam mecanismo para garantir que a tríade segurança, prevenção e responsabilidade seja observada, para evitar incidentes de segurança com os dados do titular. Caso as medidas de prevenção adotadas *a priori* não sejam eficazes para garantir a segurança dos dados pessoais em poder do controlador, então este terá o dever de reparar eventuais danos (Oliveira; Lopes, 2019, p. 77-78).

Ainda que de importância inquestionável, não se pode ignorar que as leis não mudam, por si só, as práticas já arraigadas nas organizações. Portanto, como ensinado por Frazão (2019, p. 176-177), não se pode imaginar que o sistema de heterorregulação, representado pela LGPD e demais leis e atos normativos emanados do Estado sejam suficientes. Como são baseados no "sistema de comando e controle", ou seja, descrevem um comportamento e estabelecem sanções para o caso de descumprimento, deixam muitas questões sem cobertura, especialmente ante aos riscos do tratamento. Logo, a heterorregulação é insuficiente, quer porque o mercado sempre será mais rápido e em curto espaço de tempo as legislações não responderão mais aos novos problemas; quer pelas dificuldades de fiscalização e pela insuficiência da reparação. Logo, o sistema deve comportar também medidas de autorregulação e de *compliance* por parte das organizações.

A Lei 13.709 de 2018 possui o objetivo de modificar a forma de funcionamento e operação das organizações governamentais e privadas e visa a conceber um ambiente de segurança jurídica para o titular de dados. Para tanto, padroniza as regras acerca da coleta, armazenamento e tratamento dos dados pessoais, além de disciplinar como e quando acontecerá o compartilhamento desses dados, impondo uma padronização maximizada da proteção e sanções significantes para os que a infringirem (Fonseca, 2021). Destaque-se, uma vez mais, a importância da autodeterminação informativa e que a LGPD, seguindo os passos da União Europeia, alçou-a à condição de destaque, o que merece ser compreendido pelos controladores, operadores e seus empregados ou prepostos, pois como já mencionado, o dado pessoal pertence ao seu titular e não ao agente que realiza o seu tratamento. Essa compreensão impõe novas práticas ao estabelecimento ao longo de todo o ciclo das operações de tratamento, o que aponta para o necessário estabelecimento de uma governança de dados pessoais, como disposto no art. 50, da LGPD.

10 Segundo informações sistematizadas, disponíveis no site do Instituto de Pós-graduação e Graduação (IPOG, 2022), por governança de dados entenda-se um processo contínuo composto por ações e boas práticas que vão envolver todas as pessoas que atuam naquela organização, abarcando todas as etapas do tratamento de dados pessoais. Segundo descrito, "A governança de dados pode ser realizada em empresas de qualquer porte e responde a três necessidades básicas: Ter conhecimento sólido e claro sobre as informações da empresa; Saber a origem e o ciclo de vida dos dados; Entender se os dados estão alinhados com as políticas da empresa".

REVISTA MERITUM • v.18 • n.1 • p. 35-54 • Jan. - Abr. 2023

É possível afirmar que a edição da Lei Geral de Proteção de Dados Pessoais compôs um sistema protetivo que tem como matriz a Constituição Federal, ao que se somam os princípios constantes no Código de Defesa do Consumidor e o aporte do Marco Civil da Internet. Esse conjunto de normas encontra-se em alinhamento e aprofunda a proteção da pessoa, aperfeiçoando os mecanismos para que possa exercer sua autonomia frente àqueles que operam no mercado, com novas regras para a concessão do consentimento, o que leva em conta a assimetria do titular.

Como sustentado por Guimarães Filho, Ferneda e Ferraz (2020, p. 43), a LGPD está alinhada com as orientações da Organização das Nações Unidas (ONU), revisadas e expedidas em 2016, denominada Directrices para la Protección del Consumidor (2016). Este documento internacional orienta a elaboração das leis de proteção do consumidor e estabelece claramente que as boas práticas a serem adotadas deverão primar pela tutela da privacidade e da proteção de dados e, dentre os princípios para boas práticas comerciais, tanto para as operações realizadas no ambiente digital quanto fora dele, deve-se observar que dispõe o item "e" sobre proteção da privacidade, segundo o qual "Las empresas deben proteger la privacidad de los consumidores mediante una combinación de mecanismos adecuados de control, seguridad, transparencia y consentimiento en lo relativo a la recopilación y utilización de sus datos personales" (Naciones Unidas, 2016, p. 9). A observância dessas boas práticas deve perpassar por todas as atividades cotidianas e alcançar todos que realizam o processamento dos dados pessoais, independente do posto ocupado naquela organização. Ademais, condutas alinhadas com a segurança da informação e com investimentos na área de tecnologia devem integrar as bases do modelo de governança que será adotado pelo agente de tratamento.

Essas boas práticas devem ser observadas independentemente do porte da organização e sua natureza, o que se torna um desafio, sobretudo porque a LGPD não observou as especificidades de algumas organizações, como empresas de pequeno porte, *startups*, sociedades sem fins lucrativos, dentre outras, não contempladas especificamente na Lei Geral e cuja edição de orientações ficou sob responsabilidade da Autoridade Nacional de Proteção de Dados.

Com efeito, superadas as celeumas iniciais sobre a sua constituição e, em que pese a Autoridade Nacional de Proteção de Dados (ANPD)[11] ter sido identificada num primeiro momento como órgão prevalentemente fiscalizador, sua competência ultrapassa a mera fiscalização e aplicação de sanções, pois compete a ela a atividade normativa. No exercício dessa função, edita diretrizes e orientações para os agentes de tratamento, contribuindo para a criação de um ecossistema de proteção de dados pessoais que será complementado por boas práticas e governança de dados pessoais a ser adotado pela organização, tal como preceitua o art. 50, da LGPD. Esse é o tema a ser tratado no próximo tópico.

11 A ANPD estava prevista no texto original da LGPD, mas foi vetada pelo Presidente da República, Michel Temer, sob o argumento de que haveria vício de origem, sendo que o órgão a ser concebido seria parte integrante do Poder Legislativo, e a capacidade de dispor sobre a organização do estado é prerrogativa do Poder Executivo (Borges, 2018). Posteriormente sua instituição ocorreu por meio da Medida Provisória nº 869 de 2018, reinserindo a criação da ANPD na Lei nº 13.709 de 2018 (Brasil, 2018b). A votação da Medida Provisória se deu nos dias 28 e 29 de maio do ano de 2019, para posteriormente ser sancionada pelo presidente, Jair Bolsonaro, em 08 de julho de 2019, sendo convertida na Lei nº 13.853 de 2019 (Agência Senado, 2019). A previsão inicial era de que as sanções administrativas previstas na norma seriam empregadas pela ANPD a partir de agosto de 2020. Mas, a Medida Provisória nº 959 de 2020 adiou seu início para 03 de maio de 2021 (Brasil, 2020b). Entretanto no dia 10 de julho de 2020 ocorreu a promulgação da Lei nº 14.010, que passou a prever que as sanções só seriam aplicadas pela ANPD em 1º de agosto de 2021 (Brasil, 2020a). Especulava-se, frente a isso, a possibilidade de serem postergadas para o ano de 2022, caso houvesse a aprovação do Projeto de Lei nº 500 de 2021, o que não ocorreu.

4. BOAS PRÁTICAS COMO ESTRATÉGIA PARA EFETIVAR A SEGURANÇA DA INFORMAÇÃO

A observância de boas práticas por parte das organizações está intimamente ligada ao respeito aos princípios que norteiam o tratamento de dados, explicitados no art. 6º, da LGPD, com destaque neste ponto para a segurança, um dos importantes vetores da LGPD. O tema da segurança dos dados usualmente é tratado pelos gestores das organizações como tarefa de responsabilidade do setor de Tecnologia da Informação (TI), pois se associa a segurança com incidentes de segurança, acesso e uso indevido de informações e dados pessoais armazenados na base de dados ou em outro dispositivo.

Todavia, este é um entendimento bastante limitado, pois a segurança relaciona-se tanto com os dados em ambiente físico quanto aqueles cujo armazenamento depende de alguma tecnologia da informação e comunicação. Tal impõe que o cuidado com procedimentos de rotina seja o mesmo, independentemente do suporte, pois por violação de segurança dos dados se compreende "como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración acidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado de dichos datos" (González, 2019, p. 111).

Segundo o Privacy Framework, do National Institute of Standards and Technology – NIST – (2020), é preciso ter um modelo de gestão de risco que permite o diálogo desde o nível mais alto até aquele que vai implementar as atividades e operações; possibilita a identificação das necessidades da organização, de acordo com a sua missão, o negócio que realiza e os riscos que apresenta; auxilia na criação de níveis de implementação que darão o ponto de referência sobre o estado da organização, ou seja, quais os níveis de risco envolvidos nos processos e recursos da organização (2020, p. II).

Dentre as medidas técnicas e organizacionais preliminares devidas para a segurança encontra-se a análise diagnóstico da natureza do dado pessoal tratado, pois ainda que os dados mereçam proteção, camadas mais densas devem ser conferidas aqueles que oferecem maior risco para o titular. Dentre esses destacam-se os dados sensíveis, definidos no art. 5, II, da LGPD como todo aquele que, se mal empregado ou acessado indevidamente, pode produzir alguma espécie de discriminação para o seu titular.

Portanto, pensar na segurança e na governança de dados em uma organização (seja pública ou privada) pressupõe identificar, preliminarmente, os níveis de maturidade em que ela se encontra, o que implica em conhecer os fluxos internos e externos, durante todos os ciclos de tratamento. O processo de adequação deve considerar uma série de parâmetros, como o tipo de tratamento, a natureza dos dados, o número de interessados, os diferentes agentes envolvidos no tratamento, a função em que atua, o tamanho da organização e os eventuais riscos[12] de cibersegurança e de privacidade que o processamento pode produzir. Segundo o Privacy Framework, do National Institute of Standards and Technology – NIST – (US Departamento of Commerce, 2020, p. 3), enquanto os primeiros estão associados à incidentes de segurança, o que pode ocasionar a perda da confiabilidade, integridade e disponibilidade dos

12 Com relação a este último parâmetro, os riscos são inúmeros e vão desde a perda do controle dos dados, por parte de seu titular, tráfico ilícito de seus dados, uso de dados para fins diversos daqueles declarados e tratamento lesivo à sua dignidade, o que se incrementa em casos de processamento de dados sensíveis (González, 2019, p. 101).

REVISTA MERITUM • v.18 • n.1 • p. 35-54 • Jan. - Abr. 2023

dados[13]; os riscos de privacidade, por sua vez, associam-se a eventos de privacidade ocorridos no processo de tratamento dos dados. Eles são decorrentes das operações rotineiras com os sistemas, produtos e serviços que contêm dados pessoais. Tanto em um, quanto em outro caso, os impactos negativos que podem ser produzidos no titular são os mais variados, desde constrangimento a estigmas mais sérios, caracterizados em processos discriminatórios. A organização implicada, por certo, também sofrerá efeitos negativos que, no mínimo, macularão sua imagem e credibilidade no mercado.

Como se percebe, a análise precisa ser cuidadosa, o que exige que a organização detenha uma estrutura mínima para estar em conformidade, com adoção de política de segurança que assegure a confidencialidade, a integridade e a disponibilidade dos dados. Tarefas como avaliar constantemente o risco devem fazer parte da rotina das organizações, pois dessa análise poderão resultar medidas para mitigá-lo por meio de estratégias técnicas e normativas dentro da organização, sendo possível também compartilhar o risco com eventuais operadores e com os próprios titulares de dados. Em casos mais brandos é possível que a organização aceite o risco, pois sua avaliação conduziu ao entendimento de que seus benefícios superam os riscos ou, ao revés, pode-se revisar a operação e evitar o processamento do dado pessoal, caso o risco seja demasiadamente elevado (US Departamento of Commerce, 2020, p. 5).

O constante monitoramento das atividades se evidencia como um desafio, notadamente para aquelas de menor porte e, foi com levando em conta as assimetrias entre as organizações que a Autoridade Nacional de Proteção de Dados brasileira abriu consulta pública para recolher contribuições sobre o tema. A partir desse movimento, foi editada a Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, destinada a disciplinar o tratamento de dados por agentes de pequeno porte compreendidos, conforme disposto no art. 2º, como "microempresas, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, bem como pessoas naturais e entes privados despersonalizados que realizam o tratamento de dados". Caso o tratamento de dados seja de alto risco[14], as disposições da referida Resolução não se aplicam a elas (Brasil, 2022).

Diferentemente do Regulamento Europeu, no caso brasileiro a LGPD exigia que a organização tivesse um encarregado de proteção de dados (art. 41, da LGPD), o que foi flexibilizado pelo art. 11, dispensando-se também a obrigatoriedade de registro das operações de tratamento, conforme art. 9º da Resolução nº 2/2022 (Brasil, 2022).

Essas flexibilizações, no entanto, não desobrigam esses agentes de tratamento de adotarem medidas de adequação e segurança, não se olvidando que a efetividade da LGPD dependerá, em grande parte, da maneira como os dados pessoais são tratados pelos gestores e

13 A confidencialidade, a integridade e a disponibilidade são considerados os pilares da segurança das informações e dos dados pessoais nas organizações. O primeiro pilar remete aos níveis de privacidade, ou seja, a quem, dentro da organização, pode acessá-los. Refere-se ao controle do que cada um pode acessar de dados pessoais de acordo com as funções que exerce e pode ser obtido com medidas bem simples, como controle de senhas e acessos, concedidos e revisados periodicamente de acordo com a função exercida pelo colaborador. A integridade, por sua vez, liga-se à exatidão das informações dentro dos sistemas operacionais da organização, garantindo-se, pelo controle dos acessos e manutenção do sistema, que os dados pessoais não sejam adulterados, corrompidos ou destruídos, mantendo-se hígidos. Por fim, a disponibilidade refere-se à possibilidade de consulta e utilização dos dados a qualquer tempo. A organização deve garantir que os dados pessoais que processa estejam disponíveis para uso, pois a indisponibilidade dos dados poderá gerar uma série de danos patrimoniais e à reputação da organização (Telium Networks, 2018).

14 Em síntese ao disposto no Art. 4º, pode-se dizer que ocorrerá tratamento de alto risco quando houver o processamento de dados em larga escala; sejam tratados dados que possam impactar significativamente interesses e direitos fundamentais dos titulares; o processamento empregue tecnologias emergentes ou inovadoras; ocorra vigilância ou controle de áreas acessíveis ao público; sejam tomadas decisões unicamente com base em tratamento automatizado; envolvam dados pessoais sensíveis de pessoas vulneráveis, como crianças, adolescentes e idosos.

colaboradores da organização. De nada adiantará fazer consistentes investimentos em aquisição e manutenção de *softwares* de segurança se as rotinas de trabalho não estiverem em conformidade. Esse é um ponto fulcral no plano de segurança e importará na sensibilização para uma nova cultura na organização, em que os dados são compreendidos como um bem do titular e não como um objeto de propriedade do controlador ou operador.

Para auxiliar nessa tarefa de conscientização e treino dos colaboradores, deve-se valer de técnicas de segurança de informação que, mesmo simples, são de grande eficácia para o controle de exposição de dados ou acessos não autorizados. Muitas delas, aliás, já faziam parte da rotina de organizações de maior porte ou que realizavam o tratamento de dados mais sensíveis, com previsão na ABNT ISO/IEC 27001, norma técnica usualmente utilizada pelo setor de TI de empresas, mas que pode (e até mesmo deve) ser observada por todos os setores[15].

Os treinamentos e capacitações devem fazer parte da rotina da organização em todos os seus níveis, desde aquele que recebe os dados cadastrais dos titulares até quem responde pela tomada de decisão. Quanto a esses, vale lembrar que um gerente deve ser responsável por garantir que informações adequadas, conhecimento e treinamento cheguem a todos os setores. Sem um suporte de gerenciamento é possível que não existam recursos suficientes para a facilitação, compreensão e treinamento de todos (Government Communications Security Bureau, 2017).

O esforço para promover a segurança dos dados deve ser contínuo, o que exige a incorporação de boas práticas, pois estudos apontam que, sem treinamentos constantes, a atenção, consciência e o conhecimento dos colaboradores degradam-se com o passar do tempo, ampliando as chances de incidentes de segurança. Garantir de forma contínua que a segurança da informação seja de conhecimento de todos manterá os colaboradores conscientes de eventuais problemas, contribuindo para que assumam suas responsabilidades (Government Communications Security Bureau, 2017).

O investimento em *firewalls*, sistemas de antivírus e outras tecnologias de segurança fornecem proteção[16], mas não impedem, de per si, que vazamentos de dados e brechas de segurança ocorram. É importante reconhecer que investir apenas na tecnologia, sem o necessário aporte em treinamento humano, simplesmente não é efetivo quando se trata de segurança. Para dar conta do desafio da segurança da informação, especialmente de dados pessoais, é preciso que se desenvolvam práticas comprometidas com essa governança, o que envolve tarefas simples cotidianas, tais como: uso adequado da internet, com acesso aos sites seguros; não abrir links que acompanham e-mail suspeitos; adotar procedimentos e cuidados com os equipamentos e locais de trabalho; não acessar sites suspeitos no trabalho e com os equipamentos destinados e este fim; reportar ao setor competente a detecção de atividades que fogem ao padrão usual; ter cuidados com o descarte de papéis, relatórios e informações, especialmente aquelas relacionadas à tecnologia da informação; eleger senhas de acesso mais complexas e não partilhá-las com terceiros; manter a tela do computador e as mesas de trabalho limpas, sem informações que configurem dados pessoais, dentre outras orientações simples, mas que precisam ser adotadas por todos os segmentos da empres (Noticebored, 2022).

15 De acordo com Silva (2022), essa certificação confere maior competitividade para as organizações que a usam, revelando-se um diferencial. Ademais, não vai tutelar somente os dados pessoais dos titulares, como também todo o ativo de informações da organização, com utilidade à governança organizacional.

16 E são muito importantes, ainda que não sejam suficientes. Sua relevância se justifica em razão do elevado registro de incidentes de segurança no Brasil, país que, segundo o Relatório da Multinacional Trend Micro, ocupou o segundo lugar no ranking mundial de ataques de r*ansowares (*vírus maliciosos) em 2020 (Silva, 2022).

REVISTA MERITUM • v.18 • n.1 • p. 35-54 • Jan. - Abr. 2023

Com efeito, a adulteração de informações, sua indisponibilidade ou o acesso indevido por pessoas não autorizadas são problemas que antecedem à LGPD e podem comprometer de forma significativa a segurança da operação, ferindo não somente a imagem da organização e prejudicando seus próprios processos internos (Tribunal de Contas da União, 2012), como também (e principalmente) trazendo danos para o titular. Os riscos, portanto, se revelam tanto para instituições públicas quanto privadas, independentemente de seu porte.

Para melhorar a segurança da informação é necessário considerar que as ações humanas podem ser motivadas pelos mais diversos sentimentos e comportam vicissitudes, dentre eles desídia dos colaboradores em seguir os procedimentos, imprudência ou até sentimentos de vingança. As pessoas, junto com os equipamentos e todo o aparato tecnológico utilizado compõem o sistema de segurança das organizações. Logo, é necessário pensar de forma holística: "sistemas" não são apenas as máquinas, eles incluem os usuários, os administradores e os gerentes dos processos. Erros são causados por falhas nos sistemas, processos e condições que levam pessoas a errarem ou falharem em sua prevenção, o que indica que as ações não podem ser isoladas. (Noticebored, 2022).

Assim, com o intuito de se compensar as falhas humanas e garantir efetividade aos sistemas de segurança, o desenvolvimento de uma Política de Segurança da Informação constitui estratégia indicada não só para efetivação da LGPD, mas como salvaguarda de outros ativos, garantindo que todos tenham onde recorrer quando não estiverem convictos do que deve ser feito ou como devem agir em determinada situação.

Tal instrumento se desenvolve como um conjunto de princípios que deverão ser utilizados como norte para a gestão de segurança e de informações, devendo ser atendido por todos os usuários internos e externos, incluídos o corpo gerencial e diretor. As diretrizes que forem estabelecidas nessa política vão assegurar os recursos computacionais e as informações, devendo ter a cooperação em sua elaboração de colaboradores de áreas críticas da instituição, como a alta direção e os gerentes dos sistemas utilizados (Tribunal de Contas da União, 2012).

Os programas de conscientização e treinamento devem ser estruturados de modo a auxiliar para que os usuários dos sistemas se tornem familiarizados com suas atribuições e responsabilidades; que conheçam os requerimentos legais ou regulatórios; compreendam os mandamentos de qualquer agência regulatória e seus requerimentos; prestem apoio para o cumprimento dos requisitos de segurança; auxiliem na manutenção da confidencialidade, integridade e disponibilidade dos dados; dentre outras atitudes e habilidades que devem ser desenvolvidas (Government Communications Security Bureau, 2017).

Em acréscimo, salvaguardas são importantes para garantir a segurança da informação e a privacidade dos dados processados na organização, tais como a adoção de controles de acesso lógico para agentes que utilizam a informática como meio de geração, divulgação e armazenamento de informações. O objetivo dos controles é proteger os equipamentos, arquivos e os aplicativos contra a perda, modificação ou divulgação não autorizada, concedendo privilégios apenas a quem efetivamente necessita (Tribunal de Contas da União, 2012). No tocante aos recursos críticos, estes devem ser bem monitorados e restritos a poucas pessoas, bem como usuários devem ser impedidos de executar procedimentos que sejam incompatíveis com as suas funções ou estejam além de suas responsabilidades (Tribunal de Contas da União, 2012).

Um conceito essencial para compreender a importância da atenção ao usuário quando se trata de segurança de informação está atrelado ao Princípio de Pareto que, de forma singela, assevera que 80% dos resultados são consequências à 20% das ações. Ao se trazer esse princípio para as questões de segurança da informação é possível dizer que 80% dos problemas poderiam ser solucionados dando a devida atenção a 20% dos erros que levam a eles (Hoepers, 2020). Na maioria das organizações, mesmo que se dê muita atenção a ataques que exploram vulnerabilidades complexas, são os problemas mais simples e com soluções já conhecidas que causam a maior parte dos ataques bem sucedidos.

Para enfrentar esse quadro existem três medidas que têm o potencial de reduzir ao menos 80% dos incidentes de segurança reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), são eles: atualizar os sistemas operacionais e os aplicativos, valendo a medida para computadores, celulares*, tablets* e *internet* das coisas; b) realizar o *hardening* dos dispositivos e sistemas, ou seja, desabilitar serviços não utilizados, alterar senhas padronizadas e configurar de forma segura todos os serviços com acesso à *internet*, além de periodicamente revisão da aplicação do ponto "a"; c) melhorar processos de identificação e autenticação, o que implica na educação para a gestão de senhas, focando em não autorizar reutilização e forçar a implementação de múltiplos fatores de autenticação em todos os serviços (Hoepers, 2020).

Outro ponto de destaque quando se fala de segurança da informação refere-se ao *e-mail* institucional (*business e-mail compromisse* - BEC), cujos riscos podem envolver variadas situações, desde a alteração de conteúdo até acesso a links de sites falsos[17] enviados por meio de engenharia social e inadvertidamente acessados por colaboradores. Mais uma vez se sobressai a importância do componente humano, evidenciando-se a necessidade de um programa de boas práticas aplicar vários tratamentos[18], de forma que cada um seja complementar ao sucesso do anterior (Leverett, 2020).

Como se vê, as boas práticas de segurança de informação são medidas necessárias para a efetividade da Lei Geral de Proteção de Dados Pessoais Brasileira.

Assim, independente de ser uma grande organização ou um agente de tratamento de pequeno porte, que pode vir a ser beneficiado pela Resolução nº 2, da Autoridade Nacional de Proteção de Dados (ANPD), o treinamento e a conscientização constante do seu quadro de colaboradores mostra-se medida imprescindível.

17 No caso de s*ites* falsos, como por exemplo para venda de mercadorias ou eletrônicos, agentes mal-intencionados realizam a confecção de s*ites* com endereço de lojas e marcas famosas, com uma mínima alteração ao final do endereço, mas se utilizam até mesmo do l*ayout* original. Nesses casos observar com cuidado todo o endereço eletrônico e pesquisar a reputação da empresa, bem com desconfiar de valores muito abaixo do mercado e de conexões que não sejam criptografadas (cadeado na barra de endereços) é o recomendado para evitar danos (Cartilha, 2020).

18 Um método simples para testar o nível de consciência da equipe é por meio de testes de p*hishing,* o qual pode ser conduzido por uma consultoria especializada em medir as taxas de detecção. Desse modo é possível se verificar quantos funcionários da empresa seriam capazes de reportar o ataque por meio dos canais corretos e quantos seriam impactados por eles. Quantificar cada um desses passos e compreender as camadas de defesa técnica e humana são objetivos de um bom programa de BEC (Leverett, 2020).

REVISTA MERITUM • v.18 • n.1 • p. 35-54 • Jan. - Abr. 2023

5. CONCLUSÃO

Pelo abordado, observa-se que a proteção de dados é um tema que desperta interesse individual, coletivo, econômico e político, sobretudo ante a chamada "era do capitalismo de vigilância". O desenvolvimento das tecnologias antecipou-se ao Direito e lhe desafiou, fenômeno usual, já que o fato precede à norma.

No caso brasileiro, a legislação específica sobre a proteção de dados pessoais tardou a ser editada se comparada aos Estados Europeus, que desde a segunda metade do Século XX já se preocupavam com a matéria, quer por suas legislações internas, quer por meio de Convenções, Diretivas e, mais recentemente, o Regulamento Europeu de Proteção de Dados. Se por um lado esse atraso impediu que se estabelecesse, no país, uma cultura de respeito aos direitos do titular dos dados pessoais, ativo ainda tratado como propriedade das empresas e organizações; por outro lado o fato de ter legislado mais tardiamente permitiu que o Brasil buscasse inspiração em fontes confiáveis, como o atual Regulamento Europeu, o que nos confere confiabilidade e um grau de adequação mínima no campo normativo. E não foi somente isso: a experiência brasileira em defesa do consumidor, assim como o caminho trilhado na regulamentação do uso da internet, por meio da Lei 12.965/2014, serviram de supedâneo e criaram as bases para um microssistema. Esse microssistema é pautado em princípios comuns, como a boa-fé objetiva, o respeito à privacidade, a menção expressa à proteção dos dados pessoais, aspectos que, se observados, ampliarão a proteção do titular.

O plano da efetividade, no entanto, não está assegurado pela simples existência da lei. Medidas são necessárias para a sua implementação, sobretudo quando se analisam riscos de privacidade e de segurança, que devem ser sopesados a partir da realidade da própria organização, sua estrutura, funções e a natureza dos dados pessoais que processa. Portanto, um modelo de governança pode servir para uma organização e não ser compatível com a realidade da outra, dada às peculiaridades que envolvem sua atuação.

Essa consideração contextual se faz muito importante no caso dos agentes de tratamento de pequeno porte, onde sabidamente é mais raro contar com programas institucionais voltados à segurança da informação e onde a cultura de proteção de dados tende a ser incipiente. Esse foi o encaminhamento conferido pela Resolução nº 2/2022, da ANPD, cujo objetivo foi flexibilizar algumas das exigências da LGPD, dentre elas a obrigatoriedade de ter um encarregado de proteção de dados indicado e a faculdade de realizar o relatório do impacto dos riscos.

Entende-se que tal flexibilização não é de todo desarrazoada para um período de transição, levando-se em conta os diferentes níveis dos agentes de tratamento. No entanto, é preciso que a mesma ANPD invista em ações de treinamento online e disponibilização de tutoriais simplificados para esses agentes, papel que seria desempenhado pelo encarregado de proteção e cuja existência foi, por ora, dispensada. Em acréscimo, seria importante abrir um canal de contato direto entre a ANPD e esses agentes, objetivando sanar dúvidas e conferir mais segurança às operações, tanto com vistas ao desenvolvimento das organizações, quanto visando à proteção de direitos dos titulares.

A confecção e disponibilização de *frameworks* online, simples e intuitivos, que possam ser adaptados e adotados pelos agentes de pequeno porte também poderiam contribuir para que a organização esteja em conformidade. Mais do que flexibilizar, a ANPD deve primar por alternativas capazes de conciliar os interesses que, se de um lado não deve obstaculizar a inovação e o desenvolvimento econômico dessas organizações; de outro deve sempre ter presente o escopo da LGPD, que é a defesa dos dados pessoais dos titulares.

Ademais, deve se ter em conta o risco de Resoluções dessa natureza passarem um recado errado ao mercado, uma mensagem de não valorização da própria LGPD. Para evitar que tal aconteça, entende-se que as flexibilizações devem ser temporárias e acompanhadas de outras medidas de formação desses agentes, com promoção de cursos, palestras ou distribuição de material informativo aos gestores, que devem, uma vez treinados, constituir evidências de capacitação contínua de seus colaboradores.

Portanto deve-se, tanto quanto possível, evitar o reducionismo de supor que a governança de dados e programas de boas práticas e segurança das informações serão resolvidas com a aquisição de *softwares* e investimento em tecnologia. Há que se ter cuidado para os agentes de pequeno porte não ficarem reféns de empresas de tecnologia da informação. Como defendido, é preciso que as ações sejam complementares, pois a adequada implementação da LGPD depende tanto ou mais da conduta das pessoas que atuam nas organizações, pois de nada adiantam as tecnologias se a cultura de proteção não constituir um valor para a organização e as pessoas que nela atuam.

REVISTA MERITUM • v.18 • n.1 • p. 35-54 • Jan. - Abr. 2023

REFERÊNCIAS

AGÊNCIA SENADO. Senado aprova MP que recria órgão para proteção de dados pessoais. **Senado Notícias**, 29 maio 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/05/29/senado-aprova-mp-que-recria-orgao-para-protecao-de-dados-pessoais. Acesso em: 29 jun. 2021.

ASSIS E MENDES ADVOGADOS. **Histórico das leis de proteção de dados e da privacidade na internet.** 2 maio 202 0. Disponível em: https://assisemendes.com.br/historico-protecao-de-dados/. Acesso em: 26 jun. 2021.

BEZERRA, Arthur Coelho; WALTZ, Igor. Privacidade, Neutralidade e Inimputabilidade da Internet no Brasil: Avanços e Deficiências no Projeto do Marco Civil. **Revista Eptic Online**, v. 16, n. 02, p. 165-175, maio/ago. 2014. Disponível em: https://ridi.ibict.br/bitstream/123456789/858/2/Arthur.pdf. Acesso em: 29 jun. 2021.

BORGES, Bruna. Marco Legal da Proteção de Dados é sancionado com veto a agência fiscalizadora: Projeto de lei sugerindo a criação do órgão será encaminhado ao Legislativo em breve. **Jota**, Brasília, 14 ago. 2018. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/veto-protecao-dados-temer-14082018. Acesso em: 29 jun. 2021.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD) (Redação dada pela Lei nº 13.853, de 2019). Brasília, DF: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 jun. 2021.

BRASIL. **Lei nº 14.010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília, DF: Presidência da República, 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 29 jun. 2021.

BRASIL. **Medida provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018 , para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: Presidência da República, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 29 jun. 2021.

BRASIL. **Medida Provisória n° 959, de 29 de abril de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. Brasília, DF: Presidência da República, 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 29 jun. 2021.

BRASIL. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.** Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 16 mar. 2022.

BUSATTA, Eduardo Luiz. O dever de prevenção em matéria de proteção aos dados pessoais. *In*: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo Malheiros. **Direito Civil e Tecnologia**. Belo Horizonte: Forum, 2020 . *Ebook.* p. 29-76. ISBN 978-65-5518-036-7.

CARTILHA: Golpe? Tô fora! Presidente Prudente, 2020. Disponível em: http://www.ssp.sp.gov.br/midia/Midia/00000349.pdf. Acesso em: 14 ago. 2021.

DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 02, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 28 jun. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DW. Justiça europeia dificulta transferência de dados da UE para os EUA. **DW**, 16 jul. 2020. Notícias e Economia. Disponível em: https://www.dw.com/pt-br/justi%C3%A7a-europeia-dificulta-transfer%C3%AAncia-de-dados-da-ue-para-os-eua/a-54200667. Acesso em: 29 jun. 2021.

FONSECA, Camila. **Importância e principais pontos da Lei Geral de Proteção de Dados**. Rio de Janeiro: Alright AdTech Company, 2021. Disponível em: https://alright.com.br/lgpd/. Acesso em: 30 jun. 2021.

GODDARD, Michelle. The EU General Data Protection Regulation (GPDR): European regulation that has a global impact. **International Journal of Market Research**, v. 59, issue 6, 2017. Disponível em: https://journals.sagepub.com/doi/abs/10.2501/IJMR-2017-050?journalCode=mrea. Acesso em: 29 jun. 2021.

GONZÁLEZ, Carlos González. **GDPR**. Guía Práctico sobre a Protección de Datos: ámbito laboral. Pamplona: Thompson Reuters Aranzadi, 2019.

GOVERNMENT COMMUNICATIONS SECURITY BUREAU. **About information Security. New Zealand Information Security Manual**. Part 1, Chapters 1 -13, December 2017. Disponível em: https://nzism.gcsb.govt.nz/ism-document/ . Acesso em: 14 fev. 2023

GUIMARÃES FILHO, Pedro Andrade; FERNEDA, Ariê Scherreier; FERRAZ, Miriam Olivia Knopik. Proteção de Dados e a Defesa do Consumidor: diálogos entre o CDC, o Marco Civil da Internet e a LGPD. **Revista Meritum**, v. 15, n. 02 . p. 38-52, maio/ago. 2020. Disponível em: http://revista.fumec.br/index.php/meritum/article/view/7749. Acesso em: 29 jun. 2021.

HOEPERS, Cristine. Onde investir para reduzir o risco: um retrato a partir dos incidentes de segurança reportados e dos dados de sensores e fontes externas agregados pelo CERT.br. *In*: SEGURANÇA digital: uma análise da gestão de risco em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf. Acesso em: 9 fev. 2023.

IPOG. **Governança de Dados e LGPD**: como implementar na sua empresa. 2022. Disponível em: https://blog.ipog.edu.br/tecnologia/governanca-de-dados/. Acesso em: 9 fev. 2023.

JUÁREZ, Noé A. Riande. Privacidad, autodeterminación informativa y la responsabilidad de proteger los bienes de uso común. *In:* PALAZZI, Pablo A. (dir.). **Derechos y nuevas tecnologías**. Derechos Personalíssimos. Buenos Aires: Ad-Hoc, 2003. p. 63-70.

LEVERETT, Éireann. Gestão de riscos cibernéticos para pequenas e médias empresas. *In*: SEGURANÇA Digital: uma análise da gestão de risco em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf Acesso em: 9 fev. 2023.

NACIONES UNIDAS. **Directrices para la protección del consumidor**. Nueva York y Ginebra, 2016.

NOTICEBORED. **Information Security 101**: back to basics. 2022. Disponível em: https://www.noticebored.com/html/infosec_101.html. Acesso em: 9 fev. 2023.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei nº 13.709/2018. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 53-83.

PARLAMENTO EUROPEU E CONSELHO. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.** Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri= CELEX:31995L0046&from=PT. Acesso em: 17 jul. 2022.

SARLET, Ingo. Proteção de Dados Pessoais como direito fundamental na Constituição Federal Brasileira de 1988. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 14, n. 42, p. 179-218, ago. 2020. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/18864/2/PROTEO_DE_DADOS_PESSOAIS_COMO_DIREITO_FUNDAMENTAL_NA_CONSTITUIO_FEDERAL_BRASILEIRA_DE_1988.pdf Acesso em: 9 fev. 2023.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS – SERPRO. O que é a Lei Geral de Proteção de Dados Pessoais? Dê um "giro" pela lei e conheça desde já as principais transformações que ela traz para o país. **Gov.br**, Brasília, 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 30 de jun. 2021.

SILVA, Cinara. A ISO 27001 e a Segurança da Informação. **Templum**, 2022. Disponível em: https://certificacaoiso.com.br/tudo-o-que-precisa-saber-sobre-a-iso-27001-e-seguranca-da-informacao/. Acesso em: 20 jul. 2022.

TELIUM NETWORKS. **Confidencialidade, integridade e disponibilidade**: os três pilares da segurança da informação. 2018. Disponível em: https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao. Acesso em: 22 jul. 2022.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, n. 86. p. 269-285, 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?format=pdf&lang=pt. Acesso em: 29 jun. 2021.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em segurança da informação**. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. Disponível em: https://www.portalgsti.com.br/2014/01/guia-de-boas-praticas-em-seguranca-da-informacao.html. Acesso em: 9 fev. 2023.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. 2016. Disponível em: https://publications.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt. Acesso em: 6 maio 2018.

US DEPARTAMENTO OF COMMERCE. National Institute of Standards and Technology. **Nist Privacy Framework**: a tool for improving privacy through enterprise risk management, version 1.0. 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020pt.pdf. Acesso em: 20 jul. 2022.

WEISS, Martin; ARCHICK, Kristin. U.S.-EU Data Privacy: FromSafe Harborto Privacy Shield. **Congressional Research Service**, 19 maio 2016. Disponível em: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2016/cs2016_0076.pdf. Acesso em: 28 jun. 2021.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

Dados do processo editorial

- Recebido em: 18/08/2022
- Controle preliminar e verificação de plágio: 21/08/2022
- Avaliação 1: 29/12/2022
- Avaliação 2: 01/02/2023
- Decisão editorial preliminar: 06/02/2023
- Retorno rodada de correções: 14/02/2023
- Decisão editorial/aprovado: 20/02/2023

Equipe editorial envolvida

- Editor-chefe: 1 (SHZF)
- Editor-assistente: 1 (ASR)
- Revisores: 2