Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

YASMIN SOUSA MONTEIRO

A EFETIVIDADE DOS MECANISMOS DE PROTEÇÃO DE DADOS PESSOAIS NA LEI 13.709/2018

BRASÍLIA
2019

YASMIN SOUSA MONTEIRO

A EFETIVIDADE DOS MECANISMOS DE PROTEÇÃO DE DADOS PESSOAIS NA LEI 13.709/2018

Artigo científico apresentado como requisito para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador(a): Professor(a) Paulo César Vilela Souto Lopes Rodrigues

BRASÍLIA
2019

YASMIN SOUSA MONTEIRO

A EFETIVIDADE DOS MECANISMOS DE PROTEÇÃO DE DADOS PESSOAIS NA LEI 13.709/2018

Artigo científico apresentado como requisito para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador(a): Professor(a) Paulo César Vilela Souto Lopes Rodrigues

BRASÍLIA, 2019

BANCA AVALIADORA

_____

Professor(a) Orientador(a)

_____

Professor(a) Avaliador(a)

RESUMO

O trabalho tem por objetivo analisar os mecanismos institucionais, preventivos e repressivos de proteção de dados pessoais previstos na LGPD sob a ótica da efetividade. A originalidade do trabalho recai no baixo número de trabalhos acadêmicos que analisem especificamente os mecanismos de proteção de dados dispostos na LGPD. O método compreende a análise predominantemente do ordenamento jurídico brasileiro e tem como escopo apenas os mecanismos de proteção de dados pessoais oriundos da LGPD. Ao fim, a breve análise dos mecanismos institucionais, preventivos e repressivos de proteção de dados pessoais da LGPD permitem afirmar que a lei tem potencial para ser efetiva, desde que cada mecanismo cumpra o seu papel.

Palavras-chave: efetividade; mecanismos de proteção; dados pessoais; lei 13.709/2018.

SUMÁRIO

INTRODUÇÃO

Os últimos anos foram marcados por diversos vazamentos de dados pessoais. O caso com maior número de vítimas afetadas no mundo, até hoje, atingiu um bilhão e cem milhões de cidadãos.[1] Porém, segundo relatório de segurança cibernética do Avast, os dez maiores casos de vazamento somam dois bilhões e quatrocentos e trinta e oito milhões de usuários afetados, dentre cidadãos e empresas.[2]

O caso mais emblemático envolveu a campanha do presidente dos Estados Unidos, Donald Trump, e as empresas Facebook e Cambridge Analytica. O escândalo se deu em razão da exposição de dados de oitenta e sete milhões de usuários do Facebook para a empresa de consultoria política Cambridge Analytica, que trabalhava na campanha do então candidato à presidência.[3] Consequentemente, Mark Zuckerberg, presidente do Facebook e uma das figuras mais respeitadas no mercado da tecnologia, foi chamado a depor no parlamento americano[4] e europeu[5].

Os escândalos recorrentes relacionados à violação de dados pessoais suscitaram a edição de atos normativos por parte dos legisladores. A aprovação do General Data Protection Regulation (GDPR) na União Europeia, em vigor desde 2018, e a aprovação da Lei Geral de Proteção de

---

[1] AVAST. *Os últimos 10 maiores vazamentos de dados*. 2019. Disponível em: < https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados>. Acesso em: 15 abr. 2019.

[2] AVAST. *Os últimos 10 maiores vazamentos de dados*. 2019. Disponível em: < https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados>. Acesso em: 15 abr. 2019.

[3] VOX. *The Facebook and Cambridge Analytica scandal, explained with a simple diagram*. 2018. Disponível em: <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>. Acesso em: 15 abr. 2019.

[4] THE GUARDIAN. *The key moments from Mark Zuckerberg's testimony to Congress*. 2018. Disponível em: <https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments>. Acesso em: 15 abr. 2019.

[5] THE GUARDIAN. *Five things we learned from Mark Zuckerberg's European parliament appearance*. 2018. Disponível em: <https://www.theguardian.com/technology/2018/may/22/five-things-we-learned-from-mark-zuckerbergs-european-parliament-appearance>. Acesso em: 15 abr. 2019.

Dados (LGPD) no Brasil, também em 2018, são fatos que impulsionaram o debate sobre o tratamento de dados pessoais na esfera do direito à privacidade.

A proteção da privacidade, de acordo com Helen Nissembaum, diz respeito não somente à limitação do acesso de informações pessoais, mas ao fluxo apropriado de informações pessoais no seu contexto integral. Isto é, a proteção de dados no seu contexto integral permite não somente análises preditivas, mas também confere legitimidade aos sistemas de dados.[6]

No Brasil, o direito à privacidade é um direito fundamental assegurado na Constituição Federal de 1988, no artigo 5º, inciso X[7]. No intuito de proteger os direitos fundamentais de liberdade e de privacidade[8], a LGPD estabelece o respeito à privacidade como um dos seus principais (artigo 2º, inciso I)[9].

A LGPD é aplicável "a qualquer operação de tratamento realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional" (art. 3º, inc. I, II, III).

---

[6] NISSEMBAUM, Helen. *Privacy in context*: technology, policy and the integrity of social life. Stanford: Stanford University Press, 2010. p. 2

[7] BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 15 abr. 2019. Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

[8] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 abr. 2019. Art. 1º Esta Lei 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 de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[9] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 abr. 2019. Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; [...]

É considerado dado pessoal “a informação relacionada a pessoa natural identificada ou identificável” (art. 5º, inc. I). A lei faz diferenciação entre o dado pessoal e o dado pessoal sensível, que é definido como o “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” (art. 5º, inc. II). O titular do dado pessoal é “qualquer pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (art. 5º, inc. V).

O tratamento de dado pessoal é conceituado como “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (art. 4º, inc. X).

Um dos grandes debates sobre a LGPD diz respeito sobre os mecanismos de proteção de dados pessoais e se esses mecanismos criados pela lei terão a efetividade necessária para garantir o cumprimento do seu objetivo. O objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Para isso, a LGPD tem como fundamentos o respeito à privacidade (art. 2º, inc. I); a autodeterminação informativa (art. 2º, inc. II); a liberdade de expressão, de informação, de comunicação e de opinião (art. 2º, inc. III); a inviolabilidade da intimidade, da honra e da imagem (art. 2º, inc. IV); o desenvolvimento econômico e tecnológico e a inovação (art. 2º, inc. V); a livre iniciativa, a livre concorrência e a defesa do consumidor (art. 2º, inc. VI); e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º, inc. VII).

Ainda, a LGPD tem como princípios a finalidade do tratamento, a adequação do tratamento, a necessidade do tratamento, o livre acesso dos

titulares ao tratamento, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e prestação de contas.[10]

No presente artigo, serão analisados os mecanismos institucionais, preventivos e repressivos de proteção de dados pessoais previstos na LGPD sob a ótica da efetividade.[11] Isto é, se os mecanismos de proteção de dados pessoais criados no sistema normativo brasileiro são aptos para alcançar os objetivos propostos.

Não é o foco do trabalho analisar institutos do GDPR e nem de outros instrumentos normativos internacionais ou estrangeiros. A análise é predominantemente do ordenamento jurídico brasileiro e tem como escopo apenas os mecanismos de proteção de dados pessoais oriundos da LGPD. Além disso, alguns temas da própria LGPD não serão abordados, como o tratamento de dados pessoais pelo poder público e a transferência internacional de dados.

---

[10] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 abr. 2019. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[11] CASTRO, Rodrigo. Eficácia, eficiência e efetividade na Administração Pública. EnANPAD. Salvador, 2006. Disponível em: <http://www.anpad.org.br/enanpad/2006/dwn/enanpad2006-apsa-1840.pdf>. Acesso em: 15 abr. 2019.

A originalidade do trabalho recai no baixo número de trabalhos acadêmicos que analisem especificamente os mecanismos de proteção de dados dispostos na LGPD. A metodologia utilizada será revisão bibliográfica, através da busca de textos acadêmicos ou de relevante valor científico por meio das palavras chaves em provedores de pesquisa na internet.

Inicialmente, serão analisadas as medidas preventivas de proteção de dados, que constituem boas práticas de governança e compliance na tecnologia da informação. Em seguida, serão analisadas as medidas repressivas, oriundas da responsabilização civil e administrativa decorrente da violação da LGPD.

1. A EFETIVIDADE DOS AGENTES E DA AUTORIDADE NACIONAL COMO MECANISMOS INSTITUCIONAIS DE PROTEÇÃO DE DADOS PESSOAIS

A LGPD possui dois mecanismos institucionais de proteção de dados pessoais. O primeiro mecanismo é a instituição de agentes de proteção de dados pessoais, nas figuras do controlador e do operador, além da figura do encarregado pelo tratamento de dados pessoais. O segundo mecanismo é a criação de uma Autoridade Nacional de Proteção de Dados (ANPD), com a função principal de zelar pela proteção de dados pessoais por meio do exercício de competências normativa, deliberativa, fiscalizadora e sancionatória.

1.1. Os agentes e o encarregado pelo tratamento de dados pessoais

A LGPD define dois tipos de agentes de tratamento de dados pessoais: o controlador e o operador (art. 4º, inc. VI, VII e IX). Além disso, a lei define uma terceira pessoa, que fará o papel de encarregado pelo tratamento de dados pessoais (art. 4º, inc. VIII). Veja-se o teor dos dispositivos:

> "Art. 5º Para os fins desta Lei, considera-se:
>
> 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;
>
> VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
>
> IX - agentes de tratamento: o controlador e o operador;"

O controlador e o operador são obrigados a manter o registro das operações de tratamento de dados que realizarem (art. 37). A LGPD estabelece a hierarquia funcional entre o operador e o controlador, na qual o operador deve realizar o tratamento de dados segundo instruções fornecidas pelo controlador. Ainda, estabelece a competência do controlador em observar as instruções e normas próprias sobre o tratamento de dados (art. 39).

O controlador é competente, também, para elaborar o relatório de impacto à proteção de dados pessoais, inclusive dados pessoais sensíveis, referente a suas operações de tratamento de dados, que poderão ser exigidos pela autoridade nacional (art. 38). A LGPD prevê requisitos mínimos para a elaboração do relatório: a descrição dos tipos de dados coletados; a metodologia utilizada para a coleta; a metodologia utilizada para garantir a segurança das informações; e a análise do controlador com relação aos mecanismos de mitigação de risco adotados (art. 38, parágrafo único).

Patrícia Peck Pinheiro, ao comentar a lei, afirma que o controlador é o detentor do consentimento do titular e, por isso, é o responsável pelo ciclo de vida dos dados pessoais. Ele, também, é o responsável não só pelo registro das operações de tratamento de dados pessoais, mas pela revisão e atualização dos procedimentos adotados para que, então, a proteção dos dados pessoais seja efetiva.[12]

O GDPR pode ser utilizado como complementação à visão da necessidade da revisão e atualização dos dados pessoais, conforme expressamente dispõem os arts. 24[13] e 30[14]. Isso demonstra o cumprimento dos propósitos de tratamento de dados através da transparência e do controle das ações.[15]

---

[12] PINHEIRO, Patrícia P. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

[13] UNIÃO EUROPEIA. Regulamento (EU) 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 (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em:□□15 abr. 2019. "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

[14] UNIÃO EUROPEIA. Regulamento (EU) 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 (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em:□□15 abr. 2019. "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. […]"

[15] PINHEIRO, Patrícia P. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

Além disso, a LGPD prevê a figura do encarregado pelo tratamento de dados pessoais. O encarregado é indicado pelo controlador (art. 41) e tem como principais atividades: aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências (art. 41, § 2º, inciso I); receber comunicações da autoridade nacional e adotar providências (inciso II); orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (inciso III) e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (inciso IV).

Em síntese, a figura do encarregado assegura que as informações fiquem centralizadas, certificando o controlador de que a aplicação das normas receberá a efetiva validação.[16]

Os agentes e o encarregado pelo tratamento de dados pessoais são figuras de controle interno das empresas, que zelarão pela proteção de dados pessoais durante o exercício da atividade empresarial. A efetividade dos agentes e do encarregado dependerá não só da sua atuação no ambiente interno da empresa, mas também da sua atuação em conjunto com uma autoridade nacional, que fará o papel de zelar pela proteção de dados pessoais da perspectiva externa das empresas.

1.2. A Autoridade Nacional de Proteção de Dados Pessoais

A LGPD, alterada pela Medida Provisória nº 869, de 2018, cria a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), órgão integrante da administração pública federal que integra a estrutura da Presidência da República (art. 55-A), dotada de autonomia técnica (art. 55-B).

A ANPD é composta por pelo Conselho Diretor, Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidade administrativas e especializadas (art. 55-C).

[16] PINHEIRO, Patrícia P. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

O Conselho Diretor da ANPD, órgão máximo de direção, é composto por cinco diretores nomeados pelo Presidente da República, escolhidos dentre brasileiros de reputação ilibada, com nível superior de educação e elevado conceito no campo que atuarão, para cumprimento de um mandato de quatro anos (art. 55-D, §§ 1º, 2º e 3º).

Os membros do Conselho Diretor da ANPD só perderão o cargo em razão de renúncia, condenação judicial transitada em julgado ou demissão decorrente de processo administrativo disciplinar, cuja competência de instauração é do Ministro de Estado Chefe da Casa Civil e de julgamento é do Presidente da República, que poderá inclusive afastar preventivamente o conselheiro durante o processo (art. 55-E). Após o exercício do cargo, os conselheiros se submetem à disciplina de conflito de interesses do art. 6º da Lei nº 12.813, de 2013[17].

A ANPD tem como competência principal "zelar pela proteção dos dados pessoais" (art. 55-J, inc. I). Para isso, suas competências mais relevantes são: "editar normas e procedimentos sobre a proteção de dados pessoais" (inc. II); deliberar sobre a interpretação da LGPD, suas competências e os casos omissos (inc. III); requisitar informações aos controladores e operadores de dados pessoais (inc. IV); implementar mecanismos para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a Lei (inc. V); fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à

[17] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 abr. 2019. Art. 6º Configura conflito de interesses após o exercício de cargo ou emprego no âmbito do Poder Executivo federal: I - a qualquer tempo, divulgar ou fazer uso de informação privilegiada obtida em razão das atividades exercidas; e II - no período de 6 (seis) meses, contado da data da dispensa, exoneração, destituição, demissão ou aposentadoria, salvo quando expressamente autorizado, conforme o caso, pela Comissão de Ética Pública ou pela Controladoria-Geral da União: a) prestar, direta ou indiretamente, qualquer tipo de serviço a pessoa física ou jurídica com quem tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego; b) aceitar cargo de administrador ou conselheiro ou estabelecer vínculo profissional com pessoa física ou jurídica que desempenhe atividade relacionada à área de competência do cargo ou emprego ocupado; c) celebrar com órgãos ou entidades do Poder Executivo federal contratos de serviço, consultoria, assessoramento ou atividades similares, vinculados, ainda que indiretamente, ao órgão ou entidade em que tenha ocupado o cargo ou emprego; ou d) intervir, direta ou indiretamente, em favor de interesse privado perante órgão ou entidade em que haja ocupado cargo ou emprego ou com o qual tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego.

legislação, mediante processo administrativo (inc. VI); comunicar às autoridades competentes as infrações penais das quais tiver conhecimento (inc. VII).[18]

A criação de uma autoridade nacional deriva da convergência do legislador brasileiro ao modelo teórico da regulação de risco. A regulação de risco tem origem na resolução de problemas ambientais e de saúde e deriva da ideia de que o risco é o elemento central de normas que visam proteger direitos e liberdades coletivos.[19]

Rafael Zanatta afirma que o modelo de regulação de risco na LGPD privilegia a reunião de informações sobre os riscos regulados, a criação de padrões de conduta e, principalmente, o *enforcement* e o monitoramento das mudanças de comportamento social. Para alcançar a efetividade desejada, a LGPD deposita o *enforcement* do seu modelo regulatório na capacidade institucional de uma agência reguladora. [20]

A criação de uma autoridade com características de uma agência reguladora para interpretar a LGPD está de acordo com a visão de Cass Sunstein e Adrian Vermeule a respeito das capacidades institucionais. Ao comparar a capacidade institucional de cortes e agências na interpretação de conflitos regulatórios, os autores evidenciam que as agências reguladoras

---

[18] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 abr. 2019. Além disso, possui competências para "difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança" (inc. IX); "estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores" (inc. X); "elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade" (XI); realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD (inc. XIII); "realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica" (inc. XIV); "articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação" (inc. XV)

[19] ZANATTA, Rafael A. F. *Proteção de dados pessoais como regulação de risco*: uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017. p. 181-188.

[20] ZANATTA, Rafael A. F. *Proteção de dados pessoais como regulação de risco*: uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017. p. 181-188.

possuem um nível superior de competências técnicas e, portanto, estão melhor posicionadas para decidir qual é o melhor sentido do texto normativo. Além disso, a proximidade das agências com a atividade regulada permite melhor percepção sobre quais fatos representam ameaças reais ao cumprimento da lei.[21]

Entendendo da mesma forma, Patrícia Peck Pinheiro ao analisar o artigo 40 da LGPD[22], verifica que o poder de fiscalização da ANPD é relevante, pois o emprego de padrões de ação por esses órgãos facilita o cumprimento das normas. Logo, como a regulação dos dados pessoais será efetuada por uma agência nacional, a aplicação das sanções deve seguir os mesmos nortes e princípios do direito administrativo.[23]

No entanto, a efetividade do modelo de regulação de risco pode ser ameaçada no Brasil pela judicialização de medidas regulatórias e administrativas, com a imposição de barreiras procedimentais estratégicas por interesses econômicos específicos. Ainda, há a possibilidade de isolamento do cidadão comum do debate a respeito da proteção de dados pessoais, de modo que as negociações coletivas sejam protagonizadas apenas por grandes empresas de tecnologia e entidades civis altamente especializadas como a autoridade reguladora.[24]

Consequentemente, a efetividade dos mecanismos institucionais de proteção de dados pessoais está atrelada à capacidade dos agentes e do encarregado, no ambiente interno, e da ANPD, no ambiente externo, de conformar a atividade empresarial à LGPD por meio da implementação de

---

[21] SUNSTEIN, Cass, VERMEULE, Adrian. *Interpretation and institutions*. Public law and legal theory working paper nº 28. Chicago, 2002. Disponível em: <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=12319&context=journal_articles>. Acesso em: 15 abr. 2019.

[22] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 abr. 2019. Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

[23] PINHEIRO, Patrícia P. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

[24] ZANATTA, Rafael A. F. *Proteção de dados pessoais como regulação de risco*: uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017.

mecanismos preventivos de proteção de dados pessoais – a adoção de medidas de segurança e a formulação de regras de boas práticas e governança.

2. A EFETIVIDADE DA SEGURANÇA E DAS BOAS PRÁTICAS COMO MECANISMOS PREVENTIVOS DE PROTEÇÃO DE DADOS PESSOAIS

A LGPD possui dois mecanismos preventivos de proteção de dados pessoais. O primeiro mecanismo é a adoção de medidas de segurança aptas a proteger e evitar situações acidentais ou ilícitas de obtenção, tratamento ou perda de dados pessoais. O segundo mecanismo é a formulação de regras de boas práticas e de governança corporativa que estabeleçam a organização, os procedimentos, os padrões técnicos, os mecanismos internos de supervisão e mitigação de riscos e as obrigações dos envolvidos no tratamento de dados pessoais.

De acordo com Patrícia Peck Pinheiro, a LGPD busca estimular a aplicação de seus dispositivos em caráter preventivo, ou seja, exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de compliance digital; investimento; atualização de ferramentas de segurança de dados; revisão documental; melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura.[25]

2.1. A adoção de medidas de segurança

A LGPD obriga os agentes de tratamento a adotarem medidas de segurança de natureza técnica e administrativa para proteger dados pessoais, desde a fase de concepção do produto ou serviço até a etapa de execução. Veja-se o teor do art. 46:

> "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

[25] PINHEIRO, Patrícia P. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução."

A LGPD afirma que os agentes de tratamento devem adotar medidas de segurança e delega à ANPD a regulamentação específica a respeito de quais são os padrões de segurança a que se refere. Em se tratando de padrões de segurança da informação, é indispensável observar as normas editadas pela Organização Internacional de Padronização (International Standardization Organization - ISO).[26]

A organização possui um conjunto de normas técnicas e de procedimentos relativos aos sistemas de gerenciamento de segurança da informação, denominada ISO/IEC 27.000[27], revisada pela última vez em 2018. O conjunto de normas tem como principais regramentos a ISO/IEC 27.001[28] e a ISO/IEC 27.002[29], a primeira voltada para a certificação internacional de empresas e a segunda direcionada à certificação internacional de profissionais.

As normas da ISO são recomendadas pela Agência Brasileira de Normas Técnicas (ABNT), uma vez que são projetadas para serem aplicadas em organizações de qualquer tipo e tamanho, sejam elas empresas, organizações sem fins lucrativos ou agências governamentais.[30]

---

[26] SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no brasil*. 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro. p. 29.

[27] ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. *ISO/IEC 27.000/2018* - information technology - security techniques - information security management systems - overview and vocabulary. Disponível em: <https://www.iso.org/standard/73906.html>. Acesso em: 19 abr. 2019.

[28] ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. *ISO/IEC 27.001/2013* - information technology - security techniques - information security management systems - requirements. Disponível em: <https://www.iso.org/standard/54534.html>. Acesso em: 19 abr. 2019.

[29] ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. *ISO/IEC 27.002/2013* - information technology - security techniques - code of practice for information security controls. Disponível em: <https://www.iso.org/standard/54533.html>. Acesso em: 19 abr. 2019.

[30] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ISO/IEC 27000*: norma internacional de segurança da informação é revisada. 2018. Disponível em: <http://www.abnt.org.br/noticias/5777-iso-iec-27000-norma-internacional-de-seguranca-da-informacao-e-revisada>. Acesso em: 15 abr. 2019.

Ainda, a LGPD dispõe que em caso de eventual incidente de segurança que possa acarretar risco ou dano relevante para os titulares dos dados pessoais, o controlador deverá comunicar as informações da ocorrência à autoridade nacional e ao titular em prazo razoável (art. 48, caput e § 1º). Em seguida, a autoridade nacional deverá apurar a gravidade do incidente e, se for o caso, determinar ao controlador a adoção de providências (art. 48, § 2º), bem como avaliará se foram tomadas as medidas técnicas adequadas (art. 48, § 3º).

Enquanto na normativa brasileira, o legislador preferiu apenas definir que a comunicação seja feita em prazo razoável, o GDPR, ao contrário, aponta no artigo 33 que a notificação deve ocorrer sem demora injustificada e sempre que possível em até 72 horas após ter conhecimento do ocorrido.[31] Nesse ponto, o GDPR buscou ser mais efetivo do que a LGPD e portanto, pode ser um parâmetro a ser observado.

Diante do exposto, as medidas de segurança de natureza técnica e administrativa para proteção de dados pessoais só serão efetivas se estiverem diretamente relacionadas com a formulação de regras de boas práticas e de governança.

2.2. A formulação de regras de boas práticas e de governança

A LGPD faculta aos controladores e operadores de tratamentos de dados pessoais a formulação de regras de boas práticas e de governança. Veja-se o teor do art. 50, a seguir:

> "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."

A lei prevê alguns parâmetros para consideração do controlador e do operador no momento de elaboração das regras de boas práticas, como a

[31] PINHEIRO, Patrícia P. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

natureza, o escopo, a finalidade e a probabilidade e gravidade dos riscos e benefícios decorrentes do tratamento de dados do titular (art. 50, § 1º).

A lei recomenda a implementação de um programa de governança em privacidade, com base nos princípios da segurança e da prevenção. O programa deve levar em consideração a estrutura, escala e volume das operações, bem como a sensibilidade dos dados e a probabilidade e gravidade dos danos para os titulares dos dados (art. 50, § 2º). Além disso, deve cumprir com os requisitos mínimos a seguir (art. 50, § 2º, I):

> "a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
>
> g) conte com planos de resposta a incidentes e remediação; e
>
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas."

Ainda, a lei recomenda que seja demonstrada a efetividade do programa de governança em privacidade quando apropriado, especialmente a pedido da ANPD ou outra entidade que de qualquer forma promova o cumprimento da LGPD (art. 50, § 2º, II).

A Gartner, empresa de consultoria referência no mercado de tecnologia da informação, fornece uma definição de boas práticas de governança:

> "especificação das razões de decisão e de um quadro de responsabilidades para incentivar a implementação de boas práticas na criação, armazenamento, uso, avaliação e arquivamento de informação. Inclui os processos, responsabilidades e métricas que garantem o uso

> eficiente da informação para permitir que uma organização atinja seus objetivos."[32]

A introdução de medidas e regras de boas práticas e de governança é essencial para que todos os requisitos necessários à proteção dos dados pessoas sejam efetivados, segundo Patrícia Peck Pinheiro.[33]

A autora observa que a lei prevê e exige que existam encarregados da proteção dos dados pessoais nas organizações. Ainda, o controlador e o operador devem pensar em regras e meios técnicos para proteger os dados pessoais e comprovar sua efetividade nas empresas, seja por aplicação de recursos de anonimização, controle de acesso, procedimentos, políticas de gestão e treinamentos para equipes. [34]

Nesse sentido, as empresas devem adequar suas políticas de segurança da informação, bem como seus regulamentos internos de segurança da informação e seus termos de uso da segurança da informação.[35]

As boas práticas e a governança não se restringem ao setor de tecnologia da informação de uma empresa. Na verdade, as políticas de segurança de informação deverão ser observadas desde a concepção dos produtos e serviços de uma empresa.

Isso porquê a LGPD impõe a adequação da atividade empresarial ao conceito de privacidade por design - privacy by design (art. 46, § 2º). O termo privacy by design é definido na GDPR como a "proteção de dados por meio do design de tecnologias". Isso significa que as medidas de proteção à

---

[32] GARTNER IT GLOSSARY. *Information governance*. Disponível em: <https://www.gartner.com/it-glossary/information-governance>. Acesso em: 15 abr. 2019. Tradução livre do trecho: "Gartner defines information governance as the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals."

[33] PINHEIRO, Patrícia P. *Proteção de dados pessoais*: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

[34] PINHEIRO, Patrícia P. *Proteção de dados pessoais*: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

[35] LIMA, Caio Cesar C., MONTEIRO, Renato L. *Panorama brasileiro sobre a proteção de dados pessoais*: discussão e análise comparada. Revista A.to.Z., Curitiba, v.2, n.1, UFPR, 2013. p. 69.

privacidade devem ser incorporadas às soluções tecnológicas oferecidas pelas empresas desde a etapa inicial de planejamento. Desse modo, as empresas são responsáveis, também, por capacitar permanentemente todos os seus colaboradores que participam do desenvolvimento de tecnologias nas políticas de segurança da informação e em normas internas de processamento de dados.[36]

As empresas certamente terão dificuldades de se conformar à LGPD, em razão do elevado número de alterações que deverão proceder no cotidiano de sua atividade empresarial. Para que as boas práticas e a governança sejam efetivas, portanto, existem diversas consultorias e escritórios de advocacia que se dispõe auxílio no processo de conformação.

Enquanto a lei ainda não está em vigor, é possível encontrar diversas cartilhas e artigos de associações, consultorias, escritórios de advocacia, bem como a oferta de serviços consultivos para conformação de empresas com base na LGPD.[37]

Ocorre que, a efetividade dos mecanismos preventivos de proteção de dados pessoais seja pela adoção de medidas de segurança, seja pela formulação de regras de boas práticas e de governança só terão enforcement se forem interpretadas em conjunto com as regras de responsabilização administrativa e civil como mecanismos repressivos de proteção de dados pessoais.

---

[36] KUJAWSKI, Fabio F., THOMAZ, Alan C. E. *Brazil*. In: RAUL, Alan C. (coord.). The privacy, data protection and cybersecurity law review. 5ª ed. Derbyshire: Encompass Print Solutions, 2018. p. 105.

[37] À título de exemplo, cite-se a FIESP, disponível em: <https://www.fiesp.com.br/arquivo-download/?id=252615>; Ernest Young, disponível em: <https://www.ey.com/Publication/vwLUAssets/018-07-Folder-Cyber-PLC53/$File/2018-07-Folder-Cyber-PLC53-FINAL-simples.pdf>; PricewaterhouseCoopers, disponível em: <https://www.pwc.com.br/pt/consultoria-negocios/lei-geral-de-protecao-de-dados-pessoais.html?utm_campaign=59553fef94a326580f02325f&utm_content=5baaa33104e4f4000100c659&utm_medium=smarpshare&utm_source=twitter>; Thomson Reuters, disponível em: <https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/white-paper/thomson-reuters-legal-whitepaper-lei-geral-de-protecao-de-dados.pdf>; Mattos Filho, disponível em: <http://publicacoes.mattosfilho.com.br/books/bdtv/>; Machado Meyer, disponível em: <https://www.machadomeyer.com.br/index.php?option=com_content&catid=112&id=9087&view=article&Itemid=614&nosef=1&lang=pt>; Levy e Salomão, disponível em: <http://www.levysalomao.com.br/files/publicacao/anexo/20180815112303_nova-lei-de-protecao-de-dados-pessoais-e-atividade-jornalistica.pdf>. Acesso em: 15 abr. 2019.

3. A EFETIVIDADE DA RESPONSABILIZAÇÃO ADMINISTRATIVA E CIVIL COMO MECANISMOS REPRESSIVOS DE PROTEÇÃO DE DADOS PESSOAIS

A LGPD possui dois mecanismos repressivos de proteção de dados pessoais. O primeiro mecanismo é a responsabilização administrativa por meio de sanções aplicáveis pela autoridade nacional (ANPD), como a advertência, multa, publicização da infração, bloqueio e eliminação de dados pessoais. O segundo mecanismo é a responsabilização civil e o ressarcimento de danos, por meio do acionamento dos mecanismos tradicionais de jurisdição do Poder Judiciário.

3.1. A responsabilidade administrativa por meio de sanções

A LGPD prevê a responsabilização administrativa dos agentes de tratamento de dados em razão das infrações cometidas em prejuízo das disposições normativas que institui, por meio das seguintes sanções estabelecidas no art. 52, a seguir:

> "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;"

A aplicação das sanções será feita após procedimento administrativo, assegurada a oportunidade de ampla defesa, que considerará os seguintes parâmetros (art. 52, § 1º):

> "I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II - a boa-fé do infrator;
>
> III - a vantagem auferida ou pretendida pelo infrator;
>
> IV - a condição econômica do infrator;
>
> V - a reincidência;
>
> VI - o grau do dano;
>
> VII - a cooperação do infrator;
>
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas; e
>
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção."

Na aplicação da multa, a LGPD obriga a ANPD a considerar o faturamento total da empresa ou do grupo de empresas, desde que não disponha do valor do faturamento no ramo da atividade empresarial na qual tenha ocorrido a infração (art. 52, § 4º). Ainda, impõe à ANPD a emissão de regulamento próprio sobre as metodologias de cálculo do valor-base das sanções de multa previstas na LGPD após a realização de consulta pública (art. 53). No caso do cálculo do valor de multas diárias, a ANPD deverá observar parâmetros como a gravidade da falta e a extensão do dano ou prejuízo causado (art. 54).

As penalidades por multa levam em consideração valores elevados, o que implica em maior efetividade da norma.[38] Mesmo que um controlador ou operador esteja seguindo todas as melhores práticas e aplicando todos os controles, ainda assim, pode haver a infração e o incidente de vazamento de dados pessoais.[39]

[38] PINHEIRO, Patrícia P. *Proteção de dados pessoais*: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.
[39] PINHEIRO, Patrícia P. *Proteção de dados pessoais*: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

A vacatio legis da LGPD impede que as multas sejam aplicadas até que a lei entre, efetivamente, em vigor. Porém a previsão de multas para violações à privacidade no tratamento de dados não são novidade no setor de tecnologia.

O relatório de vazamentos de dados da DLA Piper de fevereiro de 2019 demonstra que o GDPR já foi utilizado para a aplicação de 91 multas, no universo de 59 mil denúncias de vazamentos de dados, desde que entrou em vigor.

Dentre os diversos casos de sanção administrativa por violação à GDPR, a maior multa foi aplicada em 2019 pela autoridade de proteção de dados da França contra a Google, no valor de 57 (cinquenta e sete) milhões de euros. Segundo a autoridade francesa, o mecanismo de busca da empresa não cumpriu com os requisitos de transparência, informação e consentimento, previstos na GDPR. (reuters)

Antes mesmo do GDPR entrar em vigor, houve outro caso emblemático de aplicação de multa por violação de dados pessoais. A multa se deu em razão de um acordo fechado entre a Procuradoria Geral de Nova York com a empresa Uber, em 2016, em razão do vazamento de dados de 600.000 (seiscentos mil) motoristas e 57 (cinquenta e sete) milhões de usuários da plataforma. O valor total da multa foi de 148 milhões de dólares americanos.

Segundo Patrícia Peck Pinheiro, o cálculo do valor-base na aplicação das sanções de multa, deve-se considerar o caso específico e o princípio constitucional da proporcionalidade. Ainda, deve haver um controle nas aplicações das punições, visando que elas possuem um caráter geral no setor da economia e podem atingir tanto pequenas empresas, quanto empresas que assumem maiores riscos.[40]

Consequentemente, a efetividade da responsabilidade administrativa por meio de sanções para proteção de dados pessoais deve pautar-se na

[40] PINHEIRO, Patrícia P. *Proteção de dados pessoais*: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

não exclusão da responsabilização civil e o ressarcimento de danos pelo Poder Judiciário.

3.2. A responsabilidade civil e o ressarcimento de danos

A LGPD prevê a possibilidade genérica de ajuizamento de ação perante o Poder Judiciário para defesa dos interesses e dos direitos dos titulares de dados (art. 22), da seguinte maneira:

> "Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva."

No Código Civil, a previsão da responsabilização civil de pessoas físicas e jurídicas por eventuais atos ilícitos consta nos arts. 186, 187 e 927. A ocorrência de eventuais falhas relacionadas ao tratamento de dados pessoais podem gerar danos, que por sua vez geram o dever de reparação civil.[41]

A LGPD impõe ao controlador e ao operador, especificamente, a obrigação de reparação de danos decorrentes da violação à legislação de proteção de dados pessoais (art. 42), da seguinte forma:

> "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."

Com o propósito de assegurar a efetiva indenização aos titulares de dados, a legislação prevê a responsabilização solidária do operador e controlador ou de controladores que estiverem envolvidos no tratamento gerador do dano (art. 42, § 1º).

Além disso, a LGPD prevê a possibilidade do magistrado promover a inversão do ônus da prova a favor do titular dos dados quando houver verossimilhança das alegações, hipossuficiência para fins de produção da prova ou for excessivamente onerosa a sua produção (art. 42, § 2º). Ainda, a

[41] SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no brasil*. 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro. p. 26.

lei permite expressamente o ajuizamento de ação de reparação de danos coletivos (art. 42, § 3º).

De acordo com Sergio Ricardo Correia de Sá Junior, a responsabilização civil das empresas, nesse caso, se dá de acordo com o Código de Defesa do Consumidor. A relação consumerista pode ser evidenciada na medida em que o titular dos dados é considerado consumidor direto ou indireto e a empresa é considerada fornecedora de produtos ou serviços.[42]

Em maior medida, nenhum tipo de segurança será capaz de cobrir absolutamente todos os riscos da atividade. Porém, com base nos preceitos do CDC, o Poder Judiciário considerará a teoria do risco da atividade para concluir pela responsabilidade objetiva do fornecedor. [43]

A irregularidade do tratamento de dados será constatada pelo magistrado quando deixar de observar a legislação ou não fornecer a segurança esperada pelo titular do dado, consideradas circunstâncias como o modo de realização, os resultados e riscos razoavelmente esperados e as técnicas de tratamento de dados pessoais disponíveis à época da realização (art. 44).

Dessa forma, o Poder Judiciário será acionado para efetivar as reparações civis previstas na LGPD e para eventuais casos de judicialização de medidas administrativas da ANPD.

[42] SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no brasil*. 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro. p. 27.
[43] SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no brasil*. 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro. p. 27.

CONSIDERAÇÕES FINAIS

A breve análise dos mecanismos institucionais, preventivos e repressivos de proteção de dados pessoais da LGPD permitem afirmar que a lei tem potencial para ser efetiva, desde que cada mecanismo cumpra o seu papel.

Os agentes e o encarregado pelo tratamento de dados deverão atuar como figuras internas à organização que pertencem, assegurando que os mecanismos preventivos de proteção de dados pessoais - as medidas de segurança e as regras de boas práticas e de governança - sejam devidamente observados.

A ANPD deverá agir como uma figura externa à organização, mas em conjunto com os agentes e o encarregado, para garantir que os mecanismos preventivos sejam regulamentados, compreendidos e devidamente aplicados.

No caso de descumprimento da LGPD por parte das empresas e/ou de seus colaboradores, deverão ser instaurados processos administrativos pela ANPD, que apurará os riscos, danos e a conduta dos envolvidos no incidente. Se a autoridade concluir que houve infração à LGPD, deverá aplicar uma das sanções administrativas.

Em situações limite, o Poder Judiciário poderá ser acionado, seja para a defesa dos direitos de titulares de dados pessoais, seja por empresas ou por seus colaboradores, para garantir a higidez da aplicação das medidas administrativas.

Ainda, a efetividade da LGPD dependerá da própria aderência do empresariado, por exemplo, no GDPR, 36% (trinta e seis porcento) dos executivos estavam em conformidade com as normas até sua data vigor e 59% (cinquenta e nove porcento) dos executivos afirmaram que o GDPR surgiu como uma oportunidade de transformação e criação de um novo modelo de negócio.[44]

Porém, a principal ameaça à efetividade da LGPD reside na instituição da ANPD por medida provisória. Vale relembrar que, inicialmente, a criação da ANPD era prevista na LGPD e foi vetada pelo Presidente da

[44] INSTITUTE FOR BUSINESS VALUE – IBM. *The end of the beginning*: unleash the transformational power of the GDPR. 2018. Disponível em: <https://www.ibm.com/downloads/cas/JEMXN6LV>. Acesso em: 15 abr. 2019.

República, por vício de iniciativa (Mensagem nº 451/2018). Em seguida, foi editada a Medida Provisória nº 869/2018, que instituiu a ANPD novamente. Porém, como se sabe, a eficácia da medida provisória é limitada e depende da tramitação de projeto de lei de conversão no Congresso Nacional.

No caso da ANPD não ser instituída, seja pela caducidade da medida provisória ou por qualquer outro motivo relacionado ao processo legislativo, a LGPD sofrerá enorme prejuízo na sua efetividade. Sem a ANPD para dispor sobre a segurança, as boas práticas e a governança, e as sanções administrativas, boa parte da lei ficará sem *enforcement*.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ISO/IEC 27000*: norma internacional de segurança da informação é revisada. 2018. Disponível em: <http://www.abnt.org.br/noticias/5777-iso-iec-27000-norma-internacional-de-seguranca-da-informacao-e-revisada>. Acesso em: 15 abr. 2019.

AVAST. *Os últimos 10 maiores vazamentos de dados*. 2019. Disponível em: <https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados>. Acesso em: 15 abr. 2019.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 15 abr. 2019.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 abr. 2019.

CASTRO, Rodrigo. Eficácia, eficiência e efetividade na Administração Pública. EnANPAD. Salvador, 2006. Disponível em: <http://www.anpad.org.br/enanpad/2006/dwn/enanpad2006-apsa-1840.pdf>. Acesso em: 15 abr. 2019.

GARTNER IT GLOSSARY. *Information governance*. Disponível em: <https://www.gartner.com/it-glossary/information-governance>. Acesso em: 15 abr. 2019.

INSTITUTE FOR BUSINESS VALUE – IBM. *The end of the beginning*: unleash the transformational power of the GDPR. 2018. Disponível em: <https://www.ibm.com/downloads/cas/JEMXN6LV>. Acesso em: 15 abr. 2019.

KUJAWSKI, Fabio F., THOMAZ, Alan C. E. *Brazil*. In: RAUL, Alan C. (coord.). The privacy, data protection and cybersecurity law review. 5ª ed. Derbyshire: Encompass Print Solutions, 2018. p. 105.

LIMA, Caio Cesar C., MONTEIRO, Renato L. *Panorama brasileiro sobre a proteção de dados pessoais*: discussão e análise comparada. Revista A.to.Z., Curitiba, v.2, n.1, UFPR, 2013. p. 69.

NISSEMBAUM, Helen. *Privacy in context*: technology, policy and the integrity of social life. Stanford: Stanford University Press, 2010.

ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. *ISO/IEC 27.000/2018* - information technology - security techniques - information security management systems - overview and vocabulary. Disponível em: <https://www.iso.org/standard/73906.html>. Acesso em: 19 abr. 2019.

ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. *ISO/IEC 27.001/2013* - information technology - security techniques - information security management systems - requirements. Disponível em: <https://www.iso.org/standard/54534.html>. Acesso em: 19 abr. 2019.

ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. *ISO/IEC 27.002/2013* - information technology - security techniques - code of practice for information security controls. Disponível em: <https://www.iso.org/standard/54533.html>. Acesso em: 19 abr. 2019.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no brasil*. 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro. p. 29.

SUNSTEIN, Cass, VERMEULE, Adrian. *Interpretation and institutions*. Public law and legal theory working paper nº 28. Chicago, 2002. Disponível em: <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=12319&context=journal_articles>. Acesso em: 15 abr. 2019.

THE GUARDIAN. *The key moments from Mark Zuckerberg's testimony to Congress*. 2018. Disponível em: <https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments>. Acesso em: 15 abr. 2019.

THE GUARDIAN. *Five things we learned from Mark Zuckerberg's European parliament appearance*. 2018. Disponível em: <https://www.theguardian.com/technology/2018/may/22/five-things-we-learned-from-mark-zuckerbergs-european-parliament-appearance>. Acesso em: 15 abr. 2019.

UNIÃO EUROPEIA. Regulamento (EU) 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 (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em:□□15 abr. 2019.

VOX. *The Facebook and Cambridge Analytica scandal, explained with a simple diagram*. 2018. Disponível em: <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>. Acesso em: 15 abr. 2019.

ZANATTA, Rafael A. F. *Proteção de dados pessoais como regulação de risco*: uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017.