FUNDAÇÃO GETULIO VARGAS
ESCOLA DE DIREITO FGV DIREITO RIO
GRADUAÇÃO EM DIREITO

CAROLINA DE OLIVEIRA SAAD

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E INCIDENTES DE SEGURANÇA: REGULAÇÃO E PRÁTICA DE VAZAMENTO DE DADOS

Rio de Janeiro
Dezembro de 2021
FUNDAÇÃO GETULIO VARGAS

ESCOLA DE DIREITO FGV DIREITO RIO

GRADUAÇÃO EM DIREITO

CAROLINA DE OLIVEIRA SAAD

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E INCIDENTES DE SEGURANÇA: REGULAÇÃO E PRÁTICA DE VAZAMENTO DE DADOS

Trabalho de Conclusão de Curso, sob a orientação do professor **Luca Belli**, apresentado à FGV DIREITO RIO como requisito parcial para obtenção do grau de bacharel em Direito.

Rio de Janeiro

Dezembro de 2021

ESCOLA DE DIREITO FGV DIREITO RIO

FGV DIREITO RIO

GRADUAÇÃO EM DIREITO

CAROLINA DE OLIVEIRA SAAD

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E INCIDENTES DE SEGURANÇA: REGULAÇÃO E PRÁTICA DE VAZAMENTO DE DADOS

Trabalho de Conclusão de Curso, sob a orientação do professor **Luca Belli**, apresentado à FGV DIREITO RIO como requisito parcial para obtenção do grau de bacharel em Direito.

Banca Examinadora:

_____

Luca Belli (professor orientador)

_____

Nicolo Zingales (membro da comissão examinadora)

_____

Danilo Cesar Maganhoto Doneda (membro da comissão examinadora)

Nota final: _____

Rio de Janeiro, 14 de dezembro de 2021

AGRADECIMENTOS

Agradeço a cada pessoa que passou pelo meu caminho e, de alguma forma, abriu ou fechou meus olhos, por cada troca, conversa, ensinamento e percalços enfrentados juntos. Agradeço por cada desafio que encarei durante a graduação e por cada oportunidade de crescimento que a FGV me proporcionou.

Agradeço por cada palavra de incentivo e apoio que recebi e dei, principalmente dos meus amigos e amigas de sala. Foram muitas.

Agradeço às minhas amigas mais próximas por tanto acolhimento, reciprocidade e por terem se mostrado os melhores presentes desses anos. Admiro muito cada uma de vocês.

Agradeço à Fundação Getulio Vargas e todo o seu corpo de funcionários. Agradeço a cada professor que tive por toda dedicação, por serem verdadeiros exemplos de profissionais e por me mostrarem as portas abertas do mundo.

Principalmente, agradeço à minha família, por acreditar em mim, pelo amor, apoio e incentivo incansáveis. Chegar aqui só foi possível porque tive e tenho vocês ao meu lado.

RESUMO

O presente trabalho discorre sobre direito à privacidade e proteção de dados pessoais, em relação a incidentes de segurança, com foco em vazamento de dados. O significado de privacidade vem se desenvolvendo desde a primeira menção do "direito de estar só" e, atualmente, recebe contornos influenciados principalmente pelo avanço da tecnologia e seu uso incessante, em uma sociedade hiperconectada à Internet. A quantidade de informações pessoais coletadas, os inúmeros tratamentos e o crescente número de violações e incidentes decorrentes desse uso têm incitado debates sobre proteção de dados pessoais e direito à privacidade. Nesse cenário, foi aprovada em 2018 a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais ou LGPD, que unificou, pacificou e introduziu os princípios e regras ao tema. A lei versa sobre o vazamento de dados e demais incidentes de segurança, mecanismos de governança e penalidades para os agentes de tratamento, que serão abordados neste trabalho. Para isso, foi feito um apanhado histórico acerca dos debates sobre privacidade e proteção de dados no Brasil e no mundo, além de exemplos de vazamento de dados que escancaram o potencial negativo do uso e produção incessante de dados.

Palavras-chave: privacidade; direito à privacidade; proteção de dados pessoais; dados pessoais; incidentes de segurança; vazamento de dados; mecanismos de segurança; Lei Geral de Proteção de Dados Pessoais (LGPD).

ABSTRACT

This paper discusses the right to privacy and protection of personal data, in relation to data breach, focusing on data leakage. The meaning of privacy has been developing since the first mention of the "right to be let alone" and, currently, it receives contours mainly influenced by the advancement of technology and its incessant use, in a society hyper connected to the Internet. The amount of personal information collected, the numerous treatments and the growing number of violations and incidents resulting from its use have sparked debates about the protection of personal data and the right to privacy. In this scenario, the Brazilian General Data Protection Act was approved in 2018, which unified, pacified and introduced the principles and rules on the subject. The law deals with data leakage and other data breaches, governance mechanisms and penalties for controllers and processors, which will be addressed in this paper. For this, a historical overview was made about the debates on privacy and data protection in Brazil and worldwide, as well as examples of data leakage that reveal the negative potential of the incessant use and production of data.

Keywords: privacy; right to privacy; protection of personal data; personal data; data breach; data leakage; remedies; Brazilian General Data Protection Act (in Portuguese, LGPD)

SUMÁRIO

INTRODUÇÃO

A expressão “sociedade de informação” é uma das mais utilizadas para caracterizar o contexto técnico-econômico no século XXI, sendo a sucessora da

"sociedade pós-industrial"[1]. É assim chamada porque cada vez mais informações fluem entre os mais variados sujeitos da sociedade, por diversas instâncias de comunicação surgidas pelo avanço de tecnologias.

Essa conjuntura estimula uma estrutura socioeconômica, em que o alcance nos pontos mais privilegiados se dá proporcionalmente ao acesso às tecnologias, aos meios de comunicação e serviços, como o de compras e vendas, educação à distância, acervos e bibliotecas digitais, bancos digitais, entretenimento por meio de streamings, vídeo-on-demand e aplicativos de transporte.

Esses e inúmeros outros serviços cotidianos estão em constante crescimento. O relatório anual feito em parceria entre We Are Social e Hootsuite[2], agências multinacionais de estratégias *online*, estima que, em 2021, das 7,83 bilhões de pessoas no mundo, 4,55 bilhões usam a internet, 5,22 bilhões usam telefone celular e 4,20 bilhões estão em mídias sociais. Todos esses números cresceram em relação ao ano anterior, impactados também pela pandemia da COVID-19 e a necessidade de trabalho remoto e afastamento social surgidas.

Em relação ao Brasil, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), afirmou em webinário que, em 2021, 78,3% dos brasileiros estão conectados a internet, fazendo do Brasil o 5ª no ranking de países em população on-line[3].

O lema "os dados são o novo petróleo"[4] marca a sociedade atual, em que o bem com maior valor de troca e que gera mais riqueza deixou de ser o petróleo, para serem os dados, principalmente os pessoais. Os dados representam oportunidades para que negócios cresçam tendo a eficiência e inovação como características básicas

---

[1] WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação**, Brasília, v. 29, n. 2, 2000, p. 71. Disponível em: http://revista.ibict.br/ciinf/article/view/889 . Acesso em: 20 nov. 2021.

[2] WE ARE SOCIAL; HOOTSUITE. **The Global State of Digital 2021**. Disponível em: https://www.hootsuite.com/pt/recursos/digital-trends. Acesso em 20 nov 2021.

[3] BRASIL, Brasil está entre os cinco países do mundo que mais usam internet, **Governo do Brasil,** 26/04/2021. Disponível em: https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/04/brasil-esta-entre-os-cinco-paises-do-mundo-que-mais-usam-internet#:~:text=Com%2078%2C3%25%20de%20brasileiros,fibras%20%C3%B3Pticas%20%C3%A0s%20redes%20nacionais. Acesso em 20 nov 2021.

[4] HUMBY, C. Data is the new oil. **ANA Senior marketer's summit**, Kellogg School, 3 Nov. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html. Acesso em 10 nov 2021.

e, ao contrário do petróleo, são infinitos e reutilizáveis. Cria-se um cenário onde tudo pode ser pensado, testado e melhorado de acordo com os objetivos da instituição, inclusive o comportamento humano, já que este e demais fatores são facilmente metrificados.

Os dados são essenciais para o uso da Inteligência Artificial e criaram mercados inteiramente novos, como o de *fintechs* (empresas que introduzem inovações tecnológicas nos mercados financeiros, com potencial para criar novos modelos de negócios, por plataformas *online,* como os bancos digitais).

A sociedade atual é marcada também pela Internet das Coisas (em inglês, IoT, *Internet of Things*), em que a evolução da internet faz com que objetos do cotidiano se comuniquem com os usuários e entre si, trocando comandos e agindo, tornando-se objetos inteligentes (*smart objects).*

Ainda que os avanços tecnológicos tenham encurtado fronteiras digitalmente e possibilitado novas formas de inclusão social e negócios, com o número de acessos e de pessoas *online* crescendo diariamente, é comum que novos desafios e problemas jurídicos surjam. Dentre esses estão a diminuição do escopo da privacidade e invasão ao espaço individual, pelo constante uso de mídias sociais e registros constantes da vida privada e incidentes envolvendo dados pessoais.

Informações pessoais são a todo momento produzidas, coletadas, armazenadas e processadas, inclusive sem o conhecimento do titular do dado. A partir dos rastros nos sítios eletrônicos, é possível cruzar dados pessoais sobre preferências políticas, interesses, compras feitas, lugares frequentados, endereços residenciais e profissionais e muitos outros. O resultado desses cruzamentos, contudo, pode ser utilizado contra os titulares dos danos, o que tem incitado debates públicos sobre leis de proteção de dados pessoais.

Dessa forma, percebeu-se imperativa a ação do Estado para a proteção da privacidade e dos dados pessoais, até mesmo dos que estão sob a sua tutela, a fim de garantir ao titular autonomia e direitos para proteger seus interesses e para que a sociedade caminhe em direção a uma democracia da informação. Além disso, como se verá abaixo, a ressignificação do conceito de privacidade tem tido um papel importante para o debate acerca dos limites da tecnologia. Esta, que antes versava

sobre o direito de ser deixado só, hoje é um direito fundamental que permite ao indivíduo ter controle sobre quais informações circulam sobre si. Por esses motivos, é possível enxergar as discussões sobre direito à privacidade intimamente conectadas aos debates sobre uso e coordenação de dados[5]

Isto posto, legislações atinentes à proteção de dados pessoais têm surgido mundo a fora, a fim de estabelecer os princípios, ferramentas, regras e sanções no cenário de tratamento de dados. Nesse sentido, o presente trabalho versa sobre a Lei Geral de Proteção de Dados Pessoais brasileira e foca em um dos tipos de incidentes de segurança mais preocupantes, o de vazamento de dados.

Vazamentos de dados ocorrem quando dados são indevidamente acessados e coletados por terceiros, que os usam para divulgar, vender, extorquir, manipular ou repassá-los. É comum que falhas em sistemas de segurança sejam identificadas e utilizadas para obter os dados ou que pessoas internas se utilizem de suas funções para gravar as informações e depois divulgá-las.

Considerando que a maioria dos dados atuais são armazenados em plataformas digitais, sejam essas de empresas privadas sejam de entidades públicas, é imprescindível se atentar aos malefícios que uma divulgação inapropriada pode causar. Além disso, é importante compreender que o debate acerca das externalidades negativas de vazamento de dados se dá dentro de um debate público e jurídico que tem valorizado cada vez mais a privacidade e o consentimento, no momento de aprovar a disponibilização de dados.

Assim, o progresso tecnológico reduziu drasticamente os custos e tem possibilitado o desenvolvimento de meios analíticos para processar ainda mais dados. Esse crescimento alerta para uma série de desafios globais envolvendo a proteção dos dados, privacidade, liberdade e outros direitos fundamentais.

Portanto, o presente trabalho versa sobre o tratamento dado pela Lei Geral de Proteção de Dados Pessoais (LGPD) ao vazamento de dados, percorrendo por

---

[5] MAGRANI, Eduardo; DE OLIVEIRA, Renan Medeiros. O *Bid Data* somos nós: novas tecnologias e gerenciamento pessoal de dados. *In:* **Governança e regulações da Internet na América Latina Análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance.** BELLI, Luca (org); CAVALLI, Olga (org). Rio de Janeiro: FGV Direito Rio, 2018, p. 347.

conceitos básicos atinentes à proteção de dados. A metodologia a ser empregada consistirá em revisão bibliográfica, bem como demonstração de situações fáticas.

Para tanto, o primeiro capítulo se divide no paradigma histórico anterior à LGPD sobre direito à privacidade e proteção de dados, tanto no contexto global quanto local. O segundo capítulo, por sua vez, traz as disposições e conceitos básicos sobre o tema, cujo foco é demonstrar como vazamento de dados e incidentes de segurança são tratados na legislação brasileira. Faz-se necessário neste momento apontar as influências legislativas estrangeiras, com foco no entendimento europeu sobre proteção de dados, além de exemplos de vazamentos. Por último, a terceira parte traz possíveis soluções e mecanismos desejados para a implementação de uma cultura organizacional com foco na governança e proteção de dados, incluindo a Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED).

1. PARADIGMA ANTERIOR A LGPD SOBRE DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS

1.1 Movimentações sociais e legislativas no exterior em prol da privacidade e proteção de dados

Nos parágrafos abaixo, são trazidos fatores internacionais antecedentes à promulgação da Lei Geral de Proteção de Dados Pessoais brasileira, relevantes acerca de privacidade e proteção de dados. Nesse sentido, há a exposição de elementos de legislações estrangeiras e de acontecimentos na sociedade mundial,

importantes para o estudo e entendimento de como se formou a lei brasileira, além de conceitos, como privacidade, privacidade informacional e proteção de dados.

A privacidade é um conceito complexo que possui elementos fundamentais, como a dignidade humana, liberdade e independência do indivíduo e controle sobre uso e abuso de informações pessoais. Contudo, sempre se apresenta como um bem de valor, cuja dimensão varia a cada sociedade, fazendo com que fatores religiosos, políticos, ambientais, econômicos, sociais e tecnológicos alterem a ideia do que pode ser privado[6], em contraposição do que deve ser publicizado.

Seu significado perpassa pelo entendimento do direito à intimidade, tipificado entre os "direitos da personalidade", que buscam proteger a dignidade da pessoa humana[7]. Externamente, a tutela jurídica da privacidade é esparsa, estando presente na Declaração dos Direitos do Homem e do Cidadão de 1789, a Declaração Universal dos Direitos do Homem de 1948 (art. 12), a 9ª Conferência Internacional Americana de 1948 (art. 5º), a Convenção Europeia dos Direitos do Homem de 1950 (art. 8º), Pacto Internacional de Direitos Civis e Políticos de 1966 da Organização das Nações Unidas (ONU), a Conferência Nórdica sobre o Direito à Intimidade de 1967, Pacto de São José da Costa Rica de 1969 (art. 11, 2.), entre outros[8].

Seu debate está presente desde a filosofia antiga, demonstrada pela dicotomia aristotélica[9] entre a vida política e a vida doméstica. A primeira, *polis,* era o espaço de todos, público, onde havia a cidade e espaços atrelados. A segunda, a *oikos*, era o espaço para obtenção de necessidades individuais e coletivas da família, bens, onde havia o cerne social e doméstico[10].

---

[6] MOORE, Adam. “Privacy: Its Meaning and Value”. **American Philosophical Quarterly**, Vol. 40, 2003. p. 215-227. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1980880. Acesso em: 25 de outubro de 2021.

[7] MIRANDA, Francisco Cavalcanti Pontes de. **Tratado de direito privado.** Campinas: Bookseller, 2000, tomo VII. p. 5 e ss.

[8] HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). **Tomo: Direito Administrativo e Constitucional.** Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade

[9] ARISTÓTELES. **Política**. Rio de Janeiro: Ediouro, 1988, p. 12 e segs.

[10] “A sociedade formada por pequenos burgos forma uma cidade completa, com todos os meios de se abastecer por si, e tendo atingido, por assim dizer, o fim a que se propôs. [...] É evidente, pois, que a

A passagem do tempo transformou o conceito de privacidade junto com o desmembramento das sociedades feudais e crescimento da burguesia, momento em que, os que possuíam meios para tanto, podiam se manter reclusos[11]. Já no século XIX, o direito à privacidade era dificilmente separado da defesa da propriedade privada e da honra. A segunda metade deste século marca o início de novos debates acerca do contorno de privacidade, inclusive juridicamente, nos continentes europeu e americano.

Em 1880, o juiz norte-americano Thomas Cooley comenta pela primeira vez, em seu trabalho "*A Treatise on the Law of Torts*", sobre o "*right to be let alone*" (o direito de ser deixado em paz ou o direito de estar só), neste trecho: "*The right to one's person may be said to be a right of complete immunity: to be let alone."*[12] O aprofundamento no conceito de privacidade, contudo, ocorre apenas anos depois.

Em 1890, os juristas Samuel D. Warren e Louis D. Brandeis publicam na *Harvard Law Review* o artigo *The Right to Privacy*[13], no qual abordam as transformações sociais, econômicas e políticas e o aparecimento de invenções que passaram a invadir a vida privada, a exemplo das fotografias[14]. Para os autores, o direito da privacidade é diferente ao da propriedade privada e, ao lesioná-la, fere-se a individualidade, dignidade, honra e independência da pessoa.

---

cidade faz parte das coisas da natureza, que o homem é naturalmente um animal político, destinado a viver em sociedade". Idem, p.12

[11] Diversos fatores ocasionaram que "[...] a privacidade evoluísse como um direito típico da classe burguesa em determinados ambientes sociais.[...] A possibilidade de aproveitar plenamente a própria intimidade é uma característica que diferencia a burguesia das demais classes: e o forte componente individualista faz com que esta operação se traduza, posteriormente, em um instrumento de isolamento do indivíduo burguês em relação à sua própria classe. O burguês, em outros termos, apropria-se de um seu "espaço", com uma técnica que lembra aquela estruturada para a identificação de um direito à propriedade "solitária". Em um nível social e institucional, portanto, o nascimento da privacidade não se apresenta como a realização de uma experiência "natural" de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo. Não é por acaso que seus instrumentos jurídicos de tutela foram predominantemente modelados com base naquele característico do direito burguês por excelência: a propriedade." RODOTÀ, Stefano. **A vida na Sociedade da Vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 26-28.

[12] COOLEY, Thomas McIntyre. **A treatise on the law of torts**. Chicago: Callaghan, 1880. p. 29.

[13] WARREN, Samuel; BRANDEIS, Louis. "The Right to Privacy". Harvard Law Review, Vol. IV, n.º 5, 1890. p. 193 e ss.

[14] Os autores consideram a proteção da vida privada uma necessidade: "*The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury*" (WARREN, Samuel; BRANDEIS, Louis, op. cit., p. 196.)

Nesse sentido, a garantia da privacidade passou a ter um entorno de proteção contra intromissões indesejadas e que afetem, de alguma forma, traços individuais. O direito passaria a buscar a proteção de dados pessoais, sentimentos, nome e informações que remeteriam à vida privada de cada um. O tema evoluiu na jurisprudência norte-americana, com casos como Schuyler v. Curtis (1891)[15], Pavesich v. New England Life Ins. Co (1905)[16] e Griswold v. Connecticut (1965)[17].

É importante notar que a não interferência na vida privada de um cidadão diz respeito tanto a outro indivíduo quanto ao Estado. A ambos são colocados empecilhos e limites ao se tratar da privacidade e vida íntima alheia e, em relação ao poder estatal, é possível, ainda, reivindicar sua proteção e jurisdição[18].

No século XX, as inovações tecnológicas causaram mudanças no conceito e no grau de importância estimado pela sociedade quanto à privacidade, uma vez que passou a ocorrer quantidade maior de ofensas e tentativas de se obter informações sobre a vida alheia. Novamente, vale ressaltar apontamentos feitos da jurisprudência norte-americana, de quando a Suprema Corte percebeu haver quatro tipos de violação ao direito à privacidade, descritos por William Prosser, professor da California School of Law (Berkley), em 1960[19]: a ingerência na vida, solidão ou assuntos privados alheios; divulgação pública de fatos privados delicados; publicidade que posiciona

---

[15] O caso Schuyler v. Curtis trata do reconhecimento do direito à imagem, inclusive de uma pessoa falecida. O autor desejava proibir a construção de uma estátua em homenagem à tia em um evento. A primeira instância da Suprema Corte de Nova Iorque, observando o "*right to privacy*" descrito por Warren e Brandeis, acolheu o pedido, apontando que a falecida possuía vida reclusa. No entanto, este entendimento foi revertido, em apelação, sendo alegado que o direito à privacidade não subsistiria após a morte da senhora (HAND, Augustus N. ***Schuyler against Curtis and the Right to Privacy. The American Law Register and Review, Philadelphia,*** vol. 45, n. 12, p. 745-759, dez. 1897, passim).

[16] O caso discute a possibilidade de reprodução não autorizada de retratos, em um jornal. Na situação, o autor foi posicionado ao lado da fotografia de um homem mal cuidado, tendo sido atribuída a prosperidade desse ao fato de ter contratado uma apólice de seguro. A decisão foi no sentido de reçachar a publicação da imagem de um individuo, sem seu consentimento e com fim comercial, o que configuraria uma violação ao *right of privacy,* sem necessidade da pessoa retratada provar o dano (PROSSER, William Lloyd, ***Handbook of the law of torts***, p. 803, 4 ed. St. Paul: West, 1971)

[17] O julgamento inovou ao estender o limite do right to privacy para impedir a intervenção estatal na privacidade conjugal, ao estimar possível a negativa de coletar informações sobre uso de contraceptivos por pessoas casadas. Na decisão, o Ministro Willian O. Douglas discorre que, embora o direito à privacidade não esteja previsto na Constituição, pode ser encontrado nas “penumbras” e “emanações” de outras garantias (SOLOVE, Daniel J.; ROTENBERG, Marc; SCHWARTZ, Paul M., ***Privacy, information, and technology***. Aspen Law & Business, 2008. p. 28-29.)

[18] GAVISON, Ruth. ***Privacy and the limits of law.*** *The Yale Law Journal,* v. 89, nº 3, 1980. p. 438. Disponível em: https://digitalcommons.law.yale.edu/ylj/vol89/iss3/1. Acesso em 25/10/2021

[19] NAVARRO, Ana Maria Neves de Paiva; LEONARDOS, Gabriela. Privacidade Informacional: Origem e Fundamentos no Direito Norte-Americano. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=34f9a343f945196b>. Acesso em 25/10/2021.

alguém sob uma "falsa luz" aos olhos da sociedade (quando, por exemplo, atribui-se erroneamente uma fala a alguém) e a apropriação de imagem, nome ou outra característica alheia para fins de publicidade[20], podendo, contudo, pessoas públicas serem sujeitas a maior publicidade de alguns fatos[21].

Há algumas décadas surgiu, ainda, uma nova faceta da privacidade: a informacional, extremamente ligada a novas tecnologias da informação. Essas são tecnologias em microeletrônica, computação, telecomunicações/radiodifusão, optoeletrônica e engenharia genética[22], que propiciam uma capacidade social ininterrupta de comunicação e gerar rastros dos dados e daqueles que os geram.

Nesse sentido, vale analisar a relação entre essas novas tecnologias da informação, seus efeitos na privacidade e como o direito vem sendo instrumentalizado para prevenir e sanar efeitos negativos. Um tema, em especial, que se originou em meio a esse debate foi o da proteção de dados pessoais[23], na medida em que o ordenamento jurídico é desafiado com as implicações do tratamento informatizado de dados[24].

Legisladores ao redor do mundo ocuparam-se para resguardar além da privacidade no sentido da vida íntima, mas os dados pessoais de seus cidadãos, porque entenderam serem esses extensões dos indivíduos. Alguns países, como Espanha, Portugal, Hungria, Eslovênia e Rússia, reservam à tutela constitucional o direito à privacidade informacional[25].

Assim, é importante entender como o movimento em prol da proteção de dados e de seus titulares se deu em outros contextos, a fim de compreender o âmbito no qual se insere a lei brasileira.

---

[20] PROSSER, William. ***Privacy***. California Law Review, Vol. 48, 1960. p.383.
[21] PROSSER, William, op. cit., p. 411
[22] CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura. Vol 1. A sociedade em rede.** Trad: Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999. p. 49.
[23] Id. A Galáxia da Internet. **Reflexões sobre a internet, os negócios e a sociedade.** Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003, p. 28 e 29.
[24] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006, p. 27.
[25] VIEIRA, Tatiana Malta. **O Direito à Privacidade na Sociedade da Informação: efetividade desse direito fundamental diante da tecnologia da informação.** Porto Alegre: Sergio Antonio Fabris Editor, 2007, p. 44.

Doutrinadores defendem a visão de que a proteção de dados pessoais divide-se em quatro gerações de regulamentações[26], introduzidas por Viktor Mayer-Scönberger, professor da Universidade de Oxford. A primeira geração é vinda do Estado Moderno, onde este detinha grandes bancos de dados da população, que possibilita o controle desta. Assim, a jurisdição possuía o Estado como destinatário das primeiras leis, surgidas, por exemplo, nos Estados Unidos[27] e na Alemanha.

A segunda geração, na década de 1980, se ocupa em expandir o destinatário das leis até o setor privado, pois, de acordo com Bioni (2019, p. 115), a figura do grande irmão (Estado, o grande centralizador da base de dados) é diluída pela de pequenos irmãos (bancos de dados dispersos entre entes privados e estatais. Começam a surgir meios para cidadãos defenderem seus interesses. Nesse meio, inicia-se o debate acerca do desafio que é exercer um consentimento livre e consciente, enquanto vive-se em sociedades que constantemente demandam receber informações pessoais para prover serviços. Mayer-Schönberger salienta esse custo social a ser pago, que atormenta o direito à privacidade e à proteção de dados:

> A proteção de dados pessoais como liberdade individual pode proteger a liberdade do indivíduo. Ela pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo que se tem de pagar por isso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas? Será que nós alcançamos o estágio ótimo da proteção de dados se garantirmos os direitos à privacidade que, quando exercidos, acarretarão a exclusão do indivíduo da sociedade?[28]

Já na década de 1990, a terceira geração engaja-se na efetividade da proteção do direito à privacidade e propõe o protagonismo do cidadão no processo de tratamento de dados, mediante o seu consentimento. Este começa a ser usado para legitimar e justificar a proteção de dados pessoais e para garantir a autonomia e segurança do titular. Surgem debates acerca da autodeterminação informativa, afirmando Doneda (2011, p. 95) que a autodeterminação informativa constitui no

---

[26] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014, Capítulo 1.

[27] Um exemplo é o Privacy Act, norte-americano de 1974, que estabelece um código de práticas sobre a coleta, manutenção, uso e disseminação de informações sobre indivíduos, mantidas em sistemas de registros por agências federais. Disponível em: https://www.justice.gov/opcl/privacy-act-1974. Acesso em 27/10/2021

[28] MAYER-SCHÖNBERGER, **Generational Development of Data Protection in Europe.** In: Technology and Privacy: The New Landscape. The MIT Press: Massachusetts, 2001, p.228

direito que o indivíduo tem de controlar a obtenção, titularidade, tratamento e transmissão de dados pessoais.

Alguns exemplos de textos em lei surgidos nesse período são a introdução constitucional da proteção de dados pessoais na Holanda, a emenda na lei da Áustria de 1986 e alteração legislativa na lei norueguesa.

Neste momento também ampliam-se os meios de telecomunicação e a velocidade na transmissão de informações. O armazenamento de dados deixa de estar em uma central única e se dispersa em redes e, não raro, dificilmente se localizava o local exato de tratamento[29].

A quarta geração, presente hoje, encabeça o protagonismo do consentimento como permissão para coleta e uso de dados pessoais. As leis priorizam os titulares, em detrimento a terceiros que possam a vir manipular suas informações pessoais contra a vontade ou conhecimento desses. Por sua vez, o contorno do consentimento expande até que este seja “livre, informado, inequívoco, explícito e/ou específico”, o que vem sendo sedimentado em leis e decisões judiciais.

Assim, tem se buscado assegurar a preponderância do cidadão na gerência de seus dados pessoais. Isso pode ser percebido pelo uso de uma classificação para os chamados "dados pessoais sensíveis", que demandam extrema cautela e critérios para serem manuseados. Este impedimento total ou parcial se deve aos riscos de identificação e discriminação que podem vir a ser sofridos, caso dados como etnia, religião, orientação sexual e outros sejam disseminados.

Como se pode perceber, as normas de proteção de dados não são exclusivas da última década e se adequam a pressões e necessidades sociais que, em especial no contexto atual, mudam intensamente, por conta dos avanços tecnológicos, os seus riscos para a privacidade e a nova forma de se encarar os dados como uma fonte de renda, nos dias atuais.

[29] Ibid, p. 230.

Nesse cenário, é imprescindível apontar as legislações recentes que mais influenciaram a Lei Geral de Proteção de Dados Pessoais brasileira, a começar pelas iniciativas europeias.

A União Europeia possui diversos instrumentos normativos para promover a proteção de dados pessoais: a Carta de Direitos Fundamentais da UE (arts. 7º e 8º)[30], a Convenção 108 do Conselho de Europa (1981)[31], a Convenção Europeia dos Direitos Humanos (CEDH)[32] e a Diretiva 95/46/CE do Parlamento Europeu e do Conselho (1995)[33], também conhecida como Diretiva de Proteção de Dados. Esta é importante para a exclusão de regras contraditórias presentes nesta e na Convenção 108, já que os quinze Estados-Membro da UE em 1995 assinaram ambos documentos[34]. Note-se que países não membros da UE, mas que fazem parte do Espaço Económico Europeu (EEE), se comprometeram com o documento – a saber, a Islândia, o Listenstaine e a Noruega.

Apesar de existirem essas e outras diretivas, a que mais de destaca e se tornou influente foi o Regulamento Geral sobre a Proteção de Dados, n.º 2016/679 do Parlamento Europeu e do Conselho (*General Data Protection Regulation - GDPR* ou RGPD, na sigla sem tradução). Este revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) e entrou em vigor em maio de 2018.

As regras destinam-se a todos os cidadãos da UE contra violações da privacidade e dos dados. Alguns dos direitos incluem: consentimento claro e positivo do tratamento dos seus dados e o direito de receber informações claras e

---

[30] Os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia colocam como direitos fundamentais o respeito pela vida privada e a proteção dos dados pessoais.

[31] A Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108) do Conselho da Europa foi o primeiro instrumento internacional juridicamente vinculativo adotado acerca da proteção de dados. Visa garantir, especialmente, o direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal. Aplica-se a todos os tratamentos de dados pessoais realizados tanto pelo setor privado como pelo setor público.

[32] O artigo 8.º da Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais confirma o direito e respeito pela vida privada e familiar, domicílio e correspondência.

[33] Foi o principal instrumento jurídico da UE sobre proteção de dados relativo ao tratamento de dados pessoais e à livre circulação desses. Foi adotada em 1995, quando alguns Estados-Membros já tinham adotado leis nacionais sobre o assunto. A livre circulação de mercadorias, capitais, serviços e pessoas no mercado interno exigia o livre fluxo de dados, o que tornou imprescindível a existência de parâmetros uniformes e exigentes em relação à proteção de dados. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>. Acesso em: 28 out 2021

[34] CONSELHO DA EUROPA. **Manual da Legislação Europeia sobre Proteção de Dados.** Luxemburgo, 2014. Disponível em: <https://www.echr.coe.int/Documents/Handbook_data_protection_Por.pdf>. Acesso em 28 out 2021.

compreensíveis sobre o mesmo; o direito ao esquecimento – há a previsão do direito de exclusão de dados; o direito a transferir os dados para outro prestador de serviços (exemplo: de um provedor para outro) e o direito de saber se os seus dados foram pirateados. As novas regras aplicam-se a todas as empresas que oferecem serviços na UE, mesmo que tenham sede fora dela[35].

A aplicabilidade do GDPR para além da União Europeia impactou diretamente o Brasil. Além disso, com a sua vigência, o bloco passou a listar oficialmente os países que possuíam "níveis adequados de proteção de dados". Caso não possuíssem, seriam aplicados óbices à transferência internacional de dados[36].

O nível adequado de proteção de dados pode ser obtido, caso o país possua legislação nacional “relevante”, cujas regras, dentre outros assuntos, sejam: a proteção de dados pessoais; medidas de segurança; direitos dos titulares de dados e; previsão de medidas administrativas e judiciais efetivas para assegurá-los (art. 45, 2, “a”). A matéria sobre vazamento de dados é tratada mais à frente.

Como se verá abaixo, o GDPR serviu como fonte de inspiração à Lei Geral de Proteção de Dados Pessoais brasileira e agilizou o seu processo dentro das casas legislativas, haja vista os empecilhos que poderiam surgir sem uma lei nacional relevante sobre o tema.

2.2 Direito à privacidade e proteção de dados na legislação brasileira

Uma vez descritos os panoramas históricos gerais que antecederam a LGPD, é importante aprofundar as ligações entre as legislações brasileiras atuais de temas correlatos.

---

[35] MACIEJEWSKI, Mariusz. **Proteção de Dados pessoais. Fichas Técnicas sobre a União Europeia - 2021**. Disponível em: <https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf>. Acesso em 28 out 2021.

[36] IRAMINA, Aline. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, no 2, p. 91-117, outubro de 2020, p. 102

Aspectos políticos, econômicos e sociais fizeram com que fosse imperativo a LGPD responder aos riscos a liberdades individuais, de autodeterminação comportamental e de pensamento dos titulares, “cada vez mais comprometida diante do crescente poder de manipulação que decorre do processamento de dados”[37]. Nesse cenário, ainda que a LGPD seja tipicamente uma norma jurídica de direito privado, também se preocupa com interesses públicos e transindividuais, como a integridade dos procedimentos democráticos.

A LGPD é o principal instrumento normativo acerca do tema de proteção de dados e privacidade informacional no país. Além desta, existem previsões normativas anteriores de temas subjacentes importantes para a compreensão da LGPD. Assim, nesta parte se comenta as demais normas brasileiras que se somam à aplicação e entendimento das diretrizes da LGPD.

A proteção à privacidade, a defesa do consumidor, traços de liberdades individuais e regras para bom convívio no meio digital já foram previstas no ordenamento jurídico brasileiro.

A Constituição Federal, em seu art. 5º, X e XI trata de proteger parte da privacidade, declarando que são invioláveis a intimidade, a vida privada, a honra, a imagem e a casa das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação.

Danilo Doneda também identifica no instituto do *habeas data* (art. 5º, LXXII), a primeira materialização concreta de direitos relacionados à proteção de dados pessoais assegurados perante o Estado, porque foi vista como remédio adequado para tutelar, na via processual, “um direito material de acesso e retificação com relação aos dados pessoais"[38].

---

[37] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52. ISBN 978-85-5321-663-5. p. 49.

[38] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais.** 1. ed. Rio de Janeiro: Forense, 2021. p. 3-20. ISBN 978-85-309-9151-7. p. 13

Outros dispositivos constitucionais a serem comentados são o do direito à informação (art. 5º, XIV), liberdade de expressão (art. 5º, IX) e o da proteção contra interceptação das comunicações telefônicas, telegráficas ou de dados (art. 5º, LXXII).

A Constituição não reconhece a proteção de dados como um direito autônomo e fundamental, porém é possível defender esse status, considerando os riscos que o tratamento automatizado traz à proteção da personalidade haja vista as garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada (DONEDA, 2011, p. 103).

Tendo isso em vista, o Plenário do Senado Federal aprovou, em outubro de 2021, a Proposta de Emenda à Constituição (PEC) 17/2019[39], que torna a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental, propondo o acréscimo do inciso XII-A[40] ao art. 5º e do XXX[41] ao art. 22. A PEC também remete privativamente à União a função de legislar sobre o tema[42]. O texto, agora, necessita ser aprovado pelo Congresso Nacional.

O texto de justificativa que acompanha a PEC ressalta a evolução do assunto em legislações ao redor do mundo e a preocupação com os riscos às liberdades e garantias individuais. Sua aprovação põe no mesmo patamar de direito fundamental o direito à proteção de dados, privacidade e liberdade de informação.

O marco legal subsequente foi o Código de Defesa do Consumidor ou CDC (Lei nº 8.078/90), que "acabou por concentrar um volume considerável das demandas relacionadas a dados pessoais"[43], pois nele se encontram previsões expressas

---

[39] BRASIL, **Proposta de Emenda à Constituição nº 17 de 2019.** Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em 5 nov 2021

[40] "XII-A - é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais".

[41] "XXX - proteção e tratamento de dados pessoais"

[42] BRASIL, Senado Federal aprova Proposta de Emenda à Constituição 17 (PEC 17/2019) que inclui a proteção de dados pessoais no rol de direitos e garantias fundamentais. **Agência senado.** Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais>, 21/10/2021. Acesso em 5 nov 2021.

[43] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais.** 1. ed. Rio de Janeiro: Forense, 2021. p. 3-20. ISBN 978-85-309-9151-7. p. 13-14

relacionadas ao direito do consumidor sobre seus dados pessoais. O art. 43, *caput*, §§1° a 3° e 6° exemplificam isso, tendo parte do seu conteúdo sido replicada na LGPD, na parte de tratamento de dados pessoais em geral.

A aplicação do CDC, antes mesmo da aplicação da LGPD, exerceu influência nas decisões do Superior Tribunal de Justiça (STJ), como se observa no voto do Ministro Ricardo Villas Bôas Cueva no REsp 22.337-8/RS de 1996, quando, pela primeira vez, mencionou-se um "direito fundamental à autodeterminação informativa"[44]. O momento era de preocupação com a vulnerabilidade em escala do cidadão frente ao armazenamento de suas informações, capaz de ferir o direito constitucional à privacidade.

O Código do Consumidor também exige que cadastros, registros e dados dos consumidores sejam claros, objetivos e verdadeiros, com linguagem de fácil compreensão (art. 43, *caput* e § 1°). Para a abertura desses registros é necessária a comunicação por escrito ao consumidor (art. 43, § 2°). Caso os dados nesses registros sejam inexatos, o consumidor pode exigir a correção, a ser respondida aos destinatários eventual correção, no prazo de cinco dias úteis (art. 43, § 3°).

Assim, a lei consumerista busca proteger o consumidor de banco de dados que possam a vir atingir sua personalidade ou informações pessoais (BIONI, 2020), porém ainda não desenvolvia o tema do consentimento.

Em 2011, a lei nº 12.414/2011, Lei do Cadastro Positivo (LCP), passou a regulamentar dados derivados de operações financeiras e adimplementos dos consumidores, para facilitar a concessão de crédito e a formação de um histórico (KRIEGER, 2019. É possível afirmar que a lei consolida o conceito de autodeterminação informativa pois prioriza o consentimento como requisito para compartilhamento lícito de dados (MENDES, 2014. Recentemente, a LCP tem sido alterada, como se vê abaixo.

[44] CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do STJ. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 85-98. ISBN 978-85- 5321-663-5. p. 88

Em 2019, após a elaboração da Lei Complementar nº 166/2019[45], o Poder Executivo editou Decreto regulamentador (Decreto nº 9.936)[46], o qual modifica o modelo de inclusão dos consumidores no sistema de cadastro positivo, para ampliar a base de dados de adimplentes. Para isso, permite-se, sem haver infração ao sigilo bancário, que instituições financeiras e demais autorizadas pelo Banco Central do Brasil (BACEN) compartilhem dados de adimplemento aos gestores de bancos de dados cadastrados junto a ele.

O Decreto é especialmente interessante para este trabalho pois prevê diretrizes para a ocorrência de vazamento de dados que possam acarretar prejuízos ou riscos relevantes à Cadastrados (art. 18), *in verbis*:

> DOS PROCEDIMENTOS NA HIPÓTESE DE VAZAMENTO DE INFORMAÇÕES
>
> Art. 18. Na ocorrência de vazamento de informações de cadastrados ou de outro incidente de segurança que possa acarretar risco ou prejuízo relevante a cadastrados, o gestor de banco de dados comunicará o fato:
>
> I - à Autoridade Nacional de Proteção de Dados, na hipótese de ocorrência que envolva o fornecimento de dados de pessoas naturais;
>
> II - ao Banco Central do Brasil, na hipótese de ocorrência que envolva o fornecimento de dados prestados por instituições autorizadas a funcionar pelo Banco Central do Brasil; e
>
> III - à Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública, na hipótese de ocorrência que envolva o fornecimento de dados de consumidores.
>
> § 1º A comunicação de que trata o *caput* será feita no prazo de dois dias úteis, contado da data do conhecimento do incidente, e mencionará, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os cadastrados envolvidos;
>
> III - a indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive os procedimentos de encriptação;
>
> IV - os riscos relacionados ao incidente; e

---

[45] BRASIL. **Lei Complementar nº 166, de 8 de abril de 2019.** Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp166.HTM>. Acesso em: 05 nov 2021

[46] BRASIL. **Decreto regulamentador da Lei do Cadastro Positivo.** Decreto nº 9.936, de 24 de julho de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9936.htm >. Acesso em: 05 nov 2021.

> V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> § 2º No juízo de gravidade do incidente de que trata o caput , será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.
>
> § 3º Será obrigatória a pronta comunicação aos cadastrados afetados pelo incidente de segurança de que trata este artigo.

Desse modo, entende-se que, em caso de vazamento de dados, os gestores de dados podem ser sancionados com base na LGPD, nas normas setoriais do Banco Central, na Lei do Sigilo Bancário e no Código de Defesa do Consumidor. Além disso, permanece o dever de comunicação do incidente com informações, como a descrição da sua natureza, os riscos relacionados e medidas que foram ou serão adotadas.

Outras leis que versaram sobre proteção de dados são a Lei de Acesso à Informação – LAI (nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965), de 23 de abril de 2014 (Marco Civil da Internet).

A LAI cuida de regulamentar os dizeres constitucionais (no art. 5º, inc. XXXIII; art. 37, §3º, inc. II; e art. 216, §2º), voltados à necessidade de transparência e publicidade da Administração Pública com relação aos cidadãos. Obrigada o Governo a disponibilizar ao cidadão informações de caráter público, instituindo obrigações, prazos e procedimentos para a divulgação de dados[47]. Em seu art. 4º, IV, positivou o conceito de “informação pessoal”, praticamente igual ao de “dado pessoal”, na LGPD nos termos de seu art. 5º, I.

Por sua vez, o Marco Civil da Internet rege os princípios que regulam o uso da internet no Brasil. Seu art. 3º prevê princípios, como o da proteção da privacidade e dos dados pessoais, e assegura, como direitos e garantias dos usuários de internet a inviolabilidade e sigilo do fluxo de suas comunicações privadas armazenadas, salvo por ordem judicial[48]. Seu art. 31 reforça a ideia de que o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida

---

[47] Ministério da Justiça e Segurança Pública, Governo Federal. **Sobre a Lei de Acesso à Informação - LAI.** Disponível em: https://www.justica.gov.br/Acesso. Acesso em 5 nov 2021.

[48] Tribunal de Justiça do Distrito Federal e dos Territórios - TJDFT. **Marco Civil da Internet.** Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet. Acesso em 5 nov 2021

privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. Por fim, há que se dizer que o Marco Civil da Internet é silente em relação ao tratamento de dados pessoais sensíveis, inclusive quanto à necessidade de consentimento para uso desses.

Como se pode perceber, a disciplina da proteção de dados estava dispersa instrumentos normativos independentes até a LGPD, formando um quadro de "colcha de retalhos", de pouca segurança jurídica, conforme afirma Bruno Bioni[49]:

> “Até a aprovação da LGPD, o Brasil contava somente com leis setoriais de proteção de dados. Era uma verdadeira “colcha de retalhos” que não cobria setores importantes da economia e, dentre aqueles cobertos, não havia uniformidade em seu regramento. Essa assimetria gerava insegurança para: a) que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios; b) a formulação de políticas públicas e parcerias público privadas igualmente dependentes desse intercâmbio de dados; e c) o cidadão que não detinha uma proteção integral e universal com relação a todas as atividades do cotidiano em que fornece seus dados, seja para o setor privado ou público”.

Desta feita, a LAI e o Marco Civil da Internet não abordam procedimentos a serem seguidos em caso de vazamento de dados, apesar de serem instrumentos importantes para a consolidação de um ambiente jurídico que promove a segurança da informação. Assim, cabe à LGPD regulamentar este e demais incidentes.

2. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): violação de dados, incidentes de segurança e vazamentos de dados

2.1. LGPD: Conceitos e disposições

Conforme se tem demonstrado, a proteção de dados pessoais surgiu como um desdobramento do direito à privacidade e um imperativo na era das tecnologias de informação e comunicação. Os dados são de extrema importância para a formação da personalidade e gerência da própria vida, ao mesmo tempo em que são peças valiosas no mercado de consumo atual.

---

[49] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019. p. 133.

Tendo sido exposto o ambiente social e jurídico ao que se insere a Lei nº 13.709/2018, faz-se mister analisar quais seus preceitos e regramentos, principalmente os atinentes aos incidentes de segurança e vazamento de dados. É importante atentar ao fato de que seu texto foi aprovado em 2018, porém só entrou em vigência em setembro de 2020, enquanto a Autoridade Nacional de Proteção de Dados (ANPD) só pôde aplicar sanções a partir de 1º de agosto de 2021.

A sua entrada em vigor garantiu ao Brasil a inserção ao grupo de países com leis que versam especificamente sobre proteção de dados e que foi fortemente inspirada no Regulamento Geral sobre Proteção de Dados europeu (em inglês, GDPR).

A LGPD busca proteger a privacidade dos usuários e dos seus dados pessoais, quando tratados por pessoa jurídica de direito público ou privado, inclusive nos meios digitais (art. 1º). Para isso, inova ao garantir ao cidadão a possibilidade de acesso a informações de como seus dados são coletados, processados e armazenados e assegura à Autoridade Nacional de Proteção de Dados a competência para fiscalizar organizações. Com o objetivo de efetivamente atingir seus fins, a lei traz definições de conceitos importantes e estabelece princípios, que merecem ser brevemente mencionados.

Para a lei, o conceito de dado pessoal (art. 5º, I) é toda informação relacionada a pessoa natural identificada ou identificável. Assim, a lei permite que o dado possa por si só ou combinado com outros gerar a identificação. Há, ainda, o dado pessoal sensível (art. 5º, II)[50], sujeito a condições e tratamentos específicos, pelo seu potencial discriminatório. Outro tipo de dado que exige atenção especial é o de crianças e adolescentes, sendo imprescindível o consentimento específico e em destaque de um dos pais ou responsáveis legais (art. 14, § 1º).

A compreensão da lei passa, ainda, por um entendimento abrangente. Laura Schertel e Danilo Doneda identificam cinco núcleos principais, sendo eles: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes

[50] Art. 5º, II - dado pessoal sensível: Aquele 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.

de tratamento de dados e v) responsabilização dos agentes[51]. No momento, cabe introduzir as três primeiras divisões, pois as restantes são comentadas no capítulo seguinte, referente ao estudo dos incidentes de segurança, especificamente do vazamento de dados.

O primeiro núcleo refere-se à aplicação material da lei. O art. 3º é categórico ao afirmar que a proteção se estende a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que o tratamento tenha ocorrido no Brasil ou ofereça bens e serviços a pessoas que estejam em território nacional.

Ao se referir apenas à proteção de dados pessoais, a LGPD exclui as pessoas jurídicas (art. 1º e 5º, I). Algumas situações que tratam de dados pessoais também são escusadas de obedecerem à LGPD (art. 4º), como quando há o tratamento com cunho jornalístico, artístico, acadêmico ou sobre segurança pública[52]. É importante notar que as exceções à regra ocorrem por defesa de direito fundamental (como a liberdade de informação para fim acadêmico) ou por interesse público relevante (defesa nacional).

Em relação ao segundo núcleo (legitimação para tratamento de dados), a Lei impõe que o tratamento de dados esteja atrelado a uma hipótese autorizativa informada no art. 7º (dados pessoais), art. 11 (dados pessoais sensíveis) ou art. 23

---

[51] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor, vol. 120, ano 27**, p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018, p. 472

[52] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

(pessoas jurídicas de direito público). Alguns exemplos são o consentimento, para a proteção da vida.

Por sua vez, o terceiro núcleo da LGPD abarca os princípios e direitos do titular que, juntos, fornecem ao cidadão ferramentas para controle e proteção de seus dados por terceiros[53].

São dez os princípios da LGPD: o da finalidade[54], adequação[55], necessidade[56], livre acesso[57], qualidade dos dados[58], transparência[59], segurança[60], prevenção[61], não discriminação[62] e responsabilização[63]. Esses são peças fundamentais para que os indivíduos exerçam sua autodeterminação informativa e algum controle sobre seus dados, assim como para que haja limites nos tratamentos de dados ou, pelo menos, minimização do uso desses.

Vale mencionar que a lei, em relação ao princípio da transparência, parece colocá-lo como regra destacada, pois exige que o consentimento seja transparente, mesmo nas hipóteses em que este não é exigido prévia e expressamente.

---

[53] MENDES, Laura Schertel; DONEDA, Danilo. op. cit. p. 474.

[54] Art. 6º, 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.

[55]Art. 6º, II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

[56] Art. 6º, 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.

[57] Art. 6º, 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;

[58] Art. 6º 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.

[59] Art. 6º, 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;

[60] Art. 6º, 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;

[61] Art. 6º, VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

[62] Art. 6º, IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

[63] Art. 6º, 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.

Em relação aos direitos dos titulares, deve-se procurar o art. 18 da lei, que autoriza o titular a obter do controlador, mediante requisição, diversas ações. São elas: confirmação de tratamento (inciso I), acesso aos dados (inciso II), correção de dados incompletos, inexatos ou desatualizados (inciso III), anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei (inciso IV), portabilidade de dados (V), eliminação dos dados obtidos com consentimento (inciso VI), informação das entidades públicas e privadas com as quais o controlador compartilhou dados (inciso VII), informação sobre a possibilidade de não fornecer consentimento e sobre as consequências negativas (inciso VIII) e revogação do consentimento (inciso IX).

Tendo sido abordadas as principais disposições da lei no que tange os três primeiros núcleos, passa-se a analisar, os últimos dois, sobre obrigações dos agentes de tratamento de dados e responsabilização dos agentes.

2.2 Violação de dados, incidentes de segurança e vazamento de dados: conceitos

A privacidade e a proteção de dados pessoais relacionam-se com diversos valores e interesses de ordem social e legal. Tem-se envolvido na discussão o progresso tecnológico, fluxo de informações, tráfego internacional de dados, autodeterminação informativa, direitos da personalidade e de proteção contra discriminação, inclusive pelo cruzamento de informações.

A dinamicidade e a quantidade de dados usados em sociedade levantam a preocupação das inúmeras violações possíveis e quais seriam os atores a serem responsabilizados pela falta de mecanismos de segurança e reparação de danos. Por isso, tem crescido a preocupação com a segurança da informação e com a observância dos agentes acerca dos princípios e regramentos das normas atinentes à proteção de dados.

A segurança da informação abarca o objetivo de preservar a confidencialidade, integridade e disponibilidade da informação, a fim de gerar ações em todo o ambiente institucional das empresas, para que essas passem a ter mecanismos de prevenção, detecção e proteção de ameaças digitais

Uma das dificuldades atuais sobre a segurança das informações dos titulares é justamente a abrangência e a dominação das ferramentas tecnológicas para as mais diversas atividades, do trabalho ao lazer. Usa-se a internet e meios informáticos para armazenamento, comunicação, pesquisas, compras, transferências bancárias. A partir desses usos, são gravadas informações pessoais que podem ser combinadas com outros rastros não perceptíveis ao usuário, formando um perfil específico e desconhecido pelo próprio titular dos dados. Uma das violações mais graves para essa e demais situações é o vazamento de dados, o qual vulnerabiliza a pessoa a qualquer malfeitor.

Assim, deve ser analisada a disciplina da violação de dados e dos incidentes de segurança, com especial atenção ao vazamento de dados, perpassando por alguns deveres e conceituação de atores.

Não raro, o tratamento de dados é acompanhado do fornecimento de bens e serviços no mercado de consumo, sendo importante a ligação com o Código de Defesa do Consumidor. Tanto este (art. 4º, III)[64] quanto a LGPD (art. 6º, *caput*) têm como princípio a boa fé objetiva, o qual possui deveres anexos e de proteção[65].

Uma consequência da boa fé objetiva é o dever de informar. A informação deve ser fornecida ao titular sobre quais dados são coletados, os meios de proteção desses e os riscos envolvidos na atividade de tratamento. Isso visa proteger o titular de prejuízos e deve ser observado até mesmo após o término da relação, se houver justificativa que permita o armazenamento das informações (art. 15, I e 16 da LGPD).

Em relação ao dever de segurança, Fabiano Menke e Guilherme Damasio Goulart[66], comentam sobre os quatro atributos de uma informação intrínsecos a sua

---

[64] Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;

[65] MARTINS-COSTA, Judith; BRANCO, Gerson. **Diretrizes teóricas do novo Código Civil brasileiro.** São Paulo: Saraiva, 2002. p.133

[66] MENKE, Fabiano; GOULART, G. D. Segurança da Informação e Vazamento de Dados. In: Bruno Et Al (coords.) Bioni. "**Tratado De Proteção De Dados Pessoais"**. São Paulo: Editora Forense. 2020, versão iBooks, p. 1181.

segurança. Há a confidencialidade, que é a característica da informação que precisa ser protegida contra um acesso ou uso não autorizado, a integridade, que é o atributo que visa garantir que a informação não foi alterada no seu ciclo de vida (a não ser quando autorizada) e a disponibilidade, que é o atributo que a informação estará disponível quando necessário[67].

O quarto atributo, construído recentemente e presente no GDPR, é o da resiliência, que se desdobra na elasticidade, robustez e aptidão de adaptação. Isso significa, na prática, que erros ou incidentes são possíveis, devendo os sistemas os preverem para recomporem suas funções essenciais rapidamente[68].

A proteção desses quatro atributos são intimidados por quatro situações intrinsecamente relacionadas: vulnerabilidade, ameaça, incidente e controle. A vulnerabilidade é a mais disseminada, pois é sobre a fragilidade de todo sistema, ferramenta, processos, armazenamentos, entre outros, que pode ser atingida por uma ameaça. Por sua vez, o incidente ocorre quando uma vulnerabilidade é atingida por uma ameaça, que pode ser física, pessoal, ambiental ou técnica[69], incitando o surgimento dos controles, para que medidas sejam tomadas a fim de impedir novamente um incidente ou, pelo menos, diminuir a probabilidade de sua ocorrência[70].

Não raro, há situações em que o incidente ocorre e, mesmo havendo mecanismos de controle e tentativas de remediar a situação, o dano não pode ser estancado. É o caso dos vazamentos de dados, em que ações posteriores dificilmente conseguem apagar dos inúmeros registros de pessoas e organizações que captaram os dados, afetando o atributo da confidencialidade[71].

Para a definição de violação de dados, usa-se o regramento europeu, GDPR, art. 4º, item 12, pois a LGPD é silente neste tópico: “uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação

---

[67] BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações.** São Paulo: Atlas, 2005. p. 1.

[68] HANSEN, Marit. Kommentar Art. 32 DSGV. In: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER, Indra (org.). **Datenschutzrecht: DSGVO mit BDSG.** Nomos: Baden-Baden, 2019. p. 824.

[69] SMEDINGHOFF, Thomas J. ***Information Security Law: The Emerging Standard for Corporate Compliance. Cambridgeshire**:* ITGP, 2008. p. 15-16.

[70] PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence; MARGULIES, Jonathan. **Security in computing.** 5. ed. Boston: Prentice Hall, 2015. p. XXV e XXVI.

[71] GOBEO, Antoni; FOLWER, Connor; BUCHANAN, William J. ***GDPR and Cyber Security for Business Information Systems.*** Gistrup: River, 2018. versão Kindle, p. 2059.

ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento", não importando se foi doloso ou culposo.

A LGPD, contudo, conceitua no art. 44 tratamento irregular como sendo aquele que deixa de observar a legislação ou quando não fornece a segurança que o titular pode esperar. Caso o controlador ou operador, 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, segundo o art. 42[72].

Ainda, em seu art. 46, dispõe que 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.

Por sua vez, o vazamento de dados ocorre quando dados são acessados, coletados e repassados ou divulgados a terceiros ou na internet, sem a permissão de seus titulares ou de quem os controla.

O vazamento de dados pode ocorrer de diversas formas: através do furto de dados por quem explora vulnerabilidades em sistemas; ataques cibernéticos, sequestro de contas de usuários, cujas senhas são fracas ou foram vazadas; repasse de dados por funcionários ou ex-funcionários que copiaram informações da empresa;

---

[72] 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.
§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:
I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

furto de equipamentos; erros ou negligência humana, como ao se desfazer de *pen drives* contendendo dados despreocupadamente[73].

Dados são valiosos e possuem os atributos mencionados acima que merecem ser protegidos, por isso, o acesso a esses por agentes mal intencionados pode gerar muitos riscos aos seus detentores, além de criar um cenário de desconfiança. As informações obtidas em vazamentos podem ser o nome, CPF, endereço residencial e profissional, celular, dados financeiros e de contato, senhas, credenciais de acesso, registros de saúde e dados de terceiros.

A partir desses elementos, é possível realizar exposição da pessoa e terceiros relacionados, abertura de contas bancárias para contratar cartões de crédito e contrair empréstimos, envio de e-mails, ligações e mensagens, assinaturas em sites e outros. Assim, pode ocorrer o furto de identidade, acesso indesejado a contas e até tentativas de extorsão, quando há chantagem para que informações não sejam repassadas ou disponibilizadas *online*.

É preciso, portanto, pensar em soluções que diminuam os riscos e conscientizem as pessoas e empresas dos perigos de terem os dados vazados, para que essas sejam mais diligentes em relação aos mecanismos de proteção, que são tratados em seção especial.

2.2 Violação de dados e incidentes de segurança: exemplos de vazamento de dados no Brasil e no exterior

A tendência é que o número de incidentes cresça, com o uso crescente de tecnologias para cada atividade humana e com o uso de dados para a melhoria desses.

A pesquisa anual da IBM em parceria com o Instituto Ponemon de 2019, *Cost of a Data Breach* (o custo de violação de dados, tradução livre) avaliou mais de 500

[73] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT). **Vazamento de Dados - Cartilha de Segurança na Internet,** 2021. p. 2. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf.

empresas de 16 regiões e países, sendo 35 delas no Brasil[74]. Nesta, o Brasil ficou em quarto em termos de volume de informações vazadas, em 2018 era o quinto lugar.

Os prejuízos causados pelo vazamento de dados são muitos, passando por multas e obrigações de adequação de sistemas de segurança, perda de credibilidade e de clientes. Este último é menos sentido no Brasil, onde a concorrência entre fornecedores não é tão volumosa.

O estudo concluiu que a perda de negócios, que chega a 36,2% dos casos, é o que mais gera prejuízo quando ocorre vazamento de dados, seguido por detecção do problema em si (31,1%), reparo de eventuais problemas (27,3%) e notificações de quem teve sua informação disseminada (5,4%).

Além dessa, lançado em 2019, a Dell Technologies realizou, pela consultoria da Vanson Bourne, o *Global Data Protection Index* (pesquisa global de proteção de dados, tradução livre)[75]. Foram vistas empresas com mais de 250 funcionários, de médio e grande porte, de 18 países, incluindo o Brasil. Os dados revelam que 16% sofreram vazamento de dados e 45% alegaram possuir dificuldade em formular medidas de proteção de dados. O percentual de empresas que sofreram perda de dados é maior no Brasil: 35%.

Os resultados também foram no sentido de que a maioria das empresas brasileiras não acredita que suas soluções de governança sejam capazes de enfrentar todos os riscos no futuro e 56% são inseguras quanto à possibilidade de preencher os requisitos de nível para recuperar os sistemas de dados.

O *Massachusetts Institute of Technology* (MIT, em inglês) realizou uma pesquisa que aponta que a quantidade de informações vazadas no Brasil aumentou 493% de 2018 para 2019[76], sendo que mais de 205 milhões de dados pessoais

---

[74] HERNANDEZ, Raphael. No Brasil, empresa que falha ao proteger dados tem perdas menores. **Folha de São Paulo.** São Paulo, 19 jul 2019. Disponível em: https://www1.folha.uol.com.br/tec/2019/07/no-brasil-empresa-que-falha-ao-proteger-dados-tem-perdas-menores.shtml. Acesso em 12 nov 2021.

[75] DATA PRIVACY BRASIL. **Pesquisas revelam informações sobre proteção de dados no Brasil e no Mundo,** 2019. Disponível em: https://dataprivacy.com.br/pesquisas-revelam-informacoes-sobre-protecao-de-dados-no-brasil-e-no-mundo/. Acesso em 12 nov 2021.

[76] FOTIOS, Ricardo. Vazamento de dados aumentaram 493% no Brasil, mostra pesquisa do MIT, **UOL**, 2021. Disponível em: https://cultura.uol.com.br/noticias/colunas/ricardofotios/35_vazamentos-de-dados-aumentaram-493-no-brasil-mostra-pesquisa-do-mit.html. Acesso em 12 nov 2021.

vazaram de forma criminosa[77]. Enquanto em 2018, ocorreram 3 eventos alarmantes, em 2019 foram 16.

Um aspecto preocupante é conhecido como tempo de exposição. Segundo o estudo do MIT, a média de dias entre a data de ocorrência do vazamento e a data em que a empresa percebe que houve falha na segurança é em torno de 250 dias.

Nesse cenário, casos de mega vazamentos têm sido recorrentes no Brasil. Em 2021, foram dois: um em janeiro e outro em março. No primeiro, foram vazados 223 milhões de CPFs e dados como identidades, salários, fotos, datas de nascimento, dados do imposto de renda, *score* no banco, de pessoas vivas ou falecidas. A denúncia foi feita pela empresa de segurança da informação Psafe, ao monitorar negociações de dados sigilosos na *deep web*[78]. No segundo, com mesmo número de pessoas de dados vazados, incluía nome, data de nascimento, endereço, sexo, CPF, celular e e-mail[79]. Esta base foi colocada à venda por 0,3 bitcoin (cerca de R$96.920,00), na *deepweb*, parte da internet não indexada pelos buscadores comuns, sendo oculta para a maioria do público.

Os controladores desses dados ainda não foram identificados, mas os casos são investigados pela Polícia Federal e Autoridade Nacional de Proteção de Dados. Neste momento, é importante que essas instituições nacionais se concentrem na delimitação de se foi um ataque deliberado de hackers ou se o vazamento resultou de falhas de segurança dos controladores desses dados[80].

---

[77] NETO, Nelson Novaes; MADNICK, Stuart; PAULA, Anchises Moraes G. De; BORGES, Natasha Malara. ***D****eveloping a Global Data Breach Database and the Challenges Encountered,* **Association for Computing Machinery,** Nova York, 2021. Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873. Acesso em 12 nov 2021.

[78] CORACCINI, Raphael. Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros. **CNN Brasil**, São Paulo, 27/01/2021. Disponível em: https://www.cnnbrasil.com.br/business/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros/. Acesso em 12 nov 2021.

[79] SOPRANA, Paula. Hacker oferta base com dados de 223 milhões de brasileiros atribuída ao Poupatempo. **Folha de São Paulo**, São Paulo, 2021. Disponível em: https://www1.folha.uol.com.br/mercado/2021/03/hacker-oferta-base-com-dados-de-223-milhoes-brasileiros-atribuida-ao-poupatempo.shtml?origin=folha. Acesso em 12 nov 2021.

[80] POLIDO, Fabrício Bertini Pasquot. O que o recente vazamento em massa de dados pessoais revela para o Brasil?, **Jota**, 04/02/2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-que-o-recente-vazamento-em-massa-de-dados-pessoais-revela-para-o-brasil-04022021. Acesso em 15 nov 2021.

A crescente ocorrência desses vazamentos facilita fraudes bancárias a partir das informações pessoais, seja com o CPF ou com o número de celular e e-mail para envio de boletos fictícios, quando não há compra vinculada ao documento.

Além desses, houve também em 2021 o vazamento de 21 mil dados de funcionários da Claro e NET, concessionária de telefonia, banda larga e TV por assinatura[81]. Os técnicos e terceirizados tiveram suas informações disponibilizadas publicamente, pelo servidor mal concebido que as armazenava, contendo dados de identificação, carteira de habilitação, endereço residencial, empresa terceirizada e contratos assinados pelos funcionários. O fechamento desse servidor da Claro foi feito 6 dias depois do recebimento da denúncia por esta.

Em 2018, mais de 19 mil clientes do Banco Inter, primeiro banco digital brasileiro, tiveram seus dados pessoais vazados, sendo a maioria deles o CPF, nome, dados bancários, registros de transações, contratos, número da conta, senhas, telefone e endereço. O Ministério Público do Distrito Federal ajuizou ação civil pública para investigar o incidente, que só foi admitido pelo banco em agosto. No comunicado, os correntistas foram informados que a exposição dos dados tinha sido de "baixo impacto" e que os clientes mais afetados seriam notificados[82].

Segundo a instituição, a pessoa autorizada a atuar em seus sistemas, isto é, a realizar os tratamentos, configurando-se em operador (art. 39, LGPD), teria feito diversos ataques a base de dados do banco e capturado as informações, para extorquir a empresa. Esta, contudo, se negou a pagar e o invasor divulgou os dados na internet[83]. No acordo homologado com o Ministério Público foi acordada multa no valor de R$1,5 milhões de reais, sendo 1 milhão de reais destinado a compra de

---

[81] DEMARTINI, Felipe. Falha em servidor expôs dados de 21 mil funcionários da Claro e Net. **Canal Tech,** 21/08/2021. Disponível em: https://canaltech.com.br/seguranca/falha-em-servidor-expos-dados-de-21-mil-funcionarios-da-claro-e-net-194418/. Acesso em 12 nov 2021.

[82] **VEJA, Redação Economia,** Banco Inter vai pagar R$ 1,5 milhão por vazamento de dados de clientes 19/08/2021. Disponível em: https://veja.abril.com.br/economia/banco-inter-vai-pagar-r-15-milhao-por-vazamento-de-dados-de-clientes/. Acesso em 12 nov 2021.

[83] **UOL**, Banco Inter confirma vazamento e culpa "pessoa autorizada", São Paulo, 17/08/2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/08/17/banco-inter-confirma-vazamento-de-dados-apos-ataque-hacker.htm. Acesso em 12 nov 2021

equipamentos e softwares a instituições públicas voltadas ao combate de crimes cibernéticos e o restante a instituições de caridade, indicados pelo MPDF[84]

Como se percebe, são muitas as situações que geram vazamentos de dados, desde vulnerabilidades a ações de agentes internos, que evidenciam a demanda por uma infraestrutura de segurança da informação e uso permanente de recursos de investigação, prevenção e repressão contra esses acessos.

No entanto, esses incidentes não são exclusivos do cenário brasileiro. Em 2017, a Equifax, uma instituição de crédito norte-americana, teve documentos privados de mais de 147 milhões de clientes vazados, de diversos países. Os invasores identificaram falhas de segurança no sistema da empresa, inclusive nos processos de encriptação, e coletaram as informações durante meses[85]. A empresa assinou um acordo global com a agência norte-americana responsável pelo caso (*Federal Trade Commission),* o *Consumer Financial Protection Bureau* e 50 estados e territórios dos EUA de US$ 425 milhões para ajudar as pessoas afetadas pela violação de dados.

Na Índia, em 2018, ocorreu vazamento da base de dados biométricos de mais de um bilhão de cidadãos, a maior do mundo, que ficou à venda online. O Aadhaar é uma ferramenta criada para facilitar o envio de dinheiro de programas estatais aos cidadãos, formado por um número de identificação único de 12 dígitos, para os residentes, que chega a 89% da população[86]. A falha veio de um sistema operado por uma empresa estatal, que permitiu o acesso a nomes, números de identidade, dados

---

[84] SANTINO, Rafael. Banco Inter pagará R$ 1,5 milhão por vazar dados de quase 20 mil pessoas, **Olhar Digital**, 2018. Disponível em: https://olhardigital.com.br/2018/12/19/seguranca/banco-inter-pagara-r-1-5-milhao-por-vazar-dados-de-quase-20-mil-pessoas/. Acesso em 12 nov 2021.

[85] FRUHLINGER, Fred. Equifax data breach FAQ: What happened, who was affected, what was the impact?, **CSO Online**, Estados Unidos, 2020. Disponível em: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html. Acesso em 12 nov 2021.

[86] JAIN, Mardav. **The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment**, University of Washington, 2019. Disponível em: https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/#_ftnref4. Acesso em 15 nov 2021

bancários, fotografias, impressões digitais, varreduras de retina e outros detalhes de identificação de quase todos os cidadãos indianos[87].

Em 2021, foi descoberto que um banco de dados do governo da Argentina contendo informações do cartão de identidade nacional foi encontrado à venda na *deep web*, o que inclui nome completo, fotos, endereço domiciliar e demais informações pessoais. O RENAPER (*Registro Nacional de las Personas*) teria sido invadido por um hacker ou disponibilizado por um grupo de funcionários do governo, o que tem sido investigado[88].

Como se vê, vazamentos de dados não acontecem apenas no Brasil, sendo um fenômeno mundial que vulnerabiliza tanto quem trata os dados quanto os titulares. Uma das maiores dificuldades é descobrir se os dados foram acessados por fontes internas, externas ou por erros e falhas de segurança. Por isso, é importante o debate sobre os mecanismos de segurança, comos se vê abaixo.

3. Mitigação de Riscos e Boas Práticas de Governança na LGPD

3.1 Implementação de mecanismos de governança de dados pessoais

A governança de dados advém da governança corporativa e constitui-se em princípios e regras de organização e controle sobre as informações que circulam pelas entidades. Engloba a melhoria nos processos e nos dados utilizados, pela institucionalização de padrões éticos e regras de *compliance.* Seu escopo está em constante transformação, pois as tecnologias permitem que novos meios sejam usados em prol da proteção de dados[89].

---

[87] HK, Varun. “Aadhaar: A History of the Controversy.” **Deccan Herald**, 2018. Disponível em: https://www.deccanherald.com/national/aadhaar-act-verdict-history-693614.html. Acesso em 15 nov 2021.

[88] IKEDA, Scott. Argentinian Government Database Containing ID Card Information of Entire Country Made Available on Dark Web Forum, **CPO Magazine**, 2021. Disponível em: https://www.cpomagazine.com/cyber-security/argentinian-government-database-containing-id-card-information-of-entire-country-made-available-on-dark-web-forum/. Acesso em 17 nov 2021.

[89] BARBIERI, Carlos. **Governança de Dados: Práticas, Conceitos e Novos Caminhos**, Rio de Janeiro, Alta Books. 2020.

A necessidade de implementação de mecanismos de governança de dados pessoais é incontestável. Como se tem demonstrado, os bens jurídicos atrelados aos dados pessoais são muitos e de extremo valor para cada indivíduo e para a proteção da sociedade como um todo. Este mesmo motivo pode influenciar agentes mal intencionados a invadirem sistemas informacionais alheios para roubar e vazar informações.

Nesse sentido, toda organização ou pessoa que gere dados pessoais deve adotar medidas de segurança da informação técnicas e administrativas[90], inclusive para agir em conformidade com a lei. A maioria das providências a seguir podem ser tomadas tanto em ambientes corporativos quanto na vida pessoal de cada um.

Medidas administrativas são as que visam, principalmente, a instituição como um todo, pois corroboram para o estímulo de atuações conformes com a LGPD e para a segurança da informação institucional. O *Recital* 78 da GPDR[91], o qual faz parte do conjunto de textos que adicionam informações para explicitar o sentido dos artigos, coloca como exemplos dessas medidas a adoção de orientações internas que respeitem a proteção de dados e medidas que incluam o uso minimizado ou pseudoanonimizado dos dados. Na prática, pode-se atribuir acesso a certos dados somente aos profissionais que efetivamente os usem para suas tarefas, ou seja, que esses dados não possam ser acessados por todos.

Por sua vez, as medidas técnicas são as informacionais, como uso de *firewalls* (regras de segurança que aprovam apenas os dados em conformidade com as regras e que analisa o tráfego de rede para determinar as operações de transmissão ou recepção de dados a serem executadas), *antimalware* (proteção contra vírus que é capaz de deletar informações e arquivos infectados), antivírus, *tokens* (palavras-chave ou identificadores), criptografia e outros[92].

O já mencionado art. 46 da LGPD coloca como dever dos agentes de tratamento a adoção das medidas técnicas e administrativas, já que esses corroboram

---

[90] SMEDINGHOFF, Thomas J. Information Security Law: ***The Emerging Standard for Corporate Compliance. Cambridgeshire*****:** ITGP, 2008. p. 20-21.
[91] União Europeia. **Regulamento Geral de Proteção de Dados Pessoais, Considerando 78.** Disponível em: https://gdpr-text.com/pt/read/recital-78/. Acesso em 10 nov 2021.
[92] "SMEDINGHOFF, Thomas J. Ibid. p. 21.

para a proteção de acessos não autorizados e em situações de perda, alteração ou demais tratamentos inadequados ou ilícitos. O seu §2º determina que essas medidas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Além disso, o art. 47 determina que qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término, junto com os agentes de tratamento. Como se percebe, todas essas pessoas devem se atentar não somente aos dados e como protegê-los tecnicamente, mas também ao objetivo de estabelecer uma cultura organizacional que pratique a segurança da informação diariamente, com treinamentos e políticas de segurança, por exemplo.

O art. 50 da LGPD possibilita aos controladores e operadores adotarem boas práticas de segurança a partir de um “programa de governança em privacidade” (art. 50, § 2.º, I). Para isso, devem considerar ao tratamento, a natureza, escopo, finalidade e probabilidade e gravidade dos riscos e benefícios desse tratamento (art. 50, § 1º), além da escala e volume das operações e sensibilidade dos dados tratados e gravidade dos anos aos titulares, em observância aos princípios da transparência e segurança da lei (art. 50, § 2º). Isso demonstra o comprometimento com normas de boas práticas relativas à proteção de dados pessoais (art. 50 § 2º, I, a) e deve ser aplicado a todo o conjunto de dados pessoais que estejam sob seu controle (art. 50 § 2º, I, b).

Na política, devem existir salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade (art. 50 § 2º, I, d), integrado a sua estrutura geral de governança e com mecanismos de supervisão internos e externo (art. 50 § 2º, I, f), além de contar com planos de resposta a incidentes (art. 50 § 2º, I, g). Sua atualização constante com informações obtidas a partir de monitoramento contínuo e avaliações periódicas é prevista na lei (art. 50 § 2º, I, h), junto com o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do mesmo (art. 50 § 2º, I, e).

Seguir essas disposições ao formular o programa é relevante, pois a autoridade nacional ou outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta pode requisitar sua demonstração (art. 50 § 2º, II).

Em outubro de 2021, a Autoridade Nacional de Proteção de Dados lançou um Guia Orientativo sobre Segurança de Informação para Agentes de Tratamento de Pequeno Porte[93]. O texto reconhece que a implementação e a manutenção de medidas que atendam às obrigações podem gerar, em algumas situações, um elevado investimento, com potencial de onerar excessivamente os agentes de tratamento de pequeno porte. Por isso, exemplifica medidas de segurança da informação e de boas práticas capazes de promover um ambiente institucional mais seguro. Esta atuação confirma o dever da Autoridade de estabelecer parâmetros de segurança (art. 46, § 1º e art. 51). Há que se comentar, também, que as medidas a seguir expostas podem ser adotadas em empresas de grandes portes.

Dentre as medidas administrativas, sugere-se adotar uma Política de Segurança da Informação - PSI[94], a qual consiste em um conjunto de diretrizes e regras que possibilitam o planejamento, a implementação e o controle de ações relacionadas à segurança da informação, que deve ser periodicamente revisada. Algumas ferramentas são cópias de segurança, atualização de softwares e uso de antivírus. Apesar de não ser obrigatória, sua adoção demonstra a diligência da instituição.

É importante formalizar ou contratar treinamentos sobre segurança da informação e campanhas de conscientização sobre as obrigações relacionadas ao manuseio correto de dados pessoais. Algumas atitudes diárias também são recomendadas, como bloquear computadores quando se afastar das estações de trabalho, para impedir acessos não permitidos de terceiros, orientar funcionários a não clicarem em *links* desconhecidos ou *pop-ups* na internet e incentivar a notificação de de incidentes e vulnerabilidades detectadas[95].

---

[93] Autoridade Nacional de Proteção de Dados (ANPD). **Guia Orientativo: Segurança da Informação para Agentes de Tratamento de Pequeno Porte, Versão 01.** Brasília, DF, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em 5 nov 2021.
[94] Ibid, p. 8.
[95] Ibid, p. 9.

Recomenda-se haver uma gerência apurada dos contratos, com a adoção de cláusulas de confidencialidade em relação aos dados pessoais tratados, atenção aos contratos feitos com terceiros em relação à obediência à LGPD e inclusões de cláusulas sobre segurança da informação e regras de compartilhamento, principalmente se os serviços de TI forem terceirizados[96].

Tendo sido apresentadas algumas medidas administrativas que permeiam a governança de dados, passa-se a trazer exemplos das medidas técnicas.

Uma delas é estabelecer controles de acessos para que as informações estejam disponíveis apenas para pessoas autorizadas, instaurando um processo formado por autenticação (identificar quem acessa), autorização (determinar o que o usuário pode fazer) e auditoria (compilar o que foi feito), além da recomendação de senhas fortes, com caracteres diferentes[97]. A autenticação multi-fatores, isto é, com mais uma etapa no processo de acesso ao sistema, com envio de mensagens ou e-mails com códigos de segurança é uma solução eticamente desejada[98].

O art. 6º, III da LGPD traz o princípio da necessidade, para que somente os dados pessoais necessários sejam coletados. Por isso, o Guia ressalta a importância de haver uma revisão nos dados coletados e, se possível, pensar em alternativas que diminuam a coleta ou implementar a pseudonimização[99], principalmente de dados pessoais sensíveis, pela criptografia, por exemplo[100].

As cópias de segurança (*backups)* devem ser periódicas e armazenadas em locais seguros e distintos dos dispositivos de armazenamento principais. A possibilidade de se manter as cópias *online* não é recomendada, por haver o risco de infecção por códigos maliciosos sequestradores de dados (*ransomware*), que podem

---

[96] Ibid, p. 10.
[97] Ibid, p. 10.
[98] Ibid, p. 11.
[99] Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (art.13 § 4º da LGPD). Sobre o assunto, veja: COMISSÃO DE PROTEÇÃO DE DADOS PESSOAIS DE SINGAPURA. **Guide to Basic Data Anonymization Techniques – PDPC**. 25 jan 2018. COMISSÃO EUROPEIA. Opinion 05/2014 on Anonymization Techniques. Article 29 Data Protection Working Party – 0829/EN – WP216. Adotada em 10 abr 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em 5 nov 2021.
[100] Autoridade Nacional de Proteção de Dados, Ibid. p. 13.

acarretar em vazamento das informações[101], como aconteceu nos casos de vazamentos traduzidos no capítulo anterior.

Ao se colocar em prática essas e demais técnicas, é importante instaurar um programa de gerenciamento de vulnerabilidades, atento à existência de novas versões e correções. Isso, somado às boas práticas de tarefas diárias em prol da segurança de dados, fomenta um ambiente institucional mais seguro no que se refere ao tratamento de dados pessoais.

Essas medidas são essenciais para se estabelecer uma cultura de segurança da informação e prevenir crimes e negligências. Contudo, nota-se que, caso ocorra algum incidente, a LGPD estabelece passos a serem observados.

Ao identificar que houve vazamento de dados, seja pela veiculação na mídia ou recebimento de notificação, deve-se identificar quais dados vazaram e trocar senhas de acesso, ativar verificação em duas etapas quando possível, informar as instituições e contestar os eventuais transações, lançamentos ou modificações na conta que não sejam reconhecidas.

A LGPD coloca a mera possibilidade de haver risco ou dano relevante aos titulares obrigação do controlador de comunicar à autoridade nacional e ao titular o acontecimento (art. 48, *caput*). Este alerta deve ser feito em prazo razoável (art. 48, § 1º), contendendo: a descrição da natureza dos dados pessoais afetados (art. 48, § 1º, I), as informações sobre os titulares envolvidos (art. 48, § 1º, II), a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial (art. 48, § 1º, III), os riscos relacionados ao incidente (art. 48, § 1º, IV), os motivos da demora, no caso de a comunicação não ter sido imediata (art. 48, § 1º, V) e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (art. 48, § 1º, VI).

A implementação de práticas de governança e de políticas de segurança da informação são essenciais para a prevenção de danos, sendo, inclusive, critérios observados pela ANPD ao decidir as sanções a serem aplicadas (art. 52, § 1º, VIII e IX).

---

[101] Ibid, p. 14.

Assim como em outros incidentes, os critérios das sanções em casos de vazamento de dados deverão observar as peculiaridades do caso concreto, dispostos no art. 52, § 1º. Nesse sentido, cabe a análise de quais parâmetros mais se encaixam com o vazamento de dados.

A avaliação da gravidade e natureza das informações e do dano (incisos I e VI) é essencial para este incidente, pois a liberação indesejada de dados sensíveis pode ser o maior risco inerente a esses dados. A boa fé do infrator (inciso II) nesses casos pode ser avaliada se o vazamento ocorreu por erro interno ou invasão externa, já que, ao que parece, o legislador se referiu a boa fé subjetiva.

Uma vez que a LGPD não diferencia nem escalona a gravidade da falha interna da gravidade de uma ação de terceiro que burlou os sistemas da empresa para obter dados, é importante se atentar às futuras decisões da ANPD.

Conforme se tem demonstrado ao longo deste capítulo, a adoção de mecanismos e procedimentos internos capazes de minimizar o dano é imprescindível. O art. 52, § 1º, VIII coloca como critério e parâmetro essa implementação para a fixação das penalidades em processo administrativo próprio, já que ajudam a compreender o ambiente em que ocorreu o dano e podem funcionar como meios para realizar a "dosimetria" das sanções. Um agente de tratamento que possui regras e procedimentos de segurança não poderia ter a mesma penalidade que um que não as tivesse, por exemplo.

Assim, é importante que a Autoridade imponha sanções administrativas de acordo com o nível do prejuízo sentido (art. 52) e das medidas técnicas e administrativas adotadas pelas organizações para prevenir incidentes e proteger os dados. As sanções relacionadas ao vazamento de dados podem ser uma advertência (art. 52, I) e até mesmo uma multa limitada a R$ 50 milhões por infração (art. 52, II), multa diária (art. 52, III), e publicização da infração (art. 52, IV).

Portanto, os mecanismos de boas práticas e governança têm como objetivo buscar o cumprimento da lei, através de medidas técnicas e administrativas. Sabe-se que a eliminação completa de falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas medidas minimizam as chances de haver desvios de

comportamento e criar respostas para identificação os incidentes, forma eficaz, rápida e adequada[102].

3.2 Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED)

A LGPD, além de regular o tratamento de dados pessoais e estabelecer regras e sanções, serve para fomentar a ideia de que o controlador e o operador de dados são responsáveis pela segurança informacional, em um padrão de *accountability* normativo encontrado mundo a fora. Nesse sentido, a lei atribuiu aos agentes de tratamento o dever de pôr em prática meios eficientes para que comprovem a obediência às regras e princípios da proteção de dados[103], como demonstrado acima.

Além de seguir as disposições na LGPD e as normas que serão criadas pela Autoridade Nacional, é recomendado que os próprios agentes e pessoas envoltas ao tratamento de dados formulem e sigam ditames que minimizem riscos e estipulem controles em caso de situações de vulnerabilidade, desde a fase de concepção até a execução do produto ou serviço.

A Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED) é um dos fatores principais para estabelecer uma cultura de gestão de dados sustentável, capaz de evitar ou mitigar riscos e de maximizar seus benefícios[104]. Isso porque esta estimula padrões de comportamento desejáveis previstos por conta da avaliação de impacto. A LGPD não informa detalhes sobre esta avaliação, mas a expectativa é de que nela sejam descritas as operações de tratamento, suas justificativas, previsão de possíveis riscos e medidas pensadas para diminuir esses, fluxos de informações, identificação de riscos e de soluções, além dos padrões de segurança já adotados, pois esses são fatores presentes no Regulamento Europeu.

---

[102] DE CARVALHO, Vinicius Marques; MATTIUZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais.** 1. ed. Rio de Janeiro: Forense, 2021, p. 1168 (iBooks)

[103]WIMMER, Miriam. Os desafios do Enformecent na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: **Tratado de proteção de dados pessoais. Coordenadores** DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021

[104] BELLI, Luca. Como Implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). In: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.399.

A ideia de avaliar e estudar possíveis impactos de uma ação não foi trazida pela LGPD, existindo no ordenamento jurídico brasileiro há algumas décadas. A Constituição Federal, a partir do art. 5.º, LXXIII c/c 225, § 1.º, IV, coloca como prerrogativa do Poder Público a exigência de um Estudo do Impacto Ambiental (EIA) prévio, em caso de instalação de obra ou atividade potencialmente causadora de significativa degradação ambiental, a fim de se proteger o direito fundamental a um meio ambiente sadio.

O mesmo ocorre na LGPD, quando esta prevê a possibilidade de se instaurar uma avaliação de riscos aos dados dos titulares, cuja definição está em seu art. 5º, XVII: “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

No contexto europeu, contudo, a formulação desse documento é obrigatória, pela leitura do art. 35 do GDPR. Sempre que uma organização decide iniciar o processamento de dados do usuário que “for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" é necessário uma AIPD/RIPD (Avaliação ou Relatório de Impacto sobre Proteção de Dados), para avaliar os níveis de risco para titular de dados para cada tratamento.

As situações nas quais o RIPD é estritamente necessário, para o GDPR, são (art. 35, 3. *a, b* e *c*): quando há avaliação sistemática de pessoas que induzam a adoção de decisões cujos efeitos são jurídicos (formação de perfis); uso em grande escala de dados sensíveis ou outros em situações especiais (como dados de crianças) e há controle ordenado de espaços largamente acessados pelo público (como usar reconhecimento facial por finalidade de segurança pública).

A formulação dessa análise, caso feita pelo controlador, corrobora para o entendimento de que este segue o princípio da responsabilização e prestação de contas da LGPD (art. 6º, X), pois demonstra seu empenho em melhorar seus mecanismos de segurança, além de marcar a concepção da proteção de dados desde a concepção, previstos nos princípios de segurança (art. 6º, VII) e na ideia de privacy by design. Ao se pensar nos riscos, é necessário ter uma visão extensiva desses para

além dos titulares de dados tratados na situação, incluindo as desvantagens a virem a ser sofridas pela sociedade no geral[105].

Como já dito, a Avaliação não é obrigatória no Brasil de acordo com a LGPD, mas pode vir a ser por determinação da Autoridade Nacional, nos termos do art. 38 c/c 55-J, XIII, pois compete a ela editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais. Além disso, pela leitura do art. 4º, a ANPD possui a dupla função de emitir opiniões técnicas ou recomendações e solicitar relatórios de impacto à proteção de dados pessoais aos responsáveis. Em relação às recomendações, o Guia lançado por ela sobre mecanismos técnicos e administrativos abordado no capítulo anterior demonstra a atuação da Autoridade nesse sentido

O Relatório de Impacto pode intensificar a procura por ferramentas de proteção, principalmente quando se verificar o tratamento de dados sensíveis. Dessa forma, pensando em um cenário em que se prevê extensamente os malefícios de se ter os dados vazados, é possível que sejam elaborados mecanismos preventivos importantes a partir da análise desses relatórios.

CONCLUSÃO

A proteção da privacidade é essencial para o desenvolvimento humano e da sociedade como um todo. É um direito fundamental que tem ganhado novas interpretações e sido cada vez mais o foco de discussões interdisciplinares, por conta dos novos avanços tecnológicos. O que antes foi por muitos anos o direito de ser deixado só, hoje evoluiu para possuir diversas ramificações, incluindo o da proteção de dados pessoais.

Nesse cenário, foi imperativo o surgimento de leis de proteção de dados que protegessem o cidadão e limitassem a ingerência de entidades públicas e privadas em relação aos dados coletados e aos diversos tratamentos feitos a partir desses. Isso porque é comum que haja uma coleta incessante de dados e que o cruzamento

[105] Op Cit, p. 1263 (iBooks).

desses crie perfis que apontam para preferências, ainda que os titulares não percebam, justamente pelo valor social, econômico e cultural que os dados possuem atualmente.

Nesse sentido, foram apresentadas alguns diplomas legais que versam sobre privacidade e proteção de dados, em notoriedade o regramento europeu - GDPR - que serviu de base para a lei brasileira de proteção de dados brasileira, aprovada em 2018. A LGPD estabeleceu um amparo legal para o tratamento de dados pessoais necessário para que o Brasil estivesse entre os países que possuem lei específica sobre o tema, trazendo direitos aos titulares dos dados e consequentemente obrigações às entidades que os coletam e tratam.

Dentre as normas na lei, ressalta-se a importância daquelas atinentes aos incidentes de segurança, no que tange os direitos dos titulares, os procedimentos adequados, como preveni-los e possíveis punições. A LGPD reforça que os dados devem ser tratados prezando pela sua integridade, confidencialidade e disponibilidade. Contudo, todos esses elementos são minados em casos de vazamento de dados, que têm sido comuns em todo o globo.

Os vazamentos de dados representam um risco, ao que indica a realidade, intrínseco a todo controlador e operador e, consequentemente, à toda sociedade. Não é possível se ter controle do que é feito com as informações confidenciais que são disponibilizadas por conta desse incidente, o que por si só é um fator preocupante e que deve ensejar o máximo de esforços possíveis para que a segurança da informação e mecanismos de governança sejam aplicados desde a concepção do serviço ou produto.

Dada à significância que esse incidente possui, até mesmo instituições solidificadas no mercado, como bancos e sistemas governamentais, são atravessados pelos desafios de vazamentos de dados. A segurança, solidez e credibilidade são questionadas nesses casos.

Por isso, é importante que, para que a LPGD seja efetivamente implementada nas organizações, uma nova cultura em torno da proteção de dados pessoais seja incentivada, ao mesmo tempo em que esteja aberta a acolher as inovações

tecnológicas, os novos padrões éticos e medidas técnicas e administrativas de segurança, inclusive para balizar as Avaliações de Impacto sobre Privacidade e Ética de Dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ARISTÓTELES. **Política**. Rio de Janeiro: Ediouro, 1988,

Autoridade Nacional de Proteção de Dados (ANPD). **Guia Orientativo: Segurança da Informação para Agentes de Tratamento de Pequeno Porte**, Versão 01. Brasília, DF, out. 2021.

BARBIERI, Carlos. **Governança de Dados: Práticas, Conceitos e Novos Caminhos**, Rio de Janeiro, Alta Books. 2020.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações.** São Paulo: Atlas, 2005.

BELLI, Luca. Como Implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). In: **Tratado de proteção de dados pessoais.** Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019. p. 133.

BRASIL, Brasil está entre os cinco países do mundo que mais usam internet, **Governo do Brasil,** 26/04/2021. Disponível em: https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/04/brasil-esta-entre-os-cinco-paises-do-mundo-que-mais-usam-internet#:~:text=Com%2078%2C3%25%20de%20brasileiros,fibras%20%C3%B3Pticas%20%C3%A0s%20redes%20nacionais.

BRASIL, Senado Federal aprova Proposta de Emenda à Constituição 17 (PEC 17/2019) que inclui a proteção de dados pessoais no rol de direitos e garantias fundamentais. **Agência senado.** Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais>. Acesso em 5 nov 2021.

BRASIL. **Decreto regulamentador da Lei do Cadastro Positivo.** Decreto nº 9.936, de 24 de julho de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9936.htm >. Acesso em: 05 nov 2021.

BRASIL. **Lei Complementar nº 166, de 8 de abril de 2019.** Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp166.HTM>. Acesso em: 05 nov 2021

BRASIL, **Ministério da Justiça e Segurança Pública,** Governo Federal. Sobre a Lei de Acesso à Informação - LAI. Disponível em: https://www.justica.gov.br/Acesso. Acesso em nov 2021.

BRASIL. **Lei no 12.965 de 23 de abril de 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/lei/l12965.htm. Acesso em: 10 de novembro de 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: 11 de novembro de 2021.

BRASIL. **Lei no 8.078 de 11 de setembro de 1990**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 06 de novembro de 2021.

BRASIL. **Proposta de Emenda à Constituição n. 17, de 2019.** Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1571776978885&disposition=inline>. Acesso em: 05 de novembro de 2021.

Bruno Ricardo. **Tratado de proteção de dados pessoais.** 1. ed. Rio de Janeiro: Forense, 2021.

CALLEJÓN, FRANCISCO BALAGUER. **A Carta dos Direitos Fundamentais da União Europeia.** Direito Público, [S.l.], v. 8, n. 35, abr. 2012. ISSN 2236-1766. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/1822/1005>. Acesso em: 10 dez. 2021.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura. Vol 1. A sociedade em rede.** Trad: Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. **A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade.** Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT). **Vazamento de Dados - Cartilha de Segurança na Internet,** 2021. p. 2. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf.

COMISSÃO EUROPEIA. **Opinion 05/2014 on Anonymization Techniques**. Article 29 Data Protection Working Party – 0829/EN – WP216, 2014.

CONSELHO DA EUROPA. **Manual da Legislação Europeia sobre Proteção de Dados.** Luxemburgo, 2014.

COOLEY, Thomas McIntyre. **A treatise on the law of torts**. Chicago: Callaghan, 1880.

CORACCINI, Raphael. Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros. **CNN Brasil,** São Paulo, 27/01/2021. Disponível em: https://www.cnnbrasil.com.br/business/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros/

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do STJ. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

DATA PRIVACY BRASIL. **Pesquisas revelam informações sobre proteção de dados no Brasil e no Mundo,** 2019. Disponível em: Disponível em: https://dataprivacy.com.br/pesquisas-revelam-informacoes-sobre-protecao-de-dados-no-brasil-e-no-mundo/.

DE CARVALHO, Vinicius Marques; MATTIUZO, Marcela; PONCE, Paula Pedigoni. **Boas práticas e governança na LGPD**. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI,

DEMARTINI, Felipe. Falha em servidor expôs dados de 21 mil funcionários da Claro e Net. **Canal Tech**, 21/08/2021. Disponível em: Disponível em: https://canaltech.com.br/seguranca/falha-em-servidor-expos-dados-de-21-mil-funcionarios-da-claro-e-net-194418/.

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

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais.** In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. Tratado de proteção de dados pessoais. 1. ed. Rio de Janeiro: Forense, 2021

FOTIOS, Ricardo. Vazamento de dados aumentaram 493% no Brasil, mostra pesquisa do MIT, **UOL**, 2021. Disponível em: https://cultura.uol.com.br/noticias/colunas/ricardofotios/35_vazamentos-de-dados-aumentaram-493-no-brasil-mostra-pesquisa-do-mit.html.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

FRUHLINGER, Fred. Equifax data breach FAQ: What happened, who was affected, what was the impact?, **CSO Online**, Estados Unidos, 2020. Disponível em: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

GAVISON, Ruth. Privacy and the limits of law. **The Yale Law Journal,** v. 89, nº 3, 1980.

GOBEO, Antoni; FOLWER, Connor; BUCHANAN, William J. **GDPR and Cyber Security for Business Information Systems.** Gistrup: River, 2018.

HAND, Augustus N. Schuyler against Curtis and the Right to Privacy. **The American Law Register and Review,** Philadelphia, vol. 45, n. 12, 1897.

HANSEN, Marit. Kommentar Art. 32 DSGV. In: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER, Indra (org.). **Datenschutzrecht: DSGVO mit BDSG. Nomos: Baden-Baden**, 2019.

HERNANDEZ, Raphael. No Brasil, empresa que falha ao proteger dados tem perdas menores. **Folha de São Paulo.** São Paulo, 19 jul 2019.

HIRATA, Alessandro. **Direito à privacidade.** Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

HK, Varun. "**Aadhaar: A History of the Controversy**." Deccan Herald, 2018. Disponível em: https://www.deccanherald.com/national/aadhaar-act-verdict-history-693614.html.

IKEDA, Scott. Argentinian Government Database Containing ID Card Information of Entire Country Made Available on Dark Web Forum, **CPO Magazine**, 2021.

IRAMINA, Aline. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 12, no 2.

JAIN, Mardav. The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment, **University of Washington,** 2019. Disponível em: https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/#_ftnref4.

KRIEGER, Maria Victoria Antunes. A análise do instituto do consentimento frente à Lei Geral de Proteção de Dados do Brasil (lei nº 13.709/18). Trabalho de Conclusão de Curso (graduação) – **Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas**, 2019. Data da publicação: 05 dez. 2019.

MACIEJEWSKI, Mariusz. **Proteção de Dados pessoais.** Fichas Técnicas sobre a União Europeia - 2021.

MARTINS-COSTA, Judith; BRANCO, Gerson. **Diretrizes teóricas do novo Código Civil brasileiro.** São Paulo: Saraiva, 2002.

MAYER-SCHÖNBERGER, Generational Development of Data Protection in Europe. In: Technology and Privacy: The New Landscape. **The MIT Press**: Massachusetts, 2001.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, vol. 120, ano 27, São Paulo: Ed. RT, nov.-dez. 2018

MENKE, Fabiano; GOULART, G. D. Segurança da Informação e Vazamento de Dados. In: Bruno Et Al (coords.) Bioni. "**Tratado De Proteção De Dados Pessoais".** São Paulo: Editora Forense. 2020,

MIRANDA, Francisco Cavalcanti Pontes de. Tratado de direito privado. Campinas: Bookseller, 2000

MOORE, Adam. "Privacy: Its Meaning and Value". American Philosophical Quarterly, Vol. 40, 2003

NAVARRO, Ana Maria Neves de Paiva; LEONARDOS, Gabriela. Privacidade Informacional: Origem e Fundamentos no Direito Norte-Americano.

NETO, Nelson Novaes; MADNICK, Stuart; PAULA, Anchises Moraes G. De;

BORGES, Natasha Malara. Developing a Global Data Breach Database and the Challenges Encountered, Association for Computing Machinery, Nova York, 2021.

PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence; MARGULIES, Jonathan. Security in computing. 5. ed. Boston: Prentice Hall, 2015

POLIDO, Fabrício Bertini Pasquot. O que o recente vazamento em massa de dados pessoais revela para o Brasil?, Jota, 04/02/2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-que-o-recente-vazamento-em-massa-de-dados-pessoais-revela-para-o-brasil-04022021. Acesso em 15 nov 2021.

PROSSER, William. Privacy. California Law Review, Vol. 48, 1960

SANTINO, Rafael. Banco Inter pagará R$ 1,5 milhão por vazar dados de quase 20 mil pessoas, Olhar Digital, 2018. Disponível em: https://olhardigital.com.br/2018/12/19/seguranca/banco-inter-pagara-r-1-5-milhao-por-vazar-dados-de-quase-20-mil-pessoas/

SMEDINGHOFF, Thomas J. Information Security Law: The Emerging Standard for Corporate Compliance. Cambridgeshire: ITGP, 2008.
União Europeia. Regulamento Geral de Proteção de Dados Pessoais, Considerando 78.

SOPRANA, Paula. Hacker oferta base com dados de 223 milhões de brasileiros atribuída ao Poupatempo. Folha de São Paulo, São Paulo, 2021. Disponível em: https://www1.folha.uol.com.br/mercado/2021/03/hacker-oferta-base-com-dados-de-223-milhoes-brasileiros-atribuida-ao-poupatempo.shtml?origin=folha.

Tribunal de Justiça do Distrito Federal e dos Territórios - TJDFT. Marco Civil da Internet. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet.

UNIÃO EUROPEIA. **Directiva 95/46/CE** do Parlamento Europeu e do Conselho Europeu, de 24 de outubro de 1955. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT

UNIÃO EUROPEIA. **Opinion 05/2014 on Anonymization Techniques. Article 29 Data Protection Working Party – 0829/EN – WP216**. Adotada em 10 abr 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pd

UOL, Banco Inter confirma vazamento e culpa "pessoa autorizada", São Paulo, 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/08/17/banco-inter-confirma-vazamento-de-dados-apos-ataque-hacker.htm#:~:text=Banco%20Inter%20confirma%20vazamento%20de%20dados%20e%20culpa%20%22pessoa%20autorizada%22,-Banco%20diz%20que&text=O%20Banco%20Inter%2C%20primeiro%20a,clientes%20foram%20vazados%20na%20internet.

VEJA, Redação Economia, Banco Inter vai pagar R$ 1,5 milhão por vazamento de dados de clientes. Disponível em: https://veja.abril.com.br/economia/banco-inter-vai-pagar-r-15-milhao-por-vazamento-de-dados-de-clientes/

VIEIRA, Tatiana Malta. **O Direito à Privacidade na Sociedade da Informação: efetividade desse direito fundamental diante da tecnologia da informação**. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

WARREN, Samuel; BRANDEIS, Louis. “The Right to Privacy”. **Harvard Law Review**, Vol. IV, n.º 5, 1890.

WIMMER, Miriam. Os desafios do Enformecent na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: T**ratado de proteção de dados pessoais.** Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021.