FIB

Direito

João Pedro Ponce Lopes Calixto

VAZAMENTOS DE DADOS NA LGPD E BOAS PRÁTICAS DE GOVERNAÇA

Bauru
2022

João Pedro Ponce Lopes Calixto

VAZAMENTOS DE DADOS NA LGPD E BOAS PRÁTICAS DE GOVERNAÇA

Monografia apresentada às Faculdades Integradas de Bauru para obtenção do título de Bacharel em Direito, sob a orientação do Professora Ms. Márcia Regina Negrisoli

Bauru
2022

CALIXTO, João Pedro Ponce Lopes

Vazamentos de Dados na LGPD e Boas Práticas de Governança. João Pedro Ponce Lopes Calixto. Bauru, FIB, 2022.

46f.

Monografia, Bacharel em Direito. Faculdades Integradas de Bauru - Bauru

Orientador(a): Márcia Regina Negrisoli Fernandez Polenttini

1. privacidade; direito à privacidade; 2. proteção de dados pessoais; 3. dados pessoais; 4. incidentes de segurança; 5. vazamento de dados; 6. mecanismos de segurança; 7. Lei Geral de Proteção de Dados Pessoais (LGPD). I. Vazamentos de Dados na LGPD e Boas Práticas de Governança. Faculdades Integradas de Bauru.

CDD 340

João Pedro Ponce Lopes Calixto

VAZAMENTOS DE DADOS NA LGPD E BOAS PRÁTICAS DE GOVERNANÇA”

Monografia apresentada às Faculdades Integradas de Bauru para obtenção do título de Bacharel em Direito,

Bauru, 22 de novembro de 2022.

Banca Examinadora:

Presidente/ Orientador: Ms. Márcia Regina Negrisoli Fernandez Polenttini

Professor 1: Ms. César Augusto Micheli

Professor 2: Dra. Maria Cláudia Zaratini Maia

Bauru
2022

DEDICATÓRIA

Este trabalho é todo dedicado aos meus pais, pois é graças ao seu esforço que hoje posso concluir o meu curso;

A Deus, porque sem ele eu não teria capacidade para desenvolver este trabalho;

A minha orientadora, sem a qual não teria conseguido concluir esta difícil tarefa e a todo o curso de Direito das Faculdades Integradas de Bauru (FIB), corpo docente e discente, a quem fico lisonjeado por dele ter feito parte, dedico este trabalho a todos os que me ajudaram ao longo desta caminhada;

Dedico este trabalho aos meus colegas de curso, que assim como eu encerram uma difícil etapa da vida acadêmica;

A conclusão deste trabalho resume-se em dedicação, dedicação que vi ao longo dos anos em cada um dos professores deste curso, a quem dedico este trabalho.

AGRADECIMENTOS

Agradeço em primeiro lugar, a Deus, que fez com que meus objetivos fossem alcançados, durante todos os meus anos de estudos.

A esta Instituição de ensino, seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior, eivado pela acendrada confiança no mérito e ética aqui presentes.

A Professora Ms. Márcia Regina Negrisoli, pelo emprenho pela orientação, apoio e confiança dedicados à elaboração deste trabalho.

Agradeço a meu pai e minha mãe por sempre estarem presentes e me apoiarem no desenvolvimento do meu TCC, sem eles com certeza a tarefa teria sido muito mais árdua.

Agradeço a todos, minha família, parentes e amigos que com seu incentivo me fizeram chegar à conclusão do meu curso e começo de uma nova carreira.

A todos que direta ou indiretamente fizeram parte de minha formação, o meu muito obrigado

“Não basta que todos sejam iguais perante a lei. É preciso que a lei seja igual perante todos.”

Salvador Allende

CALIXTO, João Pedro. **Vazamentos de Dados na LGPD e as Boas Práticas da Governança.** 2022 46f. Monografia apresentada às Faculdades Integradas de Bauru, para obtenção do título de Bacharel em Direito. Bauru, 2022.

RESUMO

O presente trabalho versa 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 que se encontra vinculada 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).

PONCE LOPES CALIXTO, João Pedro. **Vazamentos de Dados na LGPD e As Boas Práticas da Governança.** 2022 46f. Monografia apresentada às Faculdades Integradas de Bauru, para obtenção do título de Bacharel em Direito. Bauru, 2022.

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

1 INTRODUÇÃO

A expressão “sociedade da informação” é uma das mais utilizadas para caracterizar o contexto técnico-econômico no século XXI, sendo a sucessora da “sociedade pós-industrial”, 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 a Hootsuite, 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 à internet, fazendo do Brasil o 5ª no ranking de países em população online. (WERTHEIN; 2000, p. 71)

A frase “Data is the new oil” (em português, “os dados são o novo petróleo”) de Clive Humby, marca a sociedade atual, na qual o bem com maior valor de troca e que gera mais riqueza deixou de ser o petróleo, para serem os dados, principalmente os pessoais. (NISTLER, 2020)

Os dados representam oportunidades para que negócios cresçam tendo a eficiência e inovação como características básicas 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 definida também pela Internet das Coisas (em inglês, 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 fazendo com que legislações 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 conceitos básicos atinentes à proteção de dados, a metodologia a ser empregada consistirá em revisão bibliográfica, bem como demonstração de situações fáticas.

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).

2 HISTÓRICO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A linha do tempo da LGPD revela as diversas mudanças que ocorreram desde que foi publicada em 2018.

Embora seja livremente inspirada no Regulamento Geral sobre a Proteção de Dados (ou GDPR (General Data Protection Regulation), a LGPD tornou-se mais complexa e adaptada ao cenário brasileiro com o decorrer dos anos, além de uma série de alterações de datas ao decorrer do tempo.

Embora o cenário atual favoreça a popularidade da LGPD, a história diz que ela já existe desde os anos 90, com a formalização do direito à privacidade.

É preciso reconhecer todas as evoluções desde então para compreender como a relação entre as pessoas e a tecnologia mudou, e com isso novas demandas tornaram-se necessárias.

2.1 Panorama Internacional

A Humanidade vem se desenvolvendo através dos séculos, desde a antiguidade até a atualidade os aperfeiçoamentos tecnológicos vêm levantando questões Macro e Micro territoriais influenciando e moldando as relações pessoais e comerciais entre os indivíduos.

Com o advento da informatização como meio mais célere e mais eficaz para o armazenamento de dados sensíveis às relações comerciais, surgiram também conflitos avindos da violação desses dados, os quais só eram protegidos moralmente por seus idealizadores e, fatalmente sofriam vazamentos por pessoas mal-intencionadas causando prejuízos irreparáveis.

Viu-se necessário então por parte dos países desenvolvidos a criação de uma política de proteção destes dados, o debate se expandiu, até que, em 2012, começa a ser idealizada a GDPR na Europa.

Em 2013, o ex-técnico da CIA, Edward Snowden, divulgou diversos esquemas de espionagem por parte dos EUA, relatando um uso mal intencionado de dados pessoais. (BESSA, 2014)

Em 2018, ocorreu o escândalo da empresa Cambridge Analytica, o qual deixou evidente a forma como os dados recolhidos através do Facebook era utilizada inapropriadamente, tais dados influenciaram desde as campanhas eleitorais estadunidenses de 2016, até a saída do Reino Unido da União Europeia (processo conhecido como Brexit). (KAISER, 2019).

Essa situação voltou a atenção internacional para a questão dos dados, já que se percebeu que seu tratamento pode vir a impactar vários países e até mesmo suas democracias.

Ainda no mesmo ano a GDPR entrou em vigor e passou a regular todo o tratamento de dados da União Europeia e influenciou outros países a criarem seu próprio regulamento, inclusive o Brasil, em sua LGPD.

Em razão da entrada em vigor da Lei europeia, da GDPR, e do escândalo da Cambridge Analytica, muitas empresas brasileiras precisaram se adequar para esta nova realidade, resultando no aumento da pressão pela aprovação da Lei Geral de Proteção de Dados (LGPD).

2.2 Contexto Brasileiro

As políticas públicas de proteção de dados pessoais no Brasil passaram a ter sua importância somente em 2010, ano em que ocorreu a primeira consulta pública sobre o tema.

Neste período surgiram algumas leis como a Lei de Acesso à Informação (Lei Nº 12.527/2011) e a Lei Carolina Dieckmann (Lei Nº 12.737/2012), leis estas relacionadas ao acesso à informação e à criminalização da obtenção de dados pessoais através de aparelhos eletrônicos.

Em 2014, o Marco Civil da Internet entrou em vigor, reforçando o direito à privacidade na Internet. No entanto, não trouxe exatamente a mesma proteção que a LGPD nos traz hoje.

Em 2015, as discussões sobre o tema ganharam mais atenção no Brasil, período em que foi realizada uma segunda consulta pública que viria a ser a base de diversos projetos de lei.

Por fim, em 2018 na Europa, o escândalo da Cambridge Analytica e a publicação da GDPR influenciaram para que a LGPD fosse aprovada no Brasil ainda em agosto deste ano. (BIONI, 2020)

A LGPD passou por um longo processo de tramitação no Congresso Nacional e também por uma grande discussão entre os mais diversos setores da sociedade.

Toda essa discussão teve como principal objetivo assegurar aos usuários o direito de saber como será realizado o consentimento, uso e tratamento de seus dados. Publicada em 14 de agosto de 2018, a LGPD passaria a valer, inicialmente, após 18 meses da data de sua publicação.

No entanto, a aprovação da LGPD passou por diversas mudanças significativas durante todo o processo de discussão para a sua validação. Muitos entendiam que havia a necessidade de um tempo maior para que as empresas e instituições conseguissem se adequar às inovações trazidas pela Lei, o que gerou constantes debates.

A Lei Nº 13.853, de 8 de julho de 2019, prorrogou a entrada em vigor da LGPD por mais 6 meses, ou seja, para agosto de 2020 e com a pandemia causada pela Covid-19, foram acentuadas as discussões sobre quando a LGPD entraria em vigor.

Em junho de 2020, a Lei Nº 14.010 foi aprovada e definiu, em seu Art. 20, que as sanções administrativas entrariam em vigor apenas a partir de agosto de 2021. Em outra alteração, foi aprovada a Medida Provisória 959/2020, que tentava prorrogar a entrada em vigor para maio de 2021.

Porém, ao se transformar na Lei Nº 14.058/20, em 17 de setembro de 2020, o artigo que tratava desta prorrogação foi excluído, portanto, valia a legislação anterior, ou seja, a Lei Nº 13.853/19, que determinava agosto de 2020 como o prazo de entrada em vigor.

Como isso ocorreu já em setembro de 2020, a LGPD passou a ter vigência imediata em 18 de setembro, um dia depois da aprovação da Lei Nº 14.058/20, com as devidas mudanças em relação à MP 959.

Em setembro de 2020 a LGPD passou a ter vigência por meio da sanção do Presidente da República, representando a concordância e anuência deste com a Lei, aprovada no Congresso.

Destaca-se que a LGPD já pode ser executada em sua totalidade desde agora, as punições em caso de desrespeito à norma já estão em vigor conforme a Lei Nº 14.010/20.

a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por regular a Lei, definir instruções para o cumprimento e fiscalizar as regras, ainda não foi plenamente estabelecida.

A lei já está em vigor e órgãos como o Procon e o Ministério Público também podem fiscalizar sua aplicação, isso significa que o Judiciário já pode decidir sobre casos que envolvam a Lei, nas quais os envolvidos se sintam prejudicados na forma em que seus dados são tratados, por exemplo.

Os titulares de dados, pessoas que compartilham seus dados em site, plataforma ou aplicativo, também já podem fazer requisições aos controladores, aos donos ou aos operadores dessas plataformas virtuais, a fim de conhecer como seus dados pessoais são tratados, as sanções podem ocorrer por meio de advertências, proibições totais ou parciais das atividades relacionadas ao tratamento de dados, além de multas que podem chegar a até 2% do faturamento das empresas, observando o limite de 50 milhões de reais. (BRASIL, 2018)

Destaca-se também que a LGPD pode ser aplicada fora do Brasil, uma vez que também considera os dados tratados dentro do território nacional, independentemente do meio aplicado, do país-sede do operador ou do país onde se localizam os dados.

Dessa forma, percebe-se a importância do objetivo da Lei Geral de Proteção de Dados, ao buscar promover a proteção dos direitos fundamentais de liberdade e de privacidade em relação aos dados de cada indivíduo.

3 PRINCÍPIOS QUE NORTEIAM A LGPD

a LGPD em seu Art. 6º enumera 10 princípios que norteiam o tratamento de dados pessoais e que vão ajudar a garantir que a empresa esteja em conformidade e adequada à lei.

3.1 Adequação

O princípio da adequação, segundo a LGPD, refere-se à “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”.

Em outras palavras, a empresa precisa justificar e garantir que os dados coletados tenham valor e sejam condizentes com o modelo de negócio da organização.

Vamos criar exemplos, primeiro, você é proprietário de uma farmácia. Ao fazer compras on-line, os clientes precisam preencher um cadastro e fornecer informações sobre orientação sexual.

Segundo o seu negócio é uma academia e você solicita, na matrícula, informações de caráter religioso e político.

De fato, nos dois exemplos apresentados, o tratamento dos dados não é compatível com o seu negócio e, consequentemente, com a lei, tornando a coleta e o tratamento injustificáveis e, inclusive, passíveis de punições e multas. (BRASIL, 2018)

3.2 Necessidade

O princípio da necessidade é interessante sob o ponto de vista da LGPD porque ele leva em consideração a responsabilidade das empresas acerca dos dados tratados.

Na prática, quanto mais dados pessoais você trata, maior é a sua responsabilidade e, por consequência, maior é a cobrança e mais caras são as multas em casos de erros e falhas.

A LGPD afirma que o princípio da necessidade envolve “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”.

A sua empresa precisa garantir que apenas os dados pessoais essenciais para o desenvolvimento do seu negócio sejam coletados e tratados. Basicamente, a LGPD diz: prenda-se ao necessário e essencial, e elimine os excessos. (BRASIL, 2018)

3.3 Livre Acesso

O princípio do livre acesso é um dos pontos fundamentais da LGPD. De acordo com a lei, o livre acesso é a “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”.

Na prática, a empresa deve criar mecanismos para que o titular dos dados tenha o direito de consultar os seus próprios dados e informações de forma gratuita. Além disso, a empresa precisa deixar evidente os seus objetivos e o período de tempo que os dados serão utilizados. (BRASIL, 2018)

3.4 Qualidade dos Dados

O princípio da qualidade dos dados se refere à “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”.

Ou seja, para respeitar as normas da LGPD, garanta que a base de dados pessoais que a sua empresa mantém seja verdadeira e esteja atualizada. Além disso, ela tem que estar alinhada com o propósito do seu negócio. (BRASIL, 2018)

3.5 Transparência

A transparência é outro princípio essencial da LGPD. Em suma, este princípio determina que as empresas precisam ser honestas com os titulares dos dados. Inclusive, devem informar aos proprietários dos dados sobre os respectivos agentes de tratamento, que são, basicamente, outras empresas envolvidas no processo de tratamento dos dados.

O princípio da transparência, de acordo com a lei, é a “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”. (BRASIL, 2018)

3.6 Prevenção

A velha máxima que diz que é melhor prevenir do que remediar também vale para a LGPD. O princípio da prevenção versa justamente sobre o ato de estar preparado para lidar com eventuais problemas envolvendo o tratamento de dados pessoais antes mesmo que eles surjam.

O princípio da prevenção determina a “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”. (BRASIL, 2018)

3.7 Não Discriminação

O tratamento de dados pessoais jamais pode ser realizado com objetivos de discriminar ou de promover abusos contra os seus titulares, neste caso, geralmente estamos falando dos dados pessoais sensíveis, como os que tratam sobre origem racial ou étnica, convicção religiosa e opinião política, por exemplo.

O princípio da não discriminação, de acordo com a LGPD, refere-se à “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”. (BRASIL, 2018)

3.8 Responsabilidade e Prestação de Contas

O princípio da responsabilização e prestação de contas dispõe sobre o cumprimento da lei tendo em vista provas e evidências de que medidas e procedimentos foram tomados pela empresa a fim de garantir a proteção dos dados

Sobre o princípio de segurança, diz a LGPD: “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”. (BRASIL, 2018)

3.9 Segurança

Como o próprio nome sugere, o princípio da segurança envolve a adoção de procedimentos, tecnologias e soluções que garantam maior proteção dos dados pessoais em casos de acessos não autorizados, como em ataques hackers, e de situações acidentais ou ilícitas de perda e alteração, por exemplo.

Sobre o princípio de segurança, diz a LGPD: “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”. (BRASIL, 2018)

4 VIOLAÇÃO DE DADOS, INCIDENTES DE SEGURANÇA E VAZAMENTOS 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 outros meios informáticos para armazenamento, comunicação, pesquisas, compras, transferências bancárias e 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 obstante, 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) quanto a LGPD (Art. 6º, Caput) têm como princípio a boa-fé objetiva, o qual possui deveres anexos e de proteção. (MARTINS-COSTA; BRANCO, 2002)

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 (Arts. 15, I e 16/LGPD).

Em relação ao dever de segurança, Fabiano Menke e Guilherme Damasio Goulart, comentam sobre os quatro atributos de uma informação intrínsecos a sua 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. (BEAL, 2005)

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 (HANSEN, 2019).

A proteção desses quatro atributos é intimidada 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, 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, 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. (GOBEO; FOLWER; BUCHANAN, 2018).

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 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.

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

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.

4.1 Violação de Dados e Incidentes de Segurança no Brasil

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 empresas de 16 regiões e países, sendo 35 delas no Brasil. (HERNANDEZ, 2019)

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%). (IBM; PONEMON, 2019)

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) segundo o Data Privacy Brasil.

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, sendo que mais de 205 milhões de dados pessoais vazaram de forma criminosa. (NETO; MADNICK: PAULA; BORGES, 2021)

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, mais de 19 mil clientes do Banco Inter, primeiro banco digital brasileiro, tiveram seus dados pessoais vazados em 2018, 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, 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.

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 equipamentos e softwares a instituições públicas voltadas ao combate de crimes cibernéticos e o restante a instituições de caridade, indicados pelo MPDF. (SANTINO, 2018)

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 falecida, a denúncia foi feita pela empresa de segurança da informação Psafe, ao monitorar negociações de dados sigilosos na deep web. (CORACCINI, 2021)

no segundo, com mesmo número de pessoas de dados vazados, incluía nome, data de nascimento, endereço, sexo, CPF, celular e e-mail, 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. (SOPRANA, 2021)

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. (POLIDO, 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. (DEMARTINI, 2021)

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.

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.

4.2 Violação de Dados e Incidentes de Segurança no Exterior

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. (FRUHLINGER, 2020)

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. (JAIN, 2019)

A falha veio de um sistema operado por uma empresa estatal, que permitiu o acesso a nomes, números de identidade, dados bancários, fotografias, impressões digitais, varreduras de retina e outros detalhes de identificação de quase todos os cidadãos indianos. (HK, 2018)

Ainda em 2021, um banco de dados do governo da Argentina contendo informações do cartão de identidade nacional foi encontrado à venda na deepweb, isto 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. (IKEDA, 2021)

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 se faz importante o debate sobre os mecanismos de segurança, como se demonstrará a seguir.

5 AS BOAS PRATICAS DA GOVERNANÇA NA LGPD E A MITIGAÇÃO DE RISCOS

5.1 A 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. (BARBIERI, 2020)

A necessidade de implementação de mecanismos de governança de dados pessoais é incontestável pois 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, inclusive para agir em conformidade com a lei. (SMEDINGHOFF, 2008)

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, 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. (SMEDINGHOFF, 2008)

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 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.

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, 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 incidentes e vulnerabilidades detectadas.

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.

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. A autenticação multifatores, 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.

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, principalmente de dados pessoais sensíveis, pela criptografia, por exemplo.

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 acarretar em vazamento das informações, 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).

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. (DE CARVALHO; MATTIUZO; PONCE, 2021).

5.2 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, seguir as disposições e as normas que serão criadas pela Autoridade Nacional, 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, como demonstrado acima. (WIMMER, 2021)

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, isso porque esta estimula padrões de comportamento desejáveis previstos por conta da avaliação de impacto. (BELLI, 2021)

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.

A ideia de analisar e averiguar os 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 Art. 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 necessária 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.

Como já dito, a Avaliação não se faz obrigatória no Brasil de acordo com a LGPD, mas poderá vir a ser por determinação da Autoridade Nacional, nos termos do Art. 38 C/C Art. 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.

6 CONSIDERAÇÕES FINAIS

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 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 apresentados 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

ALECRIM, Emerson. O que você deve saber sobre a lei de proteção de dados pessoais no Brasil. Disponível em: <https://tecnoblog.net/250718/lei-geral-protecao-dados-brasil/>. Acesso em: 14 out. 2020.

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.

BAMBINI, Gustavo; LUTAIF, Michel Kurdoglian. Estado e insegurança legislativa: a vacatio legis da LGPD. Disponível em: <https://www.jota.info/stf/supra/estado-e-inseguranca-legislativa-a-vacatio-legis-da-lgpd-07092020>. Acesso em: 17 out. 2020.

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

BRANDÃO, Marcelo. Vigência da Lei de Proteção de Dados depende de sanção da MP 959. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2020-08/vigencia-da-lei-de-protecao-de-dados-depende-de-sancao-da-mp-959>. Acesso em: 14 out. 2020.

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-etransportes/2021/04/brasil-esta-entre-os-cinco-paises-do-mundo-que-mais-usaminternet#:~:text=Com%2078%2C3%25%20de%20brasileiros,fibras%20%C3%B3 Pticas%20%C3%A0s%20redes%20nacionais. BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 17 out. 2020.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm#:~:text=Disp%C3%B5e%20sobre%20a%20tipifica%C3%A7%C3%A3o%20criminal,Art>. Acesso em: 17 out. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 out. 2020.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2>. Acesso em: 17 out. 2020.

BRASIL. Lei nº 14.010, de 10 de junho de 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm#art20>. Acesso em: 17 out. 2020.

BRASIL. Lei nº 14.058, de 17 de setembro de 2020. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2020/lei-14058-17-setembro-2020-790639-publicacaooriginal-161518-pl.html>. Acesso em: 17 out. 2020.

BRASIL, Medida Provisória nº 959, de 29 de abril de 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm>. Acesso em: 17 out. 2020.

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.

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.

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-sobreprotecao-de-dados-no-brasil-e-no-mundo/. Acesso em 12 nov 2021.

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-dadosde-21-mil-funcionarios-da-claro-e-net-194418/. Acesso em 12 nov 2021.

FIDELIS, Aline; WERNECK, Bruno; MANZUETO, Cristiane; VINCI, Guido; BRAGA, Ludmila Arruda; SANCOVSKI, Michel. As Sanções da LGPD entrarão em vigor em Agosto de 2021. [S. l.], 12 jun. 2020. Disponível em: <https://www.tauilchequer.com.br/pt/perspectives-events/publications/2020/06/lgpd-sanctions-will-take-effect-on-august-2021>. Acesso em: 17 out. 2020.

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-wasaffected-what-was-the-impact.html. Acesso em 12 nov 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-dedados-aumentaram-493-no-brasil-mostra-pesquisa-do-mit.html. Acesso em 12 nov 2021.

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/nobrasil-empresa-que-falha-ao-proteger-dados-tem-perdas-menores.shtml. Acesso em 12 nov 2021.

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.

HUMBY, Clive. 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.

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-cardinformation-of-entire-country-made-available-on-dark-web-forum/. Acesso em 17 nov 2021.

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-cardcybersecurity-issues-with-indias-biometric-experiment/#_ftnref4. Acesso em 15 nov 2021.

KUCEK, Gisele Bolonhez. LGPD – Lei Geral de Proteção de Dados e sua vigência. Disponível em: <https://www.jornaljurid.com.br/blog/auxilium/lgpd-lei-geral-de-protecao-e-dados-e-sua-vigencia>. Acesso em: 14 out. 2020.

Lei Geral de Proteção de Dados entra em vigor. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>. Acesso em: 17 out. 2020.

LGPD entra em vigor. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-entra-em-vigor>. Acesso em 14 out. 2020.

LGPD: o que é, principais determinações e resumo. Disponível em: <https://fia.com.br/blog/lgpd/>. Acesso em: 17 out. 2020.

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.

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. Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873. Acesso em 12 nov 2021.

NISTLER, Regiane. Estudos sobre Direito, Globalização e Sustentabilidade. Vol. 1., Deviant, 2020

Objetivo e Abrangência da LGPD. Disponível em: <https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/objetivo-e-abrangencia-da-lgpd>. Acesso em 14 out. 2020.

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

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-queo-recente-vazamento-em-massa-de-dados-pessoais-revela-para-o-brasil-04022021. Acesso em 15 nov 2021.

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/opinionrecommendation/files/2014/wp216_en.pdf. Acesso em 5 nov 2021.

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-interpagara-r-1-5-milhao-por-vazar-dados-de-quase-20-mil-pessoas/. Acesso em 12 nov 2021.

SANTOS, Rodrigo. Linha do tempo da LGPD: O que mudou desde o primeiro anúncio? Disponível em: <https://www.compugraf.com.br/linha-do-tempo-da-lgpd/>. Acesso em: 17 out. 2020.

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

SMEDINGHOFF, Thomas J. Information Security Law: The Emerging Standard for Corporate Compliance. Cambridgeshire: ITGP, 2008. p. 20-21.

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-milhoesbrasileiros-atribuida-ao-poupatempo.shtml?origin=folha. Acesso em 12 nov 2021.

TOMMASO, Rafael di. Lei de proteção de dados completa 50 anos. Disponível em: <https://digialogos.com.br/podcast/lei-de-protecao-de-dados-completa-50-anos>. Acesso em: 17 out. 2020.

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.

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-confirmavazamento-de-dados-apos-ataque-hacker.htm. Acesso em 12 nov 2021

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-porvazamento-de-dados-de-clientes/. Acesso em 12 nov 2021.

VERDÉLIO, Andreia. Lei Geral de Proteção de Dados entra em vigor. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/lei-geral-de-protecao-de-dados-entra-em-vigor#:~:text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o,a%20pandemia%20do%20novo%20coronav%C3%ADrus>. Acesso em: 14 out. 2020.

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.

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.