Recebido em: 26/02/2024
Aceito em: 28/11/2024
DOI: 10.25110/rcjs.v27i2.2024-10979

SEGURANÇA E PREVENÇÃO NO VAZAMENTO DE DADOS NO CDC E NA LGPD

SECURITY AND DATA LEAKAGE PREVENTION AT CDC AND LGPD

Ricardo Morishita
Doutorado em Direito pela Pontifícia Universidade Católica de São Paulo (2017). Possui mestrado em Direito na Universidade de São Paulo (2003) e graduação em Direito pela Pontifícia Universidade Católica de São Paulo (1991). Advogado e professor universitário, foi diretor do Departamento Nacional de Proteção e Defesa do Consumidor (2003-2010) e Professor e coordenador de pesquisas de direito do consumidor vinculadas ao Centro de Justiça e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas (2010-2014). Diretor de Projetos e Pesquisas no Instituto Brasiliense de Direito Público - IDP.
ricardo.morishita@idp.edu.br
https://orcid.org/0000-0002-9358-4038
http://lattes.cnpq.br/9927829490113370

Nyvea Lourenço
Doutoranda em Direito Constitucional (IDP). Possui mestrado em Administração Pública (IDP/EAB), especialização em Integração Econômica e Direito Internacional Fiscal (ESAF/União Europeia), é especialista Docente em Direito Tributário (UNIDF), pós-graduada em Direito Tributário Aplicado à Gestão Pública (NDA/FACNET). Graduada em Direito pela Universidade Santa Úrsula. É Auditora-Fiscal da Receita do Distrito Federal – SEFAZ/DF.
nyvea@uol.com.br
https://orcid.org/0000-0001-8049-6533
http://lattes.cnpq.br/0830861809290299

RESUMO: O trabalho analisa as mudanças e adaptações na rotina das pessoas introduzidas pelos meios digitais e outros fatores no mundo globalizado. Após a inserção dos dados pessoais para utilização desses meios virtuais, as pessoas, de certa maneira, perdem o controle sobre esses dados que ficam armazenados com terceiros. Importante ponto é: qual a segurança que o usuário/consumidor tem que esses dados não serão vazados e/ou utilizados de forma indevida? Nesse contexto, o trabalho objetiva trazer reflexões sobre medidas de segurança e prevenção no vazamento de dados no Código de Defesa do Consumidor - CDC e na Lei Geral de Proteção de Dados - LGPD, em especial, o Relatório de Impacto à Proteção de Dados Pessoais - RIPD, que é visto como uma forma de salvaguardar ou mitigar o risco no vazamento dos dados. O referido relatório ainda não foi regulamentado pela Autoridade Nacional de Proteção de Dados; autoridade brasileira responsável por implementar, fiscalizar e zelar pelo cumprimento da LGPD. A questão é: o RIPD deve ser obrigatório ou não para todos os Controladores? Na metodologia, o desenvolvimento do tema será utilizada a técnica de pesquisa documental e bibliográfica. Além de bibliografia utilizar-se-á legislação, artigos especializados, seminário e entendimentos jurisprudenciais.
PALAVRAS-CHAVE: Dados; Vazamento; Segurança; Prevenção.

ABSTRACT: The work analyzes the changes and adaptations in people's routines, introduced by digital media and other factors in the globalized world. After entering personal data to use these virtual media, people, in a way, lose control over these data that are stored with third parties. An important point is: what security does the user/consumer have that this data will not be leaked and/or misused? In this context, the work aims to bring reflections on security measures and prevention of data leakage at the Consumer Protection Code and General Data Protection Law, in particular, the DPIA - Data Protection Impact Assessment, which is seen as a way to safeguard or mitigate the risk of data leakage. The aforementioned report has not yet been regulated by National Data Protection Authority is the Brazilian authority responsible for implementing, inspecting, and ensuring compliance with the General Data Protection Law. The question is: should the DPIA be mandatory or not for all Controllers? In the methodology, the development of the theme will use the technique of documentary and bibliographic research. In addition to bibliography, legislation, specialized articles, Seminars and jurisprudential understandings will be used.
KEYWORDS: Data; Leak; Security; Prevention.

Como citar: MORISHITA, Ricardo; LOURENÇO, Nyvea. Segurança e Prevenção no Vazamento de Dados no CDC e na LGPD. **Revista de Ciências Jurídicas e Sociais da UNIPAR**, Umuarama, v. 27, n. 2, p. 447-466, 2024.

INTRODUÇÃO

A partir da globalização, fenômeno esse cada vez mais universalizado, tem-se utilizado cada vez mais da velocidade e dinamicidade dos eventos desta nova fase. Tais indicadores têm desempenhado um papel significativo, nas transformações e ajustes da maneira de como as pessoas vivem, tendo como destaque, no momento presente, a transformação da rotina das pessoas em virtude do impacto dos meios digitais e outros elementos atrelados a este meio.

Neste contexto, os dados dos usuários das diversas plataformas digitais existentes, ficam armazenados nos *drives*, desde as pequenas até as grandes empresas de tecnologia as quais passam a ser detentoras dessas informações.

Com o desenvolvimento dessa era, onde o meio digital é aperfeiçoado de forma progressiva e exponencial, seja para uma simples pesquisa, utilização de redes sociais ou compras online, desde o momento da inserção de dados do usuário, não há mais controle acerca de acesso e utilização dessas informações, uma vez que o armazenamento destas é realizado por terceiros. A grande questão é: como garantir a segurança desses dados de forma que não ocorra o vazamento ou uma utilização indevida? Dessa forma, é entendido que alguns acreditam que o vazamento ocorrerá inevitavelmente, apenas não se sabe quando.

Nessa perspectiva, de forma a minorar possíveis vazamentos e ainda com o objetivo principal de salvaguardar os dados dos usuários da *web,* foi criada a Autoridade Nacional de Proteção de Dados – ANPD, esse órgão da Administração Federal é responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território nacional.

Destarte, o presente trabalho tem como objetivo principal trazer ponderações acerca das medidas de segurança e prevenção no vazamento de dados no Código de Defesa do Consumidor - CDC – Lei 8.078/1990 e na Lei Geral de Proteção de Dados – LGPD - Lei 13.709/2018, e ainda a atuação e o impacto do Relatório de Impacto à Proteção de Dados - RIPD nesse cenário.

1 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

A globalização desempenha um papel significativo na sociedade atual, porém, certos impactos podem influenciar negativamente as políticas dos países, causando danos tanto internamente quanto externamente (Resende; Brasil, 2020).

Com a evolução do mundo globalizado, cada vez mais as pessoas utilizam os meios digitais, seja para realizar uma pesquisa simples, seja para fazer uso de plataformas de rede social ou até mesmo para efetuar compras através da internet.

Os usuários e/ou consumidores inserem seus dados, estes ficam armazenados com pequenas e grandes empresas de tecnologia detentoras dessas informações. As grandes empresas são chamadas *Big Techs* que por vezes são vistas como um poder paralelo, uma vez que informação é poder.

Dentre essas empresas, destacam-se as chamadas *big techs*, popularmente conhecidas como as grandes empresas. Essa categoria de empresa preza por um plano de negócios criado com o objetivo de possibilitar interações diretas entre um grande número de usuários em plataformas digitais, como *e-commerce*, busca e mídias sociais (Boissay et al[1], 2020), tradução nossa).

Nesse contexto, as inovações de um modo geral tornaram-se resultado das *big techs* – que causaram grandes impactos nas rotinas das pessoas, melhorando por um lado, mas por outro lado a velocidade da propagação das notícias pode gerar efeitos nocivos, sobretudo se a notícia não for verdadeira, como no caso das *fake news*.

Nessa esteira, o alcance em massa, se bem utilizado, pode gerar excelentes resultados. Porém, por outro lado, se as informações ou os dados forem manipulados e dissimulados podem ter consequências desastrosas. De acordo com Frederic Boissay o compromisso entre eficiência e privacidade dependerá das preferências da sociedade e variará em diferentes jurisdições.

[1] No original: The business model of big techs rests on enabling direct interactions among a large number of users on digital platforms, such as in e-commerce, search and social media.

Por isso, é essencial coordenar políticas tanto a nível nacional quanto internacional (Boissay et al., 2020, tradução nossa[2]).

Dessa forma, cabe à sociedade e aos cidadãos, dentro do possível, salvaguardar seus dados não navegando em sites desconhecidos ou em ambientes não seguros e também apurar a veracidade das informações propagadas para tomar seu próprio juízo de valor. Dessa maneira, de acordo com Zocatelli Queiroz (2021), apesar dos cidadãos terem total liberdade para compartilhar aspectos importantes ou triviais de suas vidas, é crucial assegurar a proteção adequada dos direitos fundamentais no que diz respeito ao amplo e irrestrito acesso às informações pessoais por parte de instituições públicas ou privadas de tratamento de dados.

Ademais, entende-se que apesar dos benefícios da instantaneidade ao acesso à informações e notícias, existe também um fator determinante que detém de um papel relevante no aumento da complexidade na tarefa, não só, de selecionar, como também filtrar e distinguir entre o que é verídico e o que não é. Conforme Law (2020), no momento presente, a sociedade encontra-se vivenciando a era da Revolução 4.0 ou, popularmente definida como a Quarta Revolução Industrial, a qual se destaca pela velocidade extrema na criação e disseminação de não só avanços tecnológicos, como informações e até mesmo dados pessoais.

Dentre as características presentes na “Revolução 4.0”,destaca-se o uso e a disseminação da Inteligência Artificial - IA, do avanço de pesquisas e uso da biotecnologia e outras inovações as quais têm a capacidade de transformar, de forma universal, o cotidiano da população usuária. Assim, é necessária uma adaptação ao novo mundo, onde além de um bombardeio diário com informações em tempo real, o uso de facilitadores de compras, via internet, ganha, cada vez mais, espaço entre os consumidores, o que ocasiona um volume expressivo de operações.

Neste determinado cenário específico, é importante ressaltar que o usuário ou consumidor, uma vez que forneceu suas informações pessoais, acaba por perder de uma maneira em particular, a posse e o domínio sobre

[2] No original: The nature of the new trade-off between efficiency and privacy will depend on societal preferences, and will vary across jurisdictions. This increases the need to coordinate policies both at the domestic and international level.

tais dados, vendo-se em uma situação de não ter mais pleno controle sobre os mesmos.

Assim sendo, em análise macro acerca da globalização, difusão e transporte em tempo real não só de informações, como também de dados pessoais indaga-se qual a segurança que o usuário/consumidor tem de que esses dados não serão vazados e/ou utilizados de forma indevida? Nesse aspecto, pesquisadores e estudiosos defendem que há quem diga que o vazamento ocorrerá, a incerteza gira em torno do prazo para que isso ocorra.

De forma a regulamentar o tráfego e o domínio de dados pessoais, em Setembro de 2020 entrou em vigor, no Brasil, a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, que regulamenta o tratamento de dados pessoais não só em meios digitais, mas também físicos (Zocatelli; Queiroz 2021).

Em continuidade, vale destacar a Emenda Constitucional Nº 115, de 10 de Fevereiro de 2022 que alterou os artigos 5º, 21 e 22 da Constituição Federal do Brasil de modo a incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e assim fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais; traz o seguinte texto:

> [...] Art. 5º
> LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. ”
> Art. 21.
> XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. ” (NR)
> “Art. 22.
> XXX – proteção e tratamento de dados pessoais. [...] (Brasil, 2022)

Nesse sentido, é notório que a legislação brasileira tem como principal objetivo a proteção ou até mesmo a mitigação de todo e qualquer possível vazamento. Por consequência desses pilares, foi criada a Autoridade Nacional de Proteção de Dados - ANPD, que detém o objetivo institucional de garantir, de maneira abrangente e precisa, a adequada conformidade com as diretrizes estabelecidas na Lei Geral de Proteção de Dados (LGPD) no território brasileiro. Além disso, sua atuação tem como propósito salvaguardar os

direitos fundamentais relacionados à liberdade, privacidade e crescimento livre da personalidade dos cidadãos (Macêdo; Schmidt, 2022).

Um fato que destaca o avanço e o compromisso da legislação brasileira perante à proteção dos dados dos usuários dos sistemas, páginas e demais plataformas oferecidas é a sintonia entre a LGPD e o Código de Defesa do Consumidor - CDC. Destaca-se o artigo 45 da referida Lei, onde é afirmado que as hipóteses de violação do direito no âmbito das relações de consumo, tem às suas penalidades definidas e regidas pelo CDC. Ou seja, em caso de violação, divulgação e/ou qualquer dano causado para o usuário, no âmbito de relações de consumo, a responsabilidade acerca da possível punição do agente causador é definida e regida através do CDC, conforme trecho da lei a seguir.

> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente (Brasil, 2018).

Segundo Fernandes e Nuzzi (2022), a doutrina brasileira reconhece o direito à proteção de dados pessoais como um direito fundamental e o considera como independente e de maior relevância do que a tutela da intimidade e da privacidade. Esse direito está previsto em uma legislação moderna, abrangente e aplicável a todas as situações relacionadas a essa questão.

No mundo atual, onde a privacidade é um direito cada vez mais desafiado, é fundamental agir com cautela ao lidar com dados pessoais, tendo como um dos principais objetivos a implementação dos procedimentos necessários para garantir a segurança e evitar possíveis violações. Sumariamente, de acordo com Dahle de Almeida e Soares (2022), a Lei Geral de Proteção de Dados (Lei nº 13.709/18 — LGPD), detém de uma atitude sensata ao considerar a proteção de informações pessoais, por meio de medidas indispensáveis na era digital, onde os dados pessoais são tratados como bens preciosos.

Contudo, a interpretação dos usuários ainda não vai de acordo com o esforço proposto nos normativos citados, uma vez que de acordo com a

pesquisa de privacidade do consumidor da Cisco 2021[3], foi apontado não só um baixo nível de confiança do consumidor na proteção de sua privacidade *online*, como também a busca pela transparência e controle sobre como as empresas lidam com seus dados.

Em continuidade acerca da pesquisa dita, foi constatado que, entre outras considerações, revelou-se através do estudo que uma parcela significativa dos usuários e/ou consumidores acredita que a Inteligência Artificial - IA utiliza informações para facilitar a efetivação de escolhas de forma automatizada. Tal suspeita vem sendo frequentemente levantada, deixando claro um certo grau de desconfiança em relação ao uso dessa tecnologia.

A pesquisa supracitada aborda o anúncio do Novo Padrão de Confiança da Cisco, o qual tem como objetivo o estreitamento de relações com o usuário, através principalmente da convicção acerca do tipo de tratamento, que a empresa utilizará o com dados informados pelos consumidores e/ou usuários. Dessa maneira, com o objetivo de estabelecer uma construção da confiança do consumidor, indicativos fundamentais para apertar esse laço são transparência e controle, e através desses indicadores, será possível estabelecer uma referência a qual servirá como ferramenta base para a verificação acerca da confiabilidade das empresas, no que diz respeito à transformação digital.

Diversos pesquisadores se dedicam ao estudo do fator confiança nas relações sociais, tais e quais Kant, Habermas e Luhmann, os quais tiveram como objetivo em suas obras, demonstrar para a sociedade a relevância desse princípio para a sociedade na qual o indivíduo encontra-se inserido (Verbicaro; Calandrini, 2022).

Ainda de acordo com Verbicaro e Calandrini (2022), a definição do jurista alemão Karl Larenz, revela que confiança é um princípio inseparável do direito e ainda atua como agente balizador entre as relações contratuais, de forma a exercer um papel de “motor” da atuação do indivíduo, onde passa a ser estabelecida uma conexão direta com o princípio da responsabilidade. Em continuidade acerca do entendimento de Karl, o princípio da confiança está

[3] Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/cisco-cybersecurity-series-2021-cps.pdf

fundamentado no personalismo ético de tal forma que a pessoa livre, social e racional será o fator determinante de si mesma.

O Novo Padrão de Confiança ou *New Trust Standard*, segundo a matéria, pode ser usado por qualquer organização que visa atender a um novo padrão de proteção de dados. O estudo salientou quatro elementos essenciais, estabelecidos pela Cisco, que as organizações necessitam para crescer enquanto se mantêm seguras, ao mesmo tempo em que mantêm a confiança pública, sejam eles:

> [...] Forneça comunicações claras sobre como você usa os dados do cliente [...]
> [...]Aumente a visibilidade das regulamentações e proteções de privacidade do seu país [...]
> [...] Trabalhe para criar políticas de "volta ao escritório" que forneçam um ambiente de trabalho seguro, enquanto ainda protegem e respeitam os direitos individuais e a privacidade [...] e
> [...] Prossiga com cuidado ao usar dados pessoais na tomada de decisão automatizada que afeta os clientes. [...] CISCO (Brasil).

Desta forma foi observado que a intimidação exercida pelos usuários e/ou consumidores, através da redução ou até mesmo a paralisação de compras /ou utilização de serviços virtuais, têm força significativa ao ponto de promover uma ação desencadeadora acerca de fomentar e implementar mecanismos de ações por parte das empresas, de modo a aprimorar as entregas, e como consequência aumenta a confiabilidade, dos usuários e/ou consumidores, e segurança no uso dos dados pessoais.

Ainda sobre parâmetros de proteção, com o intuito de fornecer proteção para as atividades de tratamento de dados pessoais, a legislação brasileira é taxativa quanto à definição dos princípios a serem seguidos.

Nesse contexto, destaca-se o artigo 6º da Lei Geral de Proteção de Dados, o qual elucida:

> [...]Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. *(grifo nosso)* [...] (Brasil, 2018).

De forma a assegurar o cumprimento dos princípios preditos e também destes indicadores de boas práticas, cumpre evidenciar o artigo 5º da referida lei. De forma a destrinchar o teor do artigo em comento, é importante citar que este fragmento do instrumento legal, detém a responsabilidade de conceituar as expressões, palavras e demais jargões utilizados ao longo da norma de acordo com o trecho a seguir.

> [...]Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

> VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;
> VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados; (Redação dada pela Medida Provisória nº 869, de 2018)
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
> XVII - relatório de impacto à proteção de dados pessoais: 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; [...] *(grifo nosso)* (Brasil,2018).

Conforme a definição na LGPD, o Relatório de Impacto à Proteção de Dados Pessoais - RIPD tem como objetivo a gestão de riscos existentes de forma a prover a mitigação.

Nesse contexto, caso o preposto não esteja aderindo às proeminências como expedientes de precaução e segurança e outros ditames, conforme Capítulo VII – Da Segurança e das Boas Práticas, será responsabilizado e incumbirá indenização de danos, de acordo com a Seção III – Da Responsabilidade e do Ressarcimento de Danos – art. 42 e 44, todos da Lei

13.709/2018. À vista disso, é provindo à ANPD a fiscalização e aplicação de sanções em caso de descumprimento.

É observado que a ANPD tem a delegação de competência para regulamentar o RIPD, em conformidade com o art. 55-J, inciso XIII da LGPD, e ainda que esses regulamentos deverão ser precedidos, inclusive, de análises de impacto regulatório - art. 55-J § 2º do mesmo diploma legal conforme demonstrado a seguir.

> [...]Art. 55-J. Compete à ANPD: [...]
> [...] XIII - 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 de proteção de dados pessoais previstos nesta Lei; [...] (BRASIL, 2018).

Ocorre que não há registros acerca dessa regulamentação perante a ANPD. A ausência desta normatização, cabe destacar que tal ação encontra-se prevista no artigo nº 5 inciso XVII da LGPD, incide na possível falha acerca de identificação e exposição de diversos riscos e falhas e, como consequência, medidas de segurança e prevenção de vazamento poderiam ser adotadas. Entretanto, com a ausência da obrigação acerca da elaboração do documento em questão, não há previsão para gastos financeiros e de mão de obra, uma vez que há um custo considerável e complexidade na confecção do documento.

> [...]A partir da definição adotada na LGPD, pode-se inferir que, ao importar a concepção de relatório de impacto à proteção de dados do Regulamento Geral da Proteção de Dados, a metodologia recomendada para a elaboração do referido relatório, no instrumento brasileiro, é, assim como na Europa, aquela baseada em risco. [...] (Garrote et al., 2021).

Dessa forma, é de se indagar: O RIPD deveria ser compulsório para todos os controladores, haja vista que a LGPD é negligente nesse ponto? Ou poderia valer-se de critérios ou cálculo de riscos (baixa, média e alta complexidade) e assim listar um rol de imperiosidade e/ou anulação do mencionado relatório?

É relevante evidenciar que ANPD terá total autonomia para estabelecer indicativos e critérios a fim de definir a sua escolha metodológica com o

intuito de elaboração do relatório de impacto. Ou seja, é possível dizer que a adoção tácita, pela LGPD, de uma metodologia baseada em risco não define, tampouco obriga, a escolha da Autoridade Nacional. Dessa forma, é compreensível que tal figura poderá optar por uma metodologia mais compatível com a realidade brasileira (Garrote et al., 2021).

No Seminário sobre "Vazamento de Dados e o regime de prevenção e reparação de danos no CDC e na LGPD" (2021)[4], a professora Heloísa Carpena pontuou algumas questões quanto ao tema e teceu que há uma aproximação com a disciplina do Código de Defesa do Consumidor no tocante aos produtos e serviços que são perigosos ou nocivos.

No capítulo da Qualidade do CDC – o art. 8º evidencia deveres especiais para o fornecedor que ofereça e/ou produza produtos e serviços que podem ser considerados nocivos e perigosos. E vem crescendo até o art. 10 que trata de uma regra que se assemelha com a LGPD, relativamente ao *Recall* – quando esse risco é identificado posteriormente à introdução do produto no mercado. O fornecedor tem o dever de comunicar isso amplamente.

A experiência alcançada mediante o uso do Direito do Consumidor é que essas normas foram de baixa aderência. Embora não tenha, exatamente, uma discussão, há algum tipo de controvérsia em relação a elas, na verdade, o Administrador jamais demonstrou preocupação em elaborar uma lista que trouxesse esses exemplos; e no campo jurídico tem-se escassos casos relativos a esse encargo informativo. No entanto, mediante a utilização de recursos/subsídios na doutrina do Direito do Consumidor, não se faz imprescindível a presença de tal regulamentação, todavia, a existência da regulamentação, inegavelmente, proporcionará vantagens à aplicação da norma.

> [...] a teoria do diálogo das fontes entre CDC (LGL\1990\40) e LGPD aprofunda o entendimento e amplia a tutela do indivíduo em sua vulnerabilidade frente ao tratamento de dados pessoais pelo fornecedor, agora também revestido da qualidade de agente de tratamento de dados.[...] (Oliveira; Freitas, 2021).

[4] Disponível em: https://www.youtube.com/watch?v=KKL6By2iatU

Outro enfoque residiria no que o dispositivo legal salvaguarda, com referência ao Código de Defesa do Consumidor, porém abrangendo o arcabouço jurídico em sua integralidade; o referido código é percebido como um instrumento de estabelecimento de regras no campo do comércio de bens e serviços. Não apenas como uma salvaguarda da parte mais suscetível na relação de consumo. Tal perspectiva possui uma amplitude, estando mais arraigada em algo que já possui solidez; que já conta com uma vasta experiência de aplicação da lei.

Conforme Negrisoli Fernandez Polettini (2020) é passível de assumir que além do diálogo presente, no que tange às previsões principiológicas da LGPD e as previsões do CDC, a defesa do consumidor é um dos fundamentos da Lei Geral de Proteção de Dados.

O Relatório de Impacto à Proteção de Dados Pessoais, uma vez regulamentado pela Agência Nacional de Proteção de Dados, trará suposições e a descrição de como deve este documento ser elaborado e como consequência, ocorre o favorecimento para que essa norma não se torne ineficaz perante a Lei Geral de Proteção de Dados. Entretanto, pelo fato de ter ocorrido esse levantamento, a doutrina de proteção de dados não se refere ao relatório como um mero *checklist* de conformidade, mas sim como uma análise concreta do risco em uma determinada situação. No entanto, ao cumprir com essa obrigação, o controlador/fornecedor não se isenta de responsabilização pelos danos que possam ocorrer. Isso é de extrema importância.

> A LGPD regulamenta a forma como os dados pessoais devem ser armazenados e como devem ser tratados, essencialmente, nos meios digitais. E é essa uma das mais importantes atenções dispensadas à defesa do consumidor brasileiro, ou seja, é incluir no conceito de direito à privacidade, o direito do consumidor de determinar quem pode ter acesso aos seus dados pessoais, de que forma será esse acesso e quais os limites de uso deles por terceiro (Follone; Filho, 2020).

O objeto de proteção da lei é a confiança depositada pelo proprietário dos dados, na relação estabelecida entre o homem e a rede, ou seja, é a proteção às legítimas expectativas. Em continuidade, essas expectativas se qualificam como legítimas não do ponto de vista subjetivo, e ainda a lei vai

garantir aquilo que se qualifica como legítimo. E, neste caso, a lei conceitua legítimo como aquilo que o fornecedor e/ou controlador deve fazer.

Então, esses deveres que estão previstos de forma expressa e taxativa existem muitos sobre anonimização, sobre mitigação de danos e outros, e é com fundamento nesses deveres que serão determinados os limites dessa expectativa que é protegida.

Quanto à responsabilidade civil dos agentes de tratamento, a professora Heloísa Carpena defende a tese da responsabilidade civil objetiva e acrescenta que os incidentes de segurança são por natureza acidentes de consumo, conforme art. 14 do CDC. Assim, a convergência entre a responsabilidade civil ativa e a LGPD é a ideia do risco e a tomada de decisões proativas do agente de tratamento para mitigação destes riscos.

Nessa acepção, existem algumas incumbências do agente relacionadas à periculosidade, a saber: formulação de relatório de impacto à proteção de dados pessoais, notificação à ANPD e ao interessado perante eventualidades, adoção de práticas exemplares por controladores e operadores; e criação de políticas e segurança apropriadas.

Nesse contexto, a professora Heloísa Carpena, tem como interpretação de que o RIPD deveria ser obrigatório. Contudo, não em todos os casos haja vista que o risco exacerbado como na experiência do consumidor não é presente em 100% da realidade prática, desta forma compreende-se que o relatório em questão está ligado ao grau do risco a ser enfrentado. Entretanto, nos últimos 30 anos o grau de proteção, no que diz respeito ao consumidor no território nacional, está cada vez mais alto.

No *leading case* do IBGE, em que foi anulada a MP - Medida Provisória 954/2020, havia a previsão do RIPD, contudo o momento definido seria após a transferência de dados. Ocorre que após a transação de milhões de dados de clientes das operadoras de telecomunicações ao IBGE, o Supremo Tribunal Federal – STF ressaltou que o Relatório de Impacto à Privacidade e à Proteção de Dados deveria ser antecedente e não posterior ao compartilhamento dos dados. Este veredito foi comparado com a situação ocorrida no Tribunal Constitucional da Alemanha no julgamento do censo.

Nesse cenário, o Ministro Ricardo Lewandowski ao proferir seu voto na ADI 6387, destacou que o § 2º do art. 3º da referida MP 954/2020, previa:

> [...] § 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no caput do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2020).

E, ainda o ponderou o Ministro Lewandowski que:

> [...] a confecção de relatório de impacto à proteção das informações pessoais dos consumidores não pode ser feito a destempo, depois de já compartilhados e ocorridos eventuais abusos, pois assim, ao menos em um juízo de cognição sumária, será tarde demais para que seja apurado se houve ou não adequação à legislação e como foi impactado o regime de proteção de dados. (ADI 6387-MC-REF/DF - Acórdão,Voto p.11) (Brasil, 2020).

No âmbito internacional, dentro da União Europeia, o relatório de avaliação de impacto não é compulsório para todas as entidades, existindo uma graduação no que concerne ao nível de perigo envolvido. Por outro lado, nos Estados Unidos da América, tal relatório não é obrigatório para as entidades de natureza privada, sendo aplicável exclusivamente aos órgãos pertencentes à administração pública, nas circunstâncias específicas.

Destarte, uma vez regulamentado o RIPD, a ANPD terá outras barreiras a serem superadas, tais como a efetiva fiscalização do relatório e se as ações em prol da mitigação de risco e/ou prevenção no vazamento de dados estão realmente implementadas pelas controladoras.

CONSIDERAÇÕES FINAIS

A fluidez e a celeridade dos eventos, em um globo interconectado, têm substantivamente contribuído para as transformações e adaptações no cotidiano dos indivíduos. Presentemente, as plataformas digitais alteraram esse cotidiano e os usuários estão, progressivamente, fazendo uso dos meios virtuais, desde uma simples pesquisa, seja para o emprego das redes sociais ou até mesmo para compras *online*.

Os usuários, ao registrarem suas informações, autorizam que essas sejam retidas pelas empresas de tecnologia, essas desde de pequeno e grande porte, as quais detêm o controle desses dados. As empresas de grande porte são frequentemente conhecidas como *big techs*, as quais são ocasionalmente

consideradas como uma entidade paralela, uma vez que estas utilizam da máxima de que conhecimento é sinônimo de poder. Nesse cenário, com o aparecimento das *big techs* e suas inovações, a população passou a adaptar-se à nova forma operacional de trabalho, rotina diária, comunicação e compras via internet.

Nesta circunstância, o usuário posteriormente à inserção de suas informações, de certa forma, deixa de ter o domínio absoluto sobre as mesmas. O cerne da questão reside na garantia de proteção de que o usuário possui, assegurando que tais dados não serão expostos indevidamente e/ou utilizados de maneira ilícita. Neste âmbito, existem aqueles que afirmam que a exposição haverá, apenas incerta é a data em que tal ocorrerá.

Vale elucidadar a Emenda Constitucional Nº 115, de 10 de Fevereiro de 2022 que alterou os artigos 5º, 21 e 22 da Constituição Federal de modo a incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e, consequentemente foi possível consolidar a competência privativa da União para legislar acerca da proteção e tratamento de dados pessoais.

Nesse sentido, apesar de haver uma sintonia entre o CDC e a LGPD, a legislação brasileira caminha para salvaguardar ou mitigar possível vazamento de dados privados. A partir dessa premissa foi criada a Autoridade Nacional de Proteção de Dados – ANPD, um órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território nacional.

Uma das medidas advindas como estratégia para prevenir e mitigar a possibilidade de ocorrência de vazamento de informações é o Relatório de Impacto à Proteção de Dados Pessoais – RIPD, esse documento, o qual ainda será devidamente normatizado pelo órgão fiscalizador ANPD. No entanto, uma vez superada essa fase, a ANPD encontrará obstáculos adicionais, incluindo a exigência fiscalização efetiva do relatório, bem como verificar se as ações em prol da minimização de riscos e/ou prevenção de vazamento de dados estão genuinamente implantadas pelas entidades controladoras.

Vale observar que, ainda que o RIPD esteja regulamentado, o relatório não garante total segurança quanto ao vazamento, apenas aponta que ações

estão sendo feitas para mitigar o risco de vazamento que, inclusive, tem-se como certo que ocorra, só não se sabe quando.

É de extrema relevância destacar que, mesmo considerando a regulamentação do RIPD, esse documento não assegura plena segurança em relação à divulgação indevida, apenas indica as medidas em andamento para reduzir o risco de vazamento. Uma vez que é indiscutível a ocorrência desse tipo de compartilhamento e/ou vazamento de informações pessoais, porém sua temporalidade permanece desconhecida.

Dessa maneira, nessa conjuntura, por um lado sedutor e propiciador dos meios digitais e por outro de inquietação com os dados inseridos para navegação virtual, o usuário deve procurar outras formas de resguardar sua individualidade ou seus dados, se é que é factível, com os algoritmos constantemente presentes na tecnologia.

Contudo, a própria pressão dos usuários/consumidores não realizando compras ou não utilizando tais serviços virtuais de determinadas empresas, podem gerar mecanismo de ações, por parte das empresas, para melhorar suas entregas com mais confiabilidade e segurança na utilização dos dados pessoais.

Entretanto, a própria demanda crítica dos usuários abstendo-se de adquirir ou não utilizando tais serviços virtuais de determinadas empresas, têm o poder de impulsionar mecanismos de iniciativa, por parte das empresas, visando otimizar suas entregas com maior confiabilidade e salvaguardar a utilização dos dados pessoais.

REFERÊNCIAS

BRASIL. **Lei nº 8078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. [S. l.], 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 7 dez. 2021.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. [S. l.], 10 fev. 2022. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 9 jul. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 dez. 2021.

BOISSAY, Frederic; EHLERS, Torsten; GAMBACORTA, Leonardo; SHIN, Hyun Song. Big Techs in Finance: On the New Nexus Between Data Privacy and Competition. **The Palgrave Handbook of Technological Finance**, [*s. l.*], e-book pgs 855–875.. DOI https://doi.org/10.1007/978-3-030-65117-6_31. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-65117-6_31. Acesso em: 28 jun. 2023.

BRASIL. **Medida Cautelar na Ação Direta de Inconstitucionalidade nº ADI 6387, de 7 de maio de 2020**. Medida Cautelar em Ação Direta de Inconstitucionalidade. Referendo. Medida Provisória nº 954/2020. Emergência de saúde pública de Importância internacional decorrente do novo Coronavírus (covid-19). Compartilhamento de dados Dos usuários do serviço telefônico fixo comutado e Do serviço móvel pessoal, pelas empresas Prestadoras, com o instituto brasileiro de geografia E estatística. Fumus boni juris. Periculum in mora. Deferimento. [S. l.], 7 maio 2020. Disponível em: http://www.stf.jus.br/portal/autenticacao/autenticarDocumento.asp sob o código 8505-884E-09E4-E6DB. Acesso em: 9 jul. 2023.

CISCO (Brasil). **Criação de confiança do consumidor com transparência e controle CISCO 2021** |: Pesquisa de privacidade do consumidor. *In*: CISCO (Brasil). Criação de confiança do consumidor com transparência e controle CISCO 2021 | : Pesquisa de privacidade do consumidor. [*S. l.*], 1 jun. 2020. Disponível em: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/cisco-cybersecurity-series-2021-cps.pdf. Acesso em: 5 jul. 2023.

DAHLE DE ALMEIDA, Siderly do Carmo; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas da Ciência da Informação** , https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/, v. 27, n. 3, p. 26-45, 2 dez. 2022. DOI https://doi.org/10.1590/1981-5344/25905. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/. Acesso em: 5 jul. 2023.

FERNANDES, Marcelo Eloy; NUZZI, Ana Paula Eloy. Fundamentos da Lei Geral de Proteção de Dados (LGPD): Uma revisão narrativa. **Research, Society and Development**, https://rsdjournal.org/index.php/rsd/article/view/34247/29094, v. 11, ed. 12, 15 set. 2022. DOI http://dx.doi.org/10.33448/rsd-v11i12.342471.

Disponível em: https://rsdjournal.org/index.php/rsd/article/view/34247/29094. Acesso em: 5 jul. 2023.

FOLLONE, R. A.; SIMÃO FILHO, A. A Conexão da LGPD e CDC: A Proteção de Dados Pessoais nas Relações Consumeritas e a sua Concretização como Direito Fundamental.. **Anais do Congresso Brasileiro de Processo Coletivo e Cidadania**, [S. l.], n. 8, p. 937–959, 2020. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/2112. Acesso em: 6 jul. 2023.

GARROTE, Marina Gonçalves; PASCHOALINI, Nathan; MEIRA, Marina; BIONI, Bruno R. ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais: Análise dos primeiros movimentos da Autoridade Nacional de Proteção de Dados. **JOTA**, [*S. l.*], p. 1, 13 jul. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 6 jul. 2023.

LAW, Thomas. A Lei Geral de Proteção de Dados: uma análise comparada ao novo modelo chinês. In: LAW, Thomas. **A Lei Geral de Proteção de Dados: uma análise comparada ao novo modelo chinês.** Orientador: Maria Eugênia Finkelstein. 2020. Tese de Doutorado (Doutor em Direito Comercial) - Pontifícia Universidade Católica de São Paulo, [S. l.], 2020. DOI https://tede2.pucsp.br/handle/handle/23402. Disponível em: https://tede2.pucsp.br/bitstream/handle/23402/2/Thomas%20Law.pdf. Acesso em: 3 jul. 2023.

MACÊDO, André Batisti; SCHMIDT, Roberto Eurico. O Regime de Responsabilidade Civil Aplicado na Lei Geral de Proteção de Dados **RUNA - Repositório Universitário da Ânima** , [s. l.], 14 jun. 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/25299. Acesso em: 3 jul. 2023.

NEGRISOLI FERNANDEZ POLETTINI, Márcia Regina. A LGPD e os impactos nas relações de consumo. **Revista JurisFIB,** [s. l.], v. 10, ed. 2, 5 dez. 2020. Disponível em: https://revistas.fibbauru.br/jurisfib/article/view/471. Acesso em: 6 jul. 2023.

RESENDE, Antônio Donizetti; BRASIL, Deilton Ribeiro. Impactos e consequências da globalização nos direitos fundamentais, no constitucionalismo ena soberania dos estados. **Caderno de Relações Internacionais**, [S. l.], p. 1-36, 5 fev. 2020. DOI https://doi.org/10.22293/2179-1376.v10i19.1175. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/relacoesinternacionais/article/view/1175/907. Acesso em: 28 jun. 2023.

SCHWAB, Klaus. A Quarta Revolução Industrial. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SEMINÁRIO WEBINAR DO IDP, 2021. Tema: **"Vazamento de Dados e o regime de prevenção e reparação de danos no CDC e na LGPD"** Disponível em: https://www.youtube.com/watch?v=KKL6By2iatU Acesso em: 06 dez. 2021.

VAINZOF, Rony. A LGPD e o Relatório de Impacto à Proteção de Dados Pessoais. **Revista Consultor Jurídico, 2021**. Disponível em: https://www.conjur.com.br/2021-jun-28/rony-vainzof-lgpd-relatorio-impacto-protecao-dados Acesso em: 04 dez. 2021. 085834/publico/11550929DIO.pdf. Acesso em: 3 jul. 2023.

VERBICARO, Dennis; CALANDRINI, Jorge. A proteção da confiança do consumidor e a base do legítimo interesse na lei 13.709/2018 (lei geral de proteção de dados pessoais). **Revista de Direito do Consumidor**, Brasília, v. 31, n. 139, p. 73-99, 2022. Disponível em: https://www.tjdft.jus.br/institucional/biblioteca/conteudo-revistas-juridicas/revista-de-direito-do-consumidor/2022-v-31-n-139-jan-fev. Acesso em: 5 jul. 2023.

ZANETTI DE OLIVEIRA, Dânton Hilário; ALMENDRA FREITAS, Cinthia Obladen. A responsabilidade civil do fornecedor quanto aos dados pessoais do consumidor: diálogo das fontes entre cdc e lgpd. **Revista de Direito do Consumidor**, [S. l.], v. 138, p. 225-242, 2021. Revista de Direito do Consumidor | vol. 138/2021 | p. 225 - 242 | Nov - Dez / 2021 DTR\2021\47772.

ZOCATELLI QUEIROZ, Renata Capriollo. A proteção de dados pessoais: A LGPD e a disciplina jurídica do Encarregado de Proteção de Dados Pessoais. In: ZOCATELLI QUEIROZ, Renata Capriollo. **A proteção de dados pessoais: A LGPD e a disciplina jurídica do Encarregado de Proteção de Dados Pessoais**. Orientador: Dr. Álvaro Villaça Azevedo. 2023. Tese de Doutorado (Doutor em Direito Civil) - Universidade de São Paulo - Faculdade de Direito, [S. l.], 2021. DOI https://doi.org/10.11606/T.2.2021.tde-23082022-085834. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2131/tde-23082022-.