

JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL ISSN: 2526-4281 - QUALIS B1



LEI GERAL DE PROTEÇÃO DE DADOS E A RELAÇÃO CONSUMERISTA

GENERAL DATA PROTECTION LAW AND THE CONSUMER RELATIONSHIP

Larissa Cristina Santos RODRIGUES
Faculdade Católica Dom Orione (FCDO)
E-mail: larissacristinasr@gmail.com

Lillian Fonseca FERNANDES
Faculdade Católica Dom Orione (FCDO)
E-mail: lillian@catolicaorione.edu.br



RESUMO

Este estudo tem como objetivo destrinchar o amparo da Lei Geral de Proteção de Dados em relação ao vazamento de dados no que diz respeito ao direito do consumidor e o entendimento quanto ao cabimento de indenização por danos morais, em detrimento dos princípios que fundam o direito do consumidor. O direito à privacidade refere-se ao conceito de que os dados pessoais de uma pessoa estão protegidos do escrutínio público. O direito à privacidade significa o direito à autonomia pessoal ou o direito de escolher se deseja realizar certas ações ou ter certas experiências. Portanto, uma pessoa tem o direito de determinar que tipos de informações sobre ela são coletadas e como essas informações são usadas. Deste modo, o direito à privacidade levanta a questão de por que a privacidade deve ser valorizada e protegida. Com isso em mente, os governos em todo o mundo devem tomar medidas concretas para lidar com as ameaças existentes e emergentes para afirmar e proteger o direito humano básico à privacidade, à medida que os atores governamentais e corporativos continuam a maximizar a coleta e retenção de dados. Portanto, a Lei básica de Proteção de Dados foi introduzida para garantir o direito à privacidade na era digital.

Palavras-chave: Direito do consumidor. Lei Geral de Proteção de Dados. Dados Pessoais.

ABSTRACT

This study aims to unravel the support of the General Data Protection Law in relation to data leakage with regard to consumer rights and the understanding of the appropriateness of compensation for moral damages, to the detriment of the principles that underlie the right of consumer. The right to privacy refers to the concept that a person's personal data is protected from public scrutiny. The right to privacy means the right to personal autonomy or the right to choose whether to perform certain actions or have certain experiences. Therefore, a person has the right to determine what types of information about him or her is collected and how that information is used. Therefore, the right to privacy raises the question of why privacy should be valued and protected. With this in mind, governments around the world must take concrete steps to address existing and emerging threats to assert and protect the basic human right to privacy, as government and corporate actors continue to maximize the collection and retention of Dice. Therefore, the Basic Data Protection Law was introduced to guarantee the right to privacy in the digital age.

Larissa Cristina Santos RODRIGUES; Lillian Fonseca FERNANDES. LEI GERAL DE PROTEÇÃO DE DADOS E A RELAÇÃO CONSUMERISTA. JNT- Facit Business and Technology Journal. QUALIS B1. 2022. FLUXO CONTÍNUO. Ed. 35. V. 1. Págs. 269-283. ISSN: 2526-4281 <http://revistas.faculdefacit.edu.br>. E-mail: jnt@faculdefacit.edu.br.

Keywords: Consumer law. Privacy. General Data Protection Law. Privacy. Personal data.

INTRODUÇÃO

A presente pesquisa tem por tema a proteção de dados pessoais dos consumidores na internet, à luz do direito pátrio, em face da lei Geral de Proteção de Dados - LGPD criada em 2018, justificando-se pelo avanço da tecnologia de maneira acelerada nas últimas décadas, em consequência atinge uma quantidade muito ampla de pessoas que utilizam dela diariamente em seu cotidiano. Assim será realizada uma análise dos contornos jurídicos da Lei nº 13.709/18, sendo observado os momentos históricos anteriores a Lei e sua grande importância ao instituto da proteção de dados pessoais, acompanhando a evolução da legislação mundial.

Assim, o problema baseia-se na cessão de dados pessoais a aplicações na internet, rodeados de uma enorme base de informações em relação ao indivíduo, em que se indaga, qual o tipo de preocupação/risco com o uso das informações fornecidas às empresas? Há preocupação com os casos de vazamento de dados pessoais? Assim a importância de uma análise pormenorizada quanto a Lei nº 13.709/18, que veio representar uma grande conquista do ordenamento jurídico brasileiro, acompanhando a evolução legislativa mundial acerca da temática.

Diante desse contexto, verifica-se a necessidade do oferecimento ao usuário de informação necessária quanto ao tratamento de seus dados, bem como a garantia da segurança de suas informações pessoais, assim buscando o bem-estar da pessoa no mundo virtual, garantindo direitos fundamentais básicos.

De tal modo, o legislador brasileiro, na Constituição Federal de 1988, inseriu o direito à privacidade dentro do rol de direitos fundamentais, com a expressa previsão de resguardar ao direito à vida privada e à intimidade.

Pela análise das disposições constitucionais, passa a surgir outras normas a fim de colocar a proteção dos dados em suas previsões (implícita ou explicitamente), destacando-se, a Lei 8078/90, denominado de Código de Defesa do Consumidor. Assim, em conformidade com seu artigo 43, apresentam-se a proteção frente aos bancos de dados e cadastros dos consumidores, os quais o CDC observa como instrumentos amplos e capazes de absorver inúmeros dados, indo além de meras informações negativas que objetivassem a concessão de crédito, como muitos acreditavam.

Assim, pode-se verificar a importância da pesquisa visto que o conhecimento é cada vez mais disseminado e, de forma rápida, principalmente por meio da rede mundial de computadores, que possibilita a troca instantânea de informações, onde um novo modelo de sociedade baseada na tecnologia necessita de um amparo jurídico.

Diante do exposto, o objetivo deste estudo é de analisar o amparo da Lei Geral de Proteção de Dados, referente ao vazamento de dados, no que diz respeito ao direito do consumidor e o entendimento quanto ao cabimento de indenização por danos morais, em detrimento dos princípios que fundam o direito do consumidor. Já os objetivos específicos foram analisar a origem da proteção de dados, estudar a sua aplicação, e discutir acerca das suas penalidades quanto a violação.

Deste modo, foi realizada, por meio do procedimento de pesquisa bibliográfica, documental, legislações vigentes, e estudos de casos, utilizando o método descritivo e explicativo

ORIGEM DA PROTEÇÃO DE DADOS: PRINCÍPIOS E LEGISLAÇÃO

Para uma correta apreciação quanto à proteção de dados dos consumidores é imprescindível uma análise profunda de suas origens e alterações ao longo da história, dessa maneira se trata de grande relevância a compreensão do contexto ao qual se insere.

Os dados pessoais abordados no presente estudo constituem-se de certas especificações para serem caracterizados. A princípio, conforme Krieger (2019) termo “dado” representa uma informação antecipada de interpretação ou sem um processo de elaboração. Conforme Mendes (2014, p. 55), este termo pode estar associado à uma “informação em potencial”: o dado somente será transformado em informação após passar por um processamento.

Para Santos (2019, p. 5) “dados são valores numéricos que, quando devidamente estruturados e sistematizados, transformam-se em informações. Tais informações quando filtradas e agrupadas geram conhecimento sobre determinado objeto, pessoa ou grupo.”

A definição sobre dados pessoais foi abordada no Regulamento 2016/679 da União Europeia (*General Data Protection Regulation – GDPR*) em seu art. 4º, n. 1, que *in verbis* estipula:

«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via

eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

Portanto, compreende-se conforme os autores supracitados, que os dados pessoais se referem a uma série de informações, como dados cadastrais: nome, endereço, e-mail, endereço de IP, dados biométricos, de raça, saúde, dentre outros (BIONI, 2018).

Observa-se que inúmeros negócios são baseados em Termos de Uso, sendo escritos, na maior parte das vezes, com a intenção de não serem lidos pelos usuários, no entanto configuram o contrato, que a empresa permite a ampla coleta de dados, sendo que não estão necessariamente relacionados com o escopo daquele produto ou serviço ofertado (FRAZÃO et al, 2019).

Diante do exposto, vários ordenamentos jurídicos vêm considerando a proteção de dados pessoais como um dos pilares da dignidade da pessoa humana e para a tutela do direito fundamental à privacidade. (DONEDA, 2011). Neste sentido, no que diz respeito a legislação brasileira sobre privacidade dentro do rol de direitos fundamentais, o inciso X do artigo 5º da Constituição Federal de 1988.

Assim, a proteção aos dados pessoais é originada do direito à vida privada e o direito à intimidade. Ademais, a teoria dos direitos da personalidade deu início nos países de língua germânica, que se fundamentava na ideia de um direito subjetivo além dos direitos reais e pessoais (GUIDI, 2018).

Conforme nos explica Rodotá (2008, p. 92), “a privacidade na era da informação deverá ser definida pelo direito do sujeito de manter o controle sobre as próprias informações”. Nesse sentido, valorizam-se as escolhas pessoais, levando em conta o novo poder que o indivíduo possui sobre o tratamento de seus dados.

A temática voltada para a proteção de dados já era indiretamente tratada em legislações esparsas como o Código de Defesa do Consumidor e a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet. Entretanto, não havia regulamentação seria, que tratasse da proteção de dados, colocando em evidência a importância de uma legislação específica (MENDES, 2014).

Nesta sucessão temporal, outros países instituíram suas leis. Assim, a União Europeia, com históricos na legislação com a Convenção 108 e a Diretiva 95/46, implementou uma legislação de proteção de dados extensiva que regulamentou o tratamento de dados pelos seus signatários, qual seja, a *General Data Protection Regulation (GDPR)* (LUGATI; ALMEIDA, 2020).

Importante ressaltar que, apesar da não criação de uma lei específica, este assunto foi tratado em leis internacionais e também nacionais, sendo possível citar a Declaração Americana dos Direitos e Deveres do Homem (1948), a Declaração Universal dos Direitos do Homem, O Pacto Internacional sobre Direitos Civis e Políticos (reconhecido no Brasil em 1992), a Convenção Americana Sobre Direitos Humanos (Pacto de São Jose da Costa Rica, sendo legitimado no Brasil em 1992) (GUERRA, 2014).

A discussão sobre a proteção de dados pessoais e sua possível regulamentação percorreu diversas fases, associando sua relevância e necessidade ao conceito de direito à privacidade, garantido pelo Estado dentro da esfera individual de cada um. Deste modo, o debate sobre o que atualmente se define como privacidade, teve origem a partir do momento em que as tecnologias se tornaram invasivas, abrindo espaço para a divulgação de informações da esfera privada do indivíduo (LUGATI; ALMEIDA, 2020).

Conforme Mendes (2014) um dos pontos cruciais para esse debate foi o artigo “*the right of privacy*”, escrito por Warren e Brandeis. Cancelier (2017) comenta que, o conceito de privacidade, até então, era representado pelo jurista Thomas McIntyre que salientou em 1888 a expressão “*right to be let alone*”, que traduzido para o português significa “o direito de estar só”. Antes disso, a questão somente havia sido tutelada em sede jurisprudencial, através do recurso à violação do direito de privacidade privada, à violação da confidencialidade, da confiança, ou de uma obrigação contratual.

Mendes (2014) afirma que desde de 1970 pode-se observar decisões jurídicas e legislações afirmando que os dados pessoais são uma projeção da personalidade do indivíduo e por isso são hábeis a receber tutela jurídica. Ao abordar o contexto histórico e evolutivo, faz-se necessário direcionar o contexto para o território brasileiro, foco principal do presente estudo, que conforme Lugati e Almeida (2020) ao tratar da proteção de dados o Brasil carrega uma série de legislações genéricas, insuficientes e criadas tardiamente, quando comparado a outros países (LUGATI; ALMEIDA, 2020).

O Brasil demonstrou argumentos sobre a proteção de dados através da previsão do Habeas Data no art. 5º, inc. LXXII da Constituição Federal. Em ordem cronológica, outras normas tratavam sobre a proteção de dados, como o Código de Defesa do Consumidor, em 1990. Além disso, exige-se que o consumidor seja comunicado sobre a abertura de cadastros, ficha, registro e dados pessoais e de consumo (LUGATI; ALMEIDA, 2020).

No que diz respeito a relação de consumo é, basicamente, o vínculo jurídico, que há a presença de três elementos, sendo eles; o Consumidor, fornecedor e um produto ou

serviço assim, formando pressuposto lógico do negócio jurídico celebrado de acordo com as normas da Código de Defesa do Consumidor (Lei 8.078/90) (GUERRA, 2014).

No que concerne a responsabilidade de consumo na ótica do direito do consumidor, o legislador criou um código próprio visando garantir ainda mais a eficácia na proteção dos consumidores (Lei n.8.078/1990), trazendo em seu rol de artigos princípios visando maior aplicabilidade nas relações de consumo (GUIDI, 2018).

LGPD E A APLICAÇÃO A RELAÇÃO CONSUMERISTA: DIREITO À INFORMAÇÃO

Exposto o desdobramento do uso de dados pessoais no tópico anterior, será analisado a inclinação dos ordenamentos jurídicos no desenvolvimento de normas autônomas para a proteção da matéria, considerando a criação de um direito fundamental à proteção de dados. Sendo assim, a seguir será feita uma análise da Lei Geral de Proteção de Dados brasileira e seus principais pontos.

A Constituição Federal de 1988 era a principal resposta jurídica aos problemas que surgiam nos últimos anos, relacionados ao cenário da crescente hiper conectividade. Ainda que o constituinte originário não tivesse a possibilidade de prever, na década de 80, os riscos que envolvem a proteção de dados dos dias de hoje, o artigo 5º, inciso X, da CF/88 já trazia a previsão da inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, em que garantia o direito de “indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Nesse aspecto, também se aplicavam outros diplomas ainda vigentes, como o Código Civil, dispendo, sobre a proteção à personalidade, imagem e intimidade, a Lei de Acesso à Informação (LAI), o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet (MCI), a Lei de Cadastro Positivo e a Lei de delitos informáticos (BLUM, 2018).

O CDC define quais são os direitos básicos do consumidor e as práticas comerciais utilizadas para a captura de dados, sendo que algumas já poderiam ser consideradas como abusivas diante desse contexto. Assim, o consumidor que com seus dados eventualmente coletados pelo fornecedor sem ter percebido o fato e sem concordar com essa conduta, já se encontrava em situação de vulnerabilidade técnica, possibilitando ensejar manifestação de vontade viciada, visto que não lhe foram de maneira correta informadas as características essenciais do serviço (LUGATI; ALMEIDA, 2020).

Então, finalmente, em 10 de julho de 2018, o plenário do Senado Federal aprovou o Projeto de Lei da Câmara nº 53/2018, que altera o artigo 7º, inciso X e o artigo 16, inciso

II, do Marco Civil da Internet, a fim de disciplinar a proteção dos dados pessoais no Brasil e definir as situações as quais estes poderão ser coletados e tratados, tanto por empresas quanto pelo Poder Público (FRAZÃO et al, 2019).

Unificando esses assuntos em 65 artigos, a Lei 13.709/18 (Lei Geral de Proteção de Dados – “LGPD”) veio estabelecer uma gama de restrições para instituições privadas e públicas que armazenem dados de internautas, consumidores que são partes em um contrato, usuários de serviços públicos ou alvos de políticas públicas. Dessa forma, a nova lei busca promover a necessária proteção aos direitos fundamentais da liberdade e privacidade dos indivíduos (MONTEIRO, 2018).

A proteção dos dados pessoais, que pode passar a ser um direito garantido constitucionalmente, noutra medida, é mais ampla, implicando a proteção da intimidade, da privacidade e a garantia de que os dados pessoais gerados serão tratados de acordo com a mesma legislação de proteção.

Portanto, a configuração da sociedade neste século expressa claramente o contexto de uma sociedade vista como informatizada, fruto da revolução a partir dos efeitos da revolução tecnológica, que por sua vez é contínua, abrangente e complexa. Posto isto, este cenário de convergência digital tem levado à criação de novos dispositivos, bem como de novas formas de comunicação e novas plataformas de produção de dados, dando origem a novos canais baseados na associação de diferentes mecanismos de comunicação (GUIDI, 2018).

A Lei Geral de Proteção de Dados (LGPD) pode ser resumida como uma nova lei que obriga as organizações públicas e privadas a cumprir os padrões de segurança para prevenir furto, vazamento e venda ilegal de informações.

Na prática, trata-se da Lei nº 13.709, de 1 de agosto de 2018. Inclui o tratamento de dados pessoais, inclusive em meio digital, por pessoas físicas e jurídicas de direito público ou privado.

LGPD E ANÁLISE DE CASOS PRÁTICOS DE VAZAMENTO DE DADOS E SUAS CONSEQUÊNCIAS AO CONSUMIDOR

Na atualidade podem ser observadas situações de maneira inédita na história do mundo, contudo, é necessário se alertar para a necessidade de se lidar com suas consequências. Pois, as facilidades tecnológicas e os novos meios de comunicação e relações sociais também podem trazer suas facetas nocivas.

Devido a toda essa revolução tecnológica observa-se, portanto, uma sociedade diferente, se movendo ao redor das informações que a circulam. Pode-se dizer que fator decisivo da sociedade da informação é, de fato, o advento do computador. Instaurando, por consequência, a economia do imaterial, vindo a substituir as variáveis centrais anteriores, como o trabalho e o capital, por informação e conhecimento (GONÇALVES, 2003).

Observa-se como principal resultado da internet e do computador, a globalização e uma intensa alteração na dinâmica da vida em sociedade. Todos precisaram se ajustar a essa nova realidade, tanto governo, empresa e os próprios cidadãos (MARINELI, 2018). Neste contexto, a internet, por meio de equipamentos tecnológicos facilita situações anteriormente inimagináveis, entretanto, os novos meios de comunicação e relações sociais também podem trazer suas facetas nocivas (FRAZÃO et al, 2019).

A constante progressão dos níveis de conectividade ocasiona significativos desafios nos campos da segurança e privacidade dos indivíduos. Isso porque, quanto maior o número de objetos conectados, maior será o fluxo de informações produzidas por esses dispositivos relacionadas aos seus usuários (SILVEIRA, 2017).

Assim, os consumidores não possuem conhecimento claro da forma de coleta, compartilhamento e, ainda, do potencial uso por terceiros, desses dados pessoais. Ainda, falhas de segurança possibilitam possíveis ataques a servidores e dispositivos inteligentes com intenção de obtenção de informações, em virtude do seu alto valor de mercado (CASTELLS, 2016).

Observa-se que tal preocupação cresce substancialmente, devido a recentes episódios de vazamentos de dados pessoais, que envolvem os usuários do Facebook, Uber, Delta, Equifax, dentre outras empresas. Tais incidentes expuseram milhares de dados cadastrais de consumidores, como nomes, CPFs, endereços, números de cartões de crédito e até mesmo determinadas informações sensíveis (BLUM, 2018).

Assim, estudos revelam que os algoritmos são alimentados por informações pessoais indicando quais os desejos do consumidor, criando perfis de consumo dos usuários, para publicidade direcionada e venda desses dados pessoais para outras empresas. Nesse aspecto, a proteção da privacidade passa pelo grande risco de vazamento, visto que o conhecimento é cada vez mais disseminado, e de forma rápida, que possibilita a troca instantânea de informações.

Privacidade é um termo que evolui a cada momento, principalmente na Era da Informação. Inúmeros conceitos e frases dentro de contextos históricos definiram a necessidade de privacidade até chegar nas próprias leis utilizadas no ordenamento jurídico

brasileiro que a tornou um direito fundamental. Os dados de consumidores que são influenciados por publicidade online das empresas são um mercado enorme e a perda de privacidade é o preço que os consumidores têm que pagar pelos serviços gratuitos que eles utilizam (SILVEIRA, 2017).

Desde o advento do Regulamento 2016/679 da União Europeia os termos “*privacy by design and by default*”, traduzidos “desde a concessão e por defeito”, são trazidos por juristas, profissionais da segurança da informação e executivos de grandes empresas com o intuito de explicar a necessidade de privacidade atual ligada a nova Lei Geral de Proteção de Dados (LGPD). Diante dessa necessidade de proteção de dados e garantir o direito fundamental à privacidade, segundo o art. 46, §2º da LGPD: “Deverão ser observadas medidas técnicas e administrativas para a concepção de produtos ou serviços até a sua execução.” (GROSSI, 2020)

No 14, §3º, II a única falha do consumidor deve ser provada. A hipótese de que a instituição financeira permite ou ignora a perda de dados pessoais de seus clientes é ilegal e, portanto, cria oportunidades para ações ilegais de terceiros. Com o advento das redes sociais, compartilhar o estilo de vida é uma constante na sociedade atual. A partir daí, essa fonte contínua de informações pessoais (a mera exposição da vida privada) é um recurso valioso para as empresas identificarem formas mais assertivas de divulgação e desenvolvimento de produtos e serviços (RAPÔSO, 2019).

Porém, esse movimento gera conflitos causados pela falta de privacidade, ponto em que as leis LGPD e o Direito do Consumidor (CDC) são cumpridas e garantidas pela primeira vez ao titular o direito de consentimento para uso dos dados pessoais. De fato, tanto o artigo 43 do CDC quanto o artigo 7º da LGPD estipulam a necessidade de notificação ao consumidor da coleta de dados (MONTEIRO, 2018).

No que diz respeito à relação entre LGPD e Direito do Consumidor, outro ponto crítico presente em ambas as legislações é a segurança da informação. Escândalos de perda de dados e ameaças cibernéticas sofisticadas, por exemplo, exigem proteção à vida e à saúde contra os riscos de produtos e serviços, princípios de informação e transparência tão onerosos para os direitos do consumidor, já estabelecidos no CDC (GROSSI, 2020).

Para exemplificar a prática sobre o risco constante de vazamento de dados, que pode ocorrer em pequenos e grandes negócios, é possível analisar alguns casos que já foram notificados que não envolve empresas multimilionárias, como Google ou Facebook, além disso, não gerou repercussão midiática como em outras situações, entretanto, se enquadra na aplicação da Lei Geral de Proteção de Dados brasileira.

CASO 1 - Vazamento de compra de remédio controlado por funcionário da farmácia via WhatsApp:

O consumidor do medicamento controlado foi reconhecido por um dos atendentes do estabelecimento farmacêutico. Este se beneficiou da situação para tirar uma foto do receituário médico e encaminhou no grupo do WhatsApp, no qual se encontrava demais pessoas que conheciam o consumidor. O dado pessoal espalhado é considerado um dado sensível por lei, sendo necessário um maior rigor em seu tratamento. **O cliente que teve seu direito lesado procurou um advogado e deu início a uma ação.** Com o treinamento ideal dos funcionários e a conscientização acerca do que dispõe a nova normativa brasileira sobre a proteção de dados pessoais, tal ocorrido poderia ter sido evitado (EJUR, 2020).

A Lei Geral de Proteção de Dados Pessoais - LGPD (Lei 13.107), de 14 de agosto de 2018, regulamenta o tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, em qualquer meio, com a finalidade de oferecer ampla proteção aos direitos e liberdades fundamentais dos indivíduos, assegurando, dentre outros, o direito à privacidade e ao livre desenvolvimento da personalidade humana.

CASO 2 - Vazamento de atestado médico indicando que o funcionário era portador de HIV pelo RH da empresa:

A impressora utilizada pelo setor de recursos humanos era compartilhada com demais setores da empresa, mesmo o primeiro setor lidando com dados pessoais que não poderiam ser compartilhados com demais funcionários da organização. Diante deste equívoco, o atestado médico de um dos colaboradores, no qual constava que este era portador do vírus HIV, foi visto por um de seus colegas de trabalho e a informação foi vazada, interferindo na interação social e, conseqüentemente, laboral do funcionário que sua informação pessoal espalhada. **Com o mapeamento de dados realizado em cada setor da empresa, um Programa de Conformidade à LGPD poderia ter mitigado tal risco e esta situação poderia não ter ocorrido (EJUR, 2020).**

A regulamentação do tratamento dos dados visa coibir seu uso indevido, garantindo maior segurança aos seus titulares. Quando ocorre o vazamento ou utilização indevida das informações pessoais, os prejuízos podem ser descomunais.

Nesse sentido, vale lembrar o escândalo envolvendo a coleta ilegal de dados pessoais de mais de 87 milhões de usuários do Facebook, realizada pela empresa Cambridge Analytica, enquanto trabalhou na campanha eleitoral do ex-presidente Donald Trump e sua influência no resultado do pleito. (RAPÔSO, 2019)

Ademais os grandes escândalos envolvendo vazamento de dados, é recorrente em vários países como observado, visto a vastas expansões da tecnologia e seus termos de

aceites nas captações de dados que estão sendo canalizados para grandes empresas, assim, com o intuito de trazer maior proteção aos usuários, a LGPD está trazendo consigo regras as quais empresas devem observar (GROSSI, 2020).

Portanto, a proteção de dados é, obviamente, indispensável. Esta necessidade já foi reforçada pelo Decreto 7.962/13 Lei do Comércio Eletrônico), que no seu artigo 4º trata dos mecanismos de segurança para o pagamento e tratamento dos dados dos consumidores. Para seguir esses princípios, o Decreto 2.181/97 prevê a criação do Sistema Nacional de Defesa do Consumidor, que geralmente rege o funcionamento da Fundação PROCON de Defesa do Consumidor, cujas unidades atuam em praticamente todas as comunidades brasileiras.

Neste contexto, a LGPD alarga a questão da segurança e reclama técnicas administrativas que garantam a proteção dos dados pessoais e que sejam implementadas por unidades administrativas e especializadas sob a responsabilidade da autoridade nacional de proteção de dados (ANPD).

LGPD E AS PENALIDADES QUANTO A VIOLAÇÃO DA LEI

O progresso tecnológico criou uma situação de grande tensão e incompatibilidade entre o direito à privacidade. Este desenvolvimento requer repensar o conteúdo deste direito. Portanto, esta seção trata do direito à privacidade, especialmente no que diz respeito à proteção de dados pessoais sob a LGPD e as respectivas penalidades em casos de violação da lei.

Desde a promulgação da Lei 13.709 / 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD), a sociedade brasileira e a comunidade jurídica, de forma consistente, têm se envolvido fortemente no debate sobre a proteção e defesa de dados pessoais, embora este tema seja não é novo e contém uma análise complexa dos novos modelos de economia de rede insurgente (BLUM, 2018).

Porém, e apesar de o chamado LGPD não proteger apenas os ativos digitais, a relevância das notícias e os escândalos de exposição massiva e indevida de dados na rede ganham cada vez mais importância. Embora a Constituição Federal de 1988 ainda não preveja especificamente a proteção e defesa de dados, reconhece-se que isso pode ser inferido de uma série de dispositivos da Carta Magna (DONEDA, 2014).

Na contestação de que esses direitos se somam também à proteção e defesa dos consumidores através do diálogo de fontes, bem como observando a mesma regra para a aplicabilidade (infra) constitucional nas relações com os consumidores, a existência este

elemento essencial das regras, sem dúvida, irradiam eficiência e força para lidar com vazamentos de dados (GROSSI, 2020).

Em vez disso, pode-se dizer que a análise do passivo deve ser avaliada caso a caso, no caso de incidentes evidentes. Se, apesar da ocorrência do vazamento em si, o vazamento viola os princípios básicos de integridade e confidencialidade que as políticas e padrões de segurança da informação devem orientar, então tais eventos afetarão seriamente não apenas a integridade dos dados do consumidor. Mas também a finalidade, a segurança e qualidade do processamento de dados essenciais, princípios básicos a serem observados, especialmente se os ativos forem dados sensíveis (artigos 5º, II e 11 a 13 da Lei 13.709 / 2018).

As comunicações sobre vazamento de dados são fornecidas na arte. O artigo 48 da lei acima também pode ser responsabilizado sempre que a violação comprometer a integridade, disponibilidade e confidencialidade dos dados (BIONI, 2018).

O artigo 42 da LGPD é muito semelhante à cláusula de responsabilidade geral deste artigo. Artigo 186 do Código Civil Brasileiro. É de responsabilidade da pessoa responsável pelos danos repará-lo. Os operadores têm uma obrigação comum, mas somente se o operador não cumprir as regras de proteção de dados ou não cumprir a decisão do controlador (GROSSI, 2020).

A redação do artigo 43 da LGPD é semelhante à redação da responsabilidade civil por produtos ou serviços nos artigos 12 e 14 da Lei de Proteção ao Consumidor. Seção de arte. Art. 43 não descarta a responsabilidade do agente na ausência de litígios, se o ato é ilegal ou se o dano é causado pela absoluta falta de proprietários de dados ou de terceiros (RAPÔSO, 2019).

Por outro lado, o artigo 44 do GPA determina quando atos ilegais ocorrerão para determinar a responsabilidade. Se a empresa deixar de cumprir a lei ou a garantia fornecida falhar, as ações da empresa poderão ser consideradas responsabilidade civil se a garantia for insuficiente.

O LGPD não possui uma medida do valor da compensação. Para a Cambridge Analytica, o Escritório do Information Commissioner (ICO-UK) aplicou certos critérios para avaliar uma multa de £ 500.000. Como os seguintes critérios: (i) afetando um grande número de pessoas, (ii) e o número de cidadãos que estão seriamente ameaçados. No final do relatório, analisamos a lentidão da sociedade de 2015 a 2018 e tomamos medidas eficazes para lidar com certas coisas. Os reguladores brasileiros ou o judiciário devem usar todos esses critérios ao avaliar as obrigações de pagamento (GUIDI, 2018).

No último caso, foi relatada uma pesquisa do MPDFT Boa Vista, que supostamente vazou o banco de dados. Os membros levaram essa base ao seu departamento interno de segurança e análise, descreveram as etapas e descobriram uma vulnerabilidade específica do aplicativo; o banco de dados estava corrompido; mas esse é um banco de dados de teste sem dados armazenados.

Portanto, em termos de responsabilidades de proteção de dados, a melhor solução é encontrar um equilíbrio entre três fatores: empresários (uso legal e responsável dos dados para gerar desenvolvimento econômico sustentável), indivíduos (direitos básicos são garantidos em outros aspectos, existem muito poucos), Controle de personalidade e aconselhamento (haverá boas oportunidades de carreira aqui e nos próximos anos) (GROSSI, 2020).

Se um empreendedor quiser usar os dados da sua empresa, use-os de maneira responsável, para que os direitos de todos sejam respeitados, porque a lei garante e reflete sua personalidade. Portanto, mesmo que não tenhamos controle sobre todos os dados, podemos pelo menos interferir na maneira como os dados são colocados, solicitando ao controlador e pedindo para apagar, se necessário.

CONSIDERAÇÕES FINAIS

A inovação de mercado, combinada com a tecnologia da informação, revela o valor dos dados pessoais e mostra a vulnerabilidade da privacidade pessoal no contexto da inserção de dados pessoais no mundo das commodities. Demonstra ainda os mecanismos de privacidade e proteção de dados pessoais, bem como a utilização dos dados pessoais disponibilizados pela LGPD, com enfoque no intercâmbio de dados pessoais, demonstrando que o direito à privacidade é superado por interesses econômicos.

O direito à privacidade oferece proteção nas relações com outras pessoas e com instituições nas quais a realização e o desenvolvimento da identidade pessoal podem ser alcançados. O poder normativo dessa abordagem pode ser reforçado por uma elaboração mais explícita dos bens em jogo.

Na prática, grande parte das relações jurídicas que serão afetadas pela LGPD também serão influenciadas pela legislação de defesa do consumidor. É o caso das relações bancárias, seguros de saúde e serviços públicos, entre outros.

Respeitar o cumprimento da LGPD e dos regulamentos nacionais, mais do que uma necessidade, será um dever de todas as pequenas, médias e grandes empresas. Um passo

positivo será mudar o tamanho de suas operações de dados, agregando valores de sustentabilidade da informação, ética e transparência ao negócio e à marca.

Para os usuários e clientes, isso significa o pleno exercício da autodeterminação informativa sobre o manuseio de seus dados pessoais. Em última análise, o Brasil ganhará confiabilidade internacional e mostrará a outras nações que trata os dados pessoais de seus cidadãos com seriedade e respeito.

Portanto, a LGPD regulamenta apenas o processamento de dados de pessoas identificadas ou identificáveis, mas se aplica às atividades de processamento dentro ou fora do Brasil. Portanto, a lei anterior foi criada para garantir o direito à privacidade na era digital.

REFERÊNCIAS

BIONI, B. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2018.

BLUM, R. **O direito à privacidade e à proteção dos dados do consumidor**. São Paulo, 2018

BRASIL. **Constituição: República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018

CASTELLS, M. **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade**. Rio de Janeiro: Jorge Zahar Ed., 2003. Tradução: Maria Luiza X. de A. Borges. A sociedade em rede. São Paulo, 2016.

CONSULTOR Jurídico. **O vazamento de dados de consumidores gera dano moral indenizável**. Disponível em: <<https://www.conjur.com.br/2019-dez-03/muriel-silvavazamento-dados-consumidores-gera-dano-moral>>. Acesso dia 22 de outubro de 2021.

DONEDA, D. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico. Joaçaba, 2011.

DONEDA, Danilo. **Proteger dados pessoais é um direito fundamental**. Revista de Direito Espacial 12/103. Direito Privado e Internet / Guilherme Magalhães Martins (Coordenador). - São Paulo: Atlas, 2014.

EJUR. **3 casos de vazamento de dados que lhe mostrarão que a Aplicação da LGPD não está tão distante da realidade do seu negócio**. Soluções Jurídicas, 2020. Disponível

Larissa Cristina Santos RODRIGUES; Lillian Fonseca FERNANDES. **LEI GERAL DE PROTEÇÃO DE DADOS E A RELAÇÃO CONSUMERISTA**. JNT- Facit Business and Technology Journal. QUALIS B1. 2022. FLUXO CONTÍNUO. Ed. 35. V. 1. Págs. 269-283. ISSN: 2526-4281 <http://revistas.faculdefacit.edu.br>. E-mail: jnt@faculdefacit.edu.br.

em < <https://ejur.com.br/blog/3-casos-de-vazamento-de-dados-que-mostram-a-aplicacao-da-igpd/> >. Acesso em: 11 out. 2021

FRAZÃO, Ana.; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. Thomson Reuters Brasil, 2019.

GONÇALVES, V. **Marco civil da internet comentado**. São Paulo, 2017.

GROSSI, Bernardo Menicucci. Uma análise preliminar da Lei 13.709/2018. In: GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados: uma análise preliminar da lei 13.709/2018**. Porto Alegre: Fi, 2020.

GUIDI, G. **Privacidade em perspectivas: Modelos Regulatórios para Proteção de Dados Pessoais**. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro, 2018.

283

GUERRA, G. **Marco Civil da Internet: Direito à inviolabilidade e ao sigilo de comunicações privadas armazenadas: um grande salto rumo à proteção judicial da privacidade na rede**. Organizadores: George Salomão e Ronaldo Lemos. São Paulo, 2014.

LUGATI, Lys Nunes; DE ALMEIDA, Juliana Evangelista. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. Revista de Direito, v. 12, n. 02, p. 01-33, 2020.

MAGRANI, E. **A internet das coisas**. Rio de Janeiro, 2018.

MARINELLI, M. **Privacidade e redes sociais virtuais**. Rio de Janeiro: Lumen Juris, 2017.

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

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil**. Artigo estratégico, v. 39, p. 1-14, 2018.

RAPÔSO, Cláudio Filipe Lima et al. **LGPD-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática**. RACE-Revista de Administração do Cesmac, v. 4, p. 58-67, 2019.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008

SANTOS, Dhiulia de Oliveira. **A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais (Lei n. 13.709/2018)**. Artigo Científico (Bacharel em Direito) Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB), 2019.

SILVEIRA, S. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais**. São Paulo, 2017.

Larissa Cristina Santos RODRIGUES; Lillian Fonseca FERNANDES. **LEI GERAL DE PROTEÇÃO DE DADOS E A RELAÇÃO CONSUMERISTA**. JNT- Facit Business and Technology Journal. QUALIS B1. 2022. FLUXO CONTÍNUO. Ed. 35. V. 1. Págs. 269-283. ISSN: 2526-4281 <http://revistas.faculdefacit.edu.br>. E-mail: jnt@faculdefacit.edu.br.