doi.org/10.51891/rease.v10i6.14400

VAZAMENTO DE DADOS PESSOAIS EM TEMPOS DE INFORMAÇÃO INSTANTÂNEA[1]

LEAKAGE OF PERSONAL DATA IN TIMES OF INSTANT INFORMATION

Italo Kelson Pereira dos Santos[2]
Gisela Carvalho de Freitas[3]

RESUMO: No mundo interligado de hoje, os dados tornaram-se um ativo inestimável, alimentando a inovação e o crescimento económico. No entanto, este vasto tesouro de informações pessoais também levanta preocupações críticas em relação à privacidade e à proteção. Em resposta a essas preocupações crescentes, o Brasil promulgou a Lei Geral de Proteção de Dados (LGPD), também conhecida como Lei Geral de Proteção de Dados, em 2018. Esta legislação histórica visa salvaguardar os direitos e a privacidade dos indivíduos, ao mesmo tempo que promove uma abordagem responsável para práticas de manipulação de dados. Este artigo investiga o significado social da LGPD, examinando o seu papel na formação do cenário contemporâneo da proteção de dados. Através de uma análise abrangente de fontes bibliográficas e documentais, exploramos a era pré-LGPD, caracterizada por um vazio legislativo na proteção de dados. A introdução da LGPD marcou um ponto de inflexão, colocando todas as atividades de processamento de dados sob a alçada do arcabouço jurídico do país. O estudo ressalta a necessidade premente da LGPD, enfatizando o imenso valor econômico dos dados pessoais. Destaca a necessidade imperativa de proteger os titulares dos dados, garantindo que os seus direitos e privacidade não sejam violados. A LGPD surgiu como uma resposta oportuna aos desafios enfrentados por indivíduos e organizações no mundo digital. Promulgada em 2018, a LGPD entrou em vigor após um período de carência conhecido como vacatio legis. Este estudo investiga a evolução do impacto da LGPD na sociedade, avaliando sua eficácia na abordagem das preocupações que foi projetada para mitigar.

Palavras-Chave: Lei Geral de proteção de dados. Marco Civil da internet. Vazamento de dados. Lei de acesso à informação.

[1]Trabalho de Conclusão de Curso apresentado no Centro Universitário Santo Agostinho – (UNIFSA), Teresina-PI,

[2]Bacharelando do Curso de Direito do Centro Universitário Santo Agostinho (UNIFSA).
[3]Mestra em Direito - Universidade Católica de Brasília, UCB/DF, Orientadora e professora do Centro Universitário Santo Agostinho (UNIFSA).

ABSTRACT: In today's interconnected world, data has become an invaluable asset, fueling innovation and economic growth. However, this vast trove of personal information also raises critical privacy and security concerns. In response to these growing concerns, Brazil enacted the General Data Protection Law (LGPD), also known as the General Data Protection Law, in 2018. This landmark legislation aims to safeguard the rights and privacy of individuals, while also which promotes a responsible approach to data handling practices. This article investigates the social significance of the LGPD, examining its role in shaping the contemporary data protection landscape. Through a comprehensive analysis of bibliographic and documentary sources, we explored the pre-LGPD era, characterized by a legislative void in data protection. The introduction of the LGPD marked an inflection point, bringing all data processing activities under the purview of the country's legal framework. The study highlights the pressing need for LGPD, emphasizing the immense economic value of personal data. It highlights the imperative need to protect data subjects, ensuring that their rights and privacy are not violated. The LGPD emerged as a timely response to the challenges faced by individuals and organizations in the digital world. Enacted in 2018, the LGPD came into force after a grace period known as vacatio legis. This study investigates the evolution of the LGPD's impact on society, evaluating its effectiveness in addressing the concerns it was designed to mitigate.

Keywords: General data protection law. Marco Civil da Internet. Data leak. Access toinformationlaw.

1 INTRODUÇÃO

A era da informação instantânea, impulsionada pela internet e pelas tecnologias digitais, proporciona acesso rápido e fácil a um mundo de informações. No entanto, essa mesma conectividade torna os dados pessoais mais vulneráveis a vazamentos, que podem ter graves consequências para indivíduos e sociedades. Nesse contexto, a facilidade de acesso a dados pessoais, como: nome, endereço, CPF, número de telefone, e-mail, informações bancárias e até mesmo o acesso adados relacionados à saúde, tornou-seuma realidade em nosso dia a dia. Essa ubiquidade, por sua vez, aumenta a vulnerabilidade em relação a possibilidade de vazamento desses dados, que pode ocasionar graves consequências para indivíduos e para a sociedade como um todo.

Assim, e diante do cenário pós-pandemia, é essencial compreender como as rápidas e frequentes inovações tecnológicas têm moldado a sociedade, especialmente no campo da informação, afetando diretamente as relações interpessoais e a forma como vivemos.

Anteriormente, as atividades e interações eram predominantemente presenciais, hoje muitas migraram para o mundo virtual, alterando significativamente nossas dinâmicas sociais.Nesta nova configuração social, onde a troca de informações é instantânea e constante, os dados se tornaram o cerne de um gigantesco sistema econômico virtual. Em um ambiente em que as mídias digitais oferecem serviços aos usuários sem cobrar diretamente por eles, é importante perceber que a economia vai além do aparente "gratuito". A verdadeira moeda são os dados dos usuários, coletados muitas vezes involuntariamente e depois tratados e vendidos a terceiros, gerando grandes lucros impulsionados pelo mercado de publicidade direcionada.

Um exemplo disso são os *cookies*, ferramentas que rastreiam as atividades dos usuários na internet para personalizar anúncios e conteúdo. Isso cria um ambiente onde os usuários são constantemente monitorados, tendo seus dados coletados e armazenados para fins comerciais, sem estarem cientes disso.

Desta forma, é urgente a necessidade de regulamentações que protejam os dados pessoais, objetivando garantir a privacidade dos usuários. No Brasil, A repercussão de situações de vazamentos de dados ganha contornos jurídicos mais relevantes após a aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. Com a legislação, o Brasil passa a contar com um importante instrumento legal que pode atuar na promoção da defesa do cidadão em relações massificadas.

A pandemia acelerou essa transformação causada pela era da informação, destacando a importância da informação instantânea e da conectividade virtual. Atividades que antes eram realizadas pessoalmente, como compras, entretenimento e comunicação, agora são predominantemente virtuais. Isso significa que todas as interações online, desde uma simples pesquisa no Google até transações comerciais e interações em redes sociais, são registradas, analisadas e muitas vezes compartilhadas para além das fronteiras nacionais, seja por motivos comerciais ou políticos.

Diante desse contexto, é crucial que existam legislações específicas para proteger os dados pessoais, dada a rápida evolução tecnológica e o valor cada vez maior da informação. A globalização e a cultura da informação transformaram os dados em um ativo de grande relevância, conferindo poder àqueles que têm acesso a eles.

Para que se possa desenvolver esse trabalho, será necessário o estudo da jurisprudência brasileira, buscando uma compreensão de forma clara e objetiva de como o Direito à Proteção de Dadospassou a ser reconhecido como direito fundamental e qual foi a implicação dos avanços tecnológicos diante da necessidade de proteção aos dados pessoais dos cidadãos brasileiros.

Portanto, o presente artigo tem por intuito analisar as legislações existentes, como a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, avaliando a evolução e proteção aos direitos individuais em um mundo cada vez mais digitalizado e interconectado, bem como a relação das regulamentações com situações concretas de vazamento de dados pessoais.

Em um mundo cada vez mais tecnológico, onde a coleta e o tratamento de informações se tornam cada vez mais frequentes, a busca pela proteção aos dados pessoais assume um papel fundamental. Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD) surge como um marco regulatório crucial no Brasil, estabelecendo princípios e diretrizes para o tratamento de dados, desde a coleta, o compartilhamento, o armazenamento, o uso, até a eliminação de dados pessoais.

Compreender a LGPD em sua complexidade e abrangência exige um estudo aprofundado, que considere não apenas os aspectos técnicos e jurídicos da legislação brasileira, mas também as diversas perspectivas internacionais sobre a proteção de dados. É nesse cenário que o direito comparado se revela como uma ferramenta essencial para o pesquisador.

Através da análise comparativa da LGPD com legislações de outros países, como o Regulamento Europeu de Proteção de Dados (chamado de *General Data ProtectionRegulation(GDPR)*,editado em 2016), este estudo busca ampliar a compreensão da proteção de dados no Brasil, identificando similaridades e diferenças entre as diversas abordagens à proteção de dados, obtendo insights para a aplicação da legislação brasileira e contribuindo para o desenvolvimento da jurisprudência sobre o tema. Ao realizar um estudo comparativo, este trabalho pretende aprofundar o conhecimento sobre o direito à proteção de dados, oferecer subsídios para a sua aplicação prática e contribuir para o debate acadêmico sobre o tema no Brasil.

2 A tutela dos dados pessoais no ordenamento jurídico brasileiro

Sobre o tema da proteção de dados e da privacidade faz-se necessário citar como fontes principais a Declaração Universal dos Direitos Humanos (DUDH) e a Constituição da República Federativa do Brasil de 1988, constatando-se que, inicialmente, esses direitos eram pouco abordados e protegidos. Além desses dois diplomas legais, o Brasil também dispõe do Código de Defesa do Consumidor (CDC/1990), do Código Civil de 2002, do Marco Civil da Internet e algumas outras poucas legislações que abordam a matéria.

A Constituição Federal de 1988 (CRFB/88) coloca a privacidade e os dados pessoais no rol dos direitos e garantias fundamentais,sendo protegidos pela inviolabilidade e sigilo, entretanto,acompanhando as mudanças sociais, esse entendimento no Brasil tem passado por alterações.

O GDPR, *General Data ProtectionRegulation*,regulamento europeu que visa proteger os direitos dos cidadãos da União Europeia, é considerado uma norma importante em relação ao tratamento de dados pessoais, pois coloca a privacidade como núcleo valorativo deste direito, concentrando-se no indivíduo titular de dados.

Com a vigência da GDPR,em 2018, o Poder Legislativo brasileiro acelerou a edição da Lei nº 13.709, que foi sancionada em14 de agosto de 2018, intitulada Lei Geral de Proteção de Dados Pessoais (LGPD), já que a GDPR previu uma aplicação extraterritorial. Assim, o disposto na legislação europeia abrange não só asempresas europeias, mas todas as demais que tratam dados pessoais de indivíduos europeus, ou seja, todas asempresas queofertem bens ou serviços à União Europeia devem estar de acordocom o GPDR, de modo que as empresas de países que não dispõem de legislação especifica para a proteção de dados pessoaisficam impedidas de realizarem transações negociais.

Segundo a percepção de PINHEIRO, a implementação do GDPR influenciou a legislação de outros países na área de proteção de dados. Isso gerou um efeito cascata, pois países e empresas que desejavam manter relações comerciais com a União Europeia precisavam adotar legislações equivalentes ao GDPR. Caso contrário, poderiam enfrentar barreiras econômicas ou dificuldades para fazer negócios com os países da UE.

A Lei nº 13.709/2018 passou a regular as atividades relacionadas ao tratamento de dados pessoais no Brasil, e de acordo com Bioni (2019), a Lei Geral de Proteção de Dados

Pessoais (LGPD), incorpora a proteção ao consumidor e à dignidade da pessoa humana, princípios fundamentais estabelecidos pela Constituição Federal no contexto da ordem econômica. O direito à proteção dos dados pessoais evolui a partir do conceito de privacidade, o qual se tornou um direito fundamental na estrutura constitucional, adaptando-se às mudanças tecnológicas ao longo do tempo.

> As suas disposições preliminares enunciam que a disciplina da proteção de dados pessoais tem como objetivo proteger os direitos fundamentais e o livre desenvolvimento da personalidade (art.1º), repetindo-os como um dos seus fundamentos ao lado do desenvolvimento econômico-tecnológico e da inovação (art.2º). A LGPD estabelece, portanto, uma dialética normativa de conciliação entre todos esses elementos

No Brasil, a regulamentação relacionada à proteção de dados pessoais foi sendo gradualmente ampliada. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, representa o ápice dessa proteção. No entanto, mesmo antes da LGPD, o ordenamento jurídico brasileiro já contemplava alguns dispositivos nesse sentido.A Constituição Federal de 1988 já tratava da proteção da informação, garantindo a inviolabilidade da intimidade e da vida privada, o sigilo das comunicações e dos dados, bem como o sigilo da fonte. Esses princípios foram incorporados à legislação infraconstitucional, que passou a regular situações mais específicas, incluindo a proteção de dados pessoais.

Dessa forma, a legislação infraconstitucional brasileira inclui o Habeas Data, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação e o Marco Civil da Internet, todos com normas relacionadas ao tratamento de dados.Com a promulgação da LGPD, foram estabelecidas diretrizes e regras claras para o compartilhamento, coleta e tratamento de dados pessoais dos usuários, incentivando as empresas a desenvolverem infraestruturas eficazes para garantir a segurança da informação e a proteção dos dados dos usuários.

2.1 DESAFIOS CONTEMPORÂNEOS NA PROTEÇÃO DA PRIVACIDADE DE DADOS: Novas Fronteiras e Responsabilidades

No ordenamento jurídico brasileiro, em especial diante do que está previsto no artigo 5°, inciso X, da Carta Magna, bem como no art. 21 do Código Civil, tem-se a base sobre a proteção do âmbito privado de um cidadão, seja em sua vida particular ou em sua intimidade.Em relação ao direito à privacidade, em especial no que toca ao direito à

intimidade, visualiza-se a segurança que um indivíduo possui em relação à sua vida íntima contra intromissões externas, aleatórias e desconvidadas, inclusive prevendo-se que a exposição na sociedade não pode acontecer sem a autorização de quem é o titular de tais direitos. A definição de privacidade é, em grande parte, resultado do veloz crescimento de como as informações e dados são colhidos e disseminados.

De acordo com Carvalho e Pedrini (2019), não há como negar que essa era de tecnologia facilitou a vida dos seres humanos, é visível o quanto a sociedade modificou-se em razão das constantes modernizações trazidas pelo momento tecnológico vivenciado. Os celulares, computadores e muitos outros dispositivos eletrônicos com acesso à internet fazem com que informações em massa sejam processadas.

Também, pode-se considerar que as pessoas estão vivendo uma era comunicacional, em que há uma busca maciça por notícias, onde os instrumentos tecnológicos podem potencializar a formação de conhecimento e a disseminação de informações. Quando se fala em conhecimento, constata-se que a Internet e seus produtos podem minimizar obstáculos do tempo e do espaço, proporcionando que o objeto envolvido alcance imediatamente número expressivo de usuários. Já quando se fala em propagação de informações, visualiza-se o espaço democrático em que estas são criadas e depois exibidas, inúmeras vezes sendo viralizadas em redes sociais, em que muitos podem acessar pelo próprio celular e até criar conteúdo a partir deste.

Claro que nem tudo o que se está na rede é verdade. "*Fake News*" aparecem o tempo todo, já que existe a possibilidade de todos os usuários divulgarem conteúdos na Internet. Compreende-se, então, que o usuário da Internet não é só destinatário de informação, mas também o veiculador. Por isso, nesse ambiente democrático que permite a muitos poderem exercer suas opiniões, existem chances de haver violação aosdireitos constitucionais, especialmente no que diz respeito à privacidade.

Sob o ângulo de proteção constitucional, não somente o direito à intimidade, à vida privada e à honra são garantidos, como também a correspondente proteção que possa resultar das possíveis violações de tais direitos, quer delas decorram danos morais ou materiais.

A partir da formação e estabelecimento permanente de todos os direitos essenciais à personalidade, há uma implacabilidade na proteção qualitativa que a entidade estatal deve

transmitir ao mesmo tempo em que estabelece deveres (OLIVEIRA JÚNIOR, 2013). Ou seja, em um estado democrático, se há uma quantidade razoável de direitos e deveres, também será necessário defender a pessoa por reconhecimento de sua personalidade, que também deve ser eficaz no domínio da proteção de dados.

A partir desta perspectiva de um país democrático, que preza pela liberdade de expressão, e diante dareal necessidade de proteção à privacidade e à proteção de dados,é importante a existência de uma entidade estatal buscando a aplicação das legislações que buscam a proteção destes direitos.

2.2 Marco civil da internet (Lei 12.965/14): Evolução da proteção de dados no brasil

No dia 23 de abril de 2014, foi aprovada a lei que regula o uso da internet no Brasil,Lei nº12.965/14, com o objetivo de dar fim a lacuna existente nas relações jurídicas realizadas por meio da internet, estabelecendo princípios, garantias, bem como direitos e deveres para o uso da internet no Brasil, popularmente denominada como Lei do Marco Civil da Internet.

Já era sabido a necessidade de uma normatização especifica no espaço virtual, bem como a necessidade de estabelecer direitos e deveres aos usuários, provedores bem como a atuação do Poder Público.

Um dos objetivos principais do Marco Civil Internet sempre foi à regulamentação dos direitos e deveres aos destinatários da legislação. Como por exemplo, o capítulo II queestabelece garantias aos usuários, como a proteção dos direitos individuais e coletivos quanto ao uso da internet, das quais ainda existia uma grande lacuna no nosso ordenamento jurídico.

Observa-se que a lei tomou por medida assegurar os direitos de inviolabilidade da intimidade e da vida privada conforme previsto no art. 7º inc. I que assim expressa:

> Art. 7° O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

Percebe-se que a lei procurou regulamentar de forma especifica um direito já assegurado e amparado pela Constituição no seu artigo 5º, inciso XII, para torná-la aplicável na esfera intima e privada das pessoas. Pelo fato de que este direito ter que ser não apenas defendido, mas preservado, como define o ilustre autor Marcelo Cardoso Pereira:

> [...] o direito das pessoas de defender e preservar um âmbito íntimo, variável segundo o momento histórico imperante, no qual estas possam desenvolver sua personalidade, bem como o poder de controlar suas informações pessoais [...] (2006, p.140)

Ainda no artigo 7º temos a garantias como o sigilo de comunicações, tanto das comunicações armazenadas peloservidor, quanto daquelas transmitidas pela internet, conforme exposto:

> "[...] II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Passou-se a regulamentar os registros de navegação, o que era algo discutido por analogia no Brasil, e não expressamente tratado, como o autor nos mostra:

> À medida que a pessoa se dispõe a "navegar" pela internet sua privacidade fica extremamente comprometida. É que com cada clique do mouse a pessoa vai deixando seu caminho marcado pela rede e, consequentemente os seus hábitos, seus vícios, suas necessidades e suas preferências." (GUERRA, 2004, p.78).

O autor supramencionado demonstra a facilidade, nas quais as monitorações ilegais de dados ocorrem aos usuários da rede. Verifica-se assim que o sigilo de comunicações armazenadas se dá não apenas com as armazenadas no dispositivo, mas também pelos provedores de internet, os quais detém informações de seus usuários, conforme o art. 10 § 1º da lei mencionada:

> Art.10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1° O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7°

Denota-se que o artigo tem por finalidade estabelecer a regulamentação do provedor devidamente envolvido quanto à intimidade de dados, e os registros de conexão de usuários bem como o sigilo das informações armazenadas.

> Como principiologia, deve ser resguardado todas as informações possíveis de maneira a garantir a intimidade e privacidade das relações havidas na rede, notadamente porque tais informações, se acessadas indiscriminadamente por terceiros, poderia servir de base para praticas infringentes, vedadas em lei." (VANCIM et al, 2015, p.69).

Ao regulamentar sobre a previsão legal de procedimento judicial, o legislador estabelece quais os requerimentos para a parte interessada, ou até mesmo como o usuário prejudicado deve proceder em determinada situação. Assim temos a previsão legal dos próprios direitos fundamentais do usuário quanto ao direito de informação. Há de se mencionar que mesmo sem um consentimento legal, o usuário é passível de um ataque virtual, conforme o trecho abaixo:

> O armazenamento de informações sobre uma determinada pessoa é, assim, algo inquietante em razão da ameaça de que estes dados possam ser acessados indevidamente, dado que os cookies são responsáveis pelo armazenamento das informações pessoais dos usuários da internet, pois abrem caminho até o disco rígido do internauta e armazenam ali um arquivo de texto que identifica o computador com um numero único." (GUERRA, 2004, p.81).

Diante do fato de que um simples acesso a um endereço na web já traz uma grande quantidade de registros, é perceptível a vontade do legislador, de impor sanções quanto ao caso, já que hoje são os meios mais utilizados para o cometimento de crimes virtuais. Observa-se ainda, a intenção do legislador de sobrepor a norma em âmbito nacional às empresas estrangeiras que prestarem serviço em território nacional, como no texto abaixo exposto:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros."

A Lei nº 12.965/14 ainda prevê sanções para o descumprimento destes artigos,estas que ser: advertências, multas ou até mesmo a proibição de exercício deatividade.

2.3 Lei de acesso a informação (Lei 12.527/2011)

A Lei nº 12.527, sancionada em 18 de novembro de 2011, regulamenta o direito constitucional de acesso dos cidadãos às informações públicas e é aplicável aos três poderes da União, dos estados, do Distrito Federal e dos municípios. (BRASIL. Lei nº 12.527(2011). Foi regulamentada pelo Decreto nº 7.724, de 16 de maio 2012, e busca trazer mais transparência ao Governo, além de disponibilizar ao cidadão as informações de caráter público seguindo os procedimentos previsto pela Constituição Federal de 88 no art. 5º, inc. XXXIII; art. 37, §3º, inc. II.

Com avanços apresentados na Carta Magna na diretriz da participação social, medidas foram tomadas para priorizar a transparência e publicização de dados públicos. Contudo, demorou mais de vinte anos para se consolidar uma lei sobre o tema no país. Em 2011, após sete anos de discussões no Congresso, foi aprovada e sancionada uma legislação sobre a regulamentação do acesso à informação, a Lei 12.527, tendo como diretriz principal que a publicidade fosse vista como preceito geral e o sigilo como exceção. Essa legislação possibilita que qualquer cidadão possa ter acesso à informação pública sendo essa garantia um dever do Estado.

A legislação aborda como a Administração Pública deve fornecer as informações aos cidadãos, seja através de iniciativa própria, ou por parte do cidadão em querer ter acesso a alguma informação pública,

A transparência ativa está no artigo 8º da lei que estabelece: "é dever dos órgãos e entidades públicas promover [...] a divulgação em local de fácil acesso [...] de informações de interesse coletivo ou geral por eles produzidos ou custodiadas" (BRASIL, 2011). De forma complementar, a transparência passiva pode ser encontrada no artigo 10º ao garantir que qualquer cidadão pode solicitar uma informação pública, sem a necessidade de justificar o motivo, ao qual está solicitando essa informação.

Em regra, o órgão público deve oferecer a informação solicitada de imediato ao cidadão, mas em casos em que é necessário estipular um prazo para resposta, a legislação é muito específica. Segundo a norma, o prazo de entrega é de 20 dias podendo ser postergado por mais 10 dias, caso necessário. A lei também estabelece que, em caso de negativas de acesso, é necessário que seja informado ao cidadão a justificativa e a possibilidade de recurso (BRASIL, 2011).

Outro aspecto importante da LAI diz respeito ao enfraquecimento da cultura de segredo para se implantar a cultura de acesso no campo público. Isso se dá, pois para se ter a disponibilização de informações torna-se necessário uma gestão pública aberta. Segundo a Controladoria Geral da União (CGU), a cultura de segredo é marcada pelo princípio de que a circulação de informações representa riscos fazendo com que a gestão pública não seja eficiente. Em um cenário de cultura de acesso tem-se a presença da consciência de que a

informação pública pertence ao cidadão, o que reforça o acesso como regra e o sigilo, a exceção, tal como preconiza a Lei (CONTROLADORIA GERAL DA UNIÃO, 2011).

3 A JURISPRIDÊNCIA BRASILEIRA: O EFEITO DA VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS

Com a vigência da Lei Geral de Proteção de Dados (LGPD), seguida pela criação da Autoridade Nacional de Proteção de Dados (ANPD), surgiram ações judiciais e entendimentos jurisprudenciais envolvendo o tema, em especial sobre indenizações em caso de vazamento de dados.

Os efeitos eram incertos, era possível a ocorrência de muitas condenações em ações pedindo indenização por danos morais por conta de vazamento de dados, mas o que se percebe é uma divisão de entendimentos, havendo várias decisões que entendem que o simples vazamento dos dados, sem efetivo dano, não gera o dever de indenizar.

As ações judiciais têm como objeto principalmente questões consumeristas e trabalhistas.

3.1 Caso Serasa

Justiça confirma liminar e determina que Serasa deixe de comercializar dados pessoais: O juiz substituto da 5ª Vara Cível de Brasília confirmou decisão liminar da 2ª Turma Cível do TJDFT que determinou que a Serasa Experian pare de comercializar dados pessoais dos titulares por meio dos produtos Lista Online e Prospecção de Clientes, oferecidos pelo site da ré, sob pena de imposição das medidas para assegurar o cumprimento da ordem judicial, conforme legislação vigente.

A Ação Civil Pública foi proposta pelo MPDFT, processo nº **0736634-81.2020.8.07.0001**, sob o argumento de que a venda dos dados fere a Lei Geral de Proteção de Dados Pessoais – LGPD, uma vez que a norma impõe a necessidade de manifestação específica para cada uma das finalidades de tratamento dos dados. Logo, o compartilhamento de tais informações, da forma que tem sido feita pela empresa, seria ilegal ao ferir o direito à privacidade das pessoas, bem como os direitos à intimidade, privacidade e honra dos titulares dos dados.

O órgão ministerial afirma que o contratante dos serviços recebe uma ou mais bases de dados de contatos com informações como CPF, nome, endereço, telefones e sexo. O serviço pode ser segmentado por meio do uso de filtros, dentro de um universo potencial de 150 cinquenta milhões de CPFs. Destaca que essa exposição generalizada é capaz de gerar um grande vazamento de dados. Por último, ressalta o risco de utilização indevida dos referidos dados durante o período eleitoral.

A ré sustenta que a ação foi proposta de forma precipitada, com base em informações superficiais buscadas no site da empresa, sem qualquer aprofundamento acerca de suas atividades. Alega que os produtos existem há anos, sem questionamentos e reclamações por parte dos consumidores, tampouco produzem danos, bem como estão alinhados com as predisposições da LGPD. Destaca que a própria lei prevê situações em que o consentimento específico do titular dos dados é dispensável. Informa, ainda, que a comercialização é inerente às suas atividades e não há divulgação de dados sensíveis dos titulares, abuso ou violação à intimidade e privacidade dos consumidores, uma vez que reúne informações públicas de natureza cadastral, fornecidas em situações cotidianas.

O entendimento do magistrado é o de que a comercialização de dados pessoais por meio dos produtos oferecidos pela ré é ilícita, tal como concluíram os desembargadores do TJDFT, quando da concessão da tutela de urgência para suspensão da comercialização dos serviços, em maio deste ano. “A partir do desenvolvimento tecnológico, da economia mais voltada ao âmbito digital e das possibilidades concretas de tratamento de dados pessoais, é evidente o relevo do valor econômico das informações sobre a coletividade, pois relevantes para o objetivo institucional de várias instituições, públicas e privadas”, pontuou o julgador.

A decisão ressalta, ainda, que o tratamento e o compartilhamento dos referidos dados, na forma como é feito pela ré, exigiria o consentimento claro e expresso do indivíduo retratado, condição para viabilizar o fluxo informacional realizado, com caráter manifestamente econômico. No caso dos autos, inexiste o indispensável consentimento em relação à universalidade de pessoas catalogadas.

“É exatamente por meio do consentimento inequívoco que o titular dos dados consegue controlar o nível de proteção e os fluxos de seus dados, permitindo ou não que suas informações sejam processadas, utilizadas e/ou repassadas a terceiros”. Além disso, o

magistrado reforçou que, mesmo para os dados públicos, exige-se o propósito legítimo e específico, a preservação dos direitos dos titulares e a observância das diretrizes básicas da LGPD.

O número da ação é 0736634-81.2020.8.07.0001

3.2 Caso prático União, Caixa Econômica, Dataprev e Autoridade nacional de proteção de dados (ANDP)

A Justiça Federal determinou que cerca de 4 milhões de pessoas sejam indenizadas em R$ 15 mil cada, por terem sido vítimas de um vazamento massivo de dados no segundo semestre de 2022. O valor deve ser pago pela União, Caixa Econômica Federal, Empresa de Tecnologia e Informações da Previdência (Dataprev) e pela Autoridade Nacional de Proteção de Dados (ANPD). A sentença é resultado de uma ação civil pública do Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, Compliance e Segurança da Informação, com manifestação favorável do Ministério Público Federal (MPF) pela garantia dos direitos dos cidadãos prejudicados. Cabe recurso contra a decisão.

O vazamento ocorreu a partir de bancos de dados mantidos pela Caixa, União e Dataprev. A maioria das vítimas recebia o Auxílio Brasil e, às vésperas da eleição presidencial de 2022, passou a contar com larga porcentagem do benefício para a contratação de crédito consignado. Os dados pessoais divulgados ilegalmente acabaram nas mãos de correspondentes bancários, que utilizaram as informações para o oferecimento dos empréstimos e de outros produtos financeiros.

Para o MPF, o fato de o vazamento ocorrer em empresas e órgãos públicos aos quais milhões de brasileiros confiaram a proteção de seus dados torna o caso ainda mais grave. “Esses dados violados pairam no registro e no banco de dados de incontáveis instituições, assim como em poder de terceiros que, facilmente, poderão fazer uso maléfico e fraudulento dessas informações, em franco prejuízo material, moral e social desses cidadãos”, destacou a procuradora da República Karen Louise Jeanette Kahn.

Além da indenização às vítimas, a sentença da 1ª Vara Cível Federal de São Paulo determinou que as rés paguem R$ 40 milhões por danos morais coletivos, valor que deve ser revertido ao Fundo de Defesa dos Direitos Difusos. Elas também deverão comunicar

formalmente, aos titulares dos dados, a ocorrência do incidente de segurança que resultou no vazamento, as medidas adotadas para mitigar as consequências e os planos para solucionar eventuais riscos. A decisão judicial estabeleceu ainda a revisão dos sistemas de armazenamento de dados, o desenvolvimento de mecanismos de segurança e controle preventivo e o fornecimento de registros e informações relacionados à violação do sigilo.

O número da ação é **5028572-20.2022.4.03.6100.** A tramitação pode ser consultada em https://pje1g.trf3.jus.br/pje/ConsultaPublica/listView.seam

CONSIDERAÇÕES FINAIS

Uma vez identificado o processo de construção da LGPD, pode-se compreender que, antes da legislação entrar em vigor, já existiam normas no ordenamento jurídico brasileiro acerca da proteção de dados pessoais, como por exemplo o próprio CDC (Lei nº 8.078/1990), a MCI (Lei nº 12.965/2014), a Lei de Acesso à Informação (Lei n° 12.527/2011), entre outras. Ao ver todo esse aparato legal, entendia-se que havia um quebra-cabeças, várias peças espalhadas, que não tinham sintonia, sendo difícil poder agrupá-las.

Diante disso, compreende-se que com a promulgação da LGPD surgiu um impacto positivo, pois antes não era possível estruturar um sistema completo, mesmo havendo grande regulamentação acerca do assunto. Assim, apesar de haver várias leis setoriais de proteção de dados pessoais, essas normas e regras estavam espalhadas faltando ainda a maior peça desse quebra-cabeça, que era uma legislação específica tratando sobre o tema. A partir de então, tornava-se possível ver todos os conceitos básicos condensados em uma única legislação, o que facilitava o trabalho de todas as entidades e cidadãos.

Compreendeu-se que a nova lei é regida por princípios que podem instigar a iniciativa pública e privada a transformar a internet em uma esfera mais democrática e, ao mesmo tempo, regulamentada. Percebe-se que imprecisões, erros ou intrusões podem ocorrer, porém, vislumbra-se que ainda assim, há mais proteção jurídica.

Vislumbra-se que a legislação produz a consolidação do uso íntegro, protetivo e legal acerca dos dados pessoais, respeitando os princípios instruídos, para garantir, acima de tudo, ao tratar da proteção da dados pessoais, o respeito ao direito fundamental à privacidade.

Considerando que o ambiente virtual é abrangente e extremamente vasto, pode-se considerar complexo e difícil manter o domínio das informações que trafegam pela internet, de modo que em várias situações pode ser que aconteça vazamentos de informações de banco de dados, pois não é possível garantir sempre a integridade dos dados em um mundo virtual, uma vez que que pode haver erros técnicos ou furto de informação.

Desta forma, após a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), torna-se viável examinar o método escolhido pelo legislador a favor da clareza, da autonomia e do cuidado do jurídico em relação aos direitos inerentes à personalidade. Compreende-se que a nova legislação veio para deixar mais transparente a relação dos agentes de tratamento de dados com os titulares, e tal relação deve estar revestida de boa-fé.

Este é um desenvolvimento significativo para os vínculos não só jurídicos, mas também de interesse comercial em nosso país. Tal lei viabiliza conceder responsabilidade a quem de fato lhe cabe e, em situações de quebra do cumprimento legal, são dadas ordens administrativas e incidem exigências de compensação e reparo em caso de perda. Isso garante uma grande credibilidade jurídica não somente ao titular das informações como também aos agentes de controle.

REFERÊNCIAS

BRASIL. Constituição Federal. Constituição da República Federativa do Brasil de 1988. Publicada no Diário Oficial da União, Brasília, 05 out. 1988.

BRASIL. Marco Civil da Internet. Brasília, DF: Congresso Nacional, 2014.

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

BURGOS, Pedro. MegaUpload é tirado do ar pela justiça dos EUA – pirataria é só um pedaço da acusação. Disponivel em <http://gizmodo.uol.com.br/megaupload-e-tirado-do-ar-pelajustica-dos-eua-pirataria-e-so-um-pedaco-da-acusacao/

BATISTA, M. A difusão da Lei de Acesso à Informação nos municípios brasileiros:fatores internos e externos. Brasília: Enap, 2017.

FREITAS, José Carlos. A Constituição Federal e o direito à informação. Disponível em<http://www.estadao.com.br/noticias/geral,a-constituicao-federal-e-o-direito-ainformacao,496041

L12737. Planalto.gov.br. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>.

MÜLLER, Leonardo. Operadoras vs. WhatsApp: Anatel pode não ter como resolver a peleja. Disponivel em < http://www.tecmundo.com.br/whatsapp/85194-operadoras-vs-whatsappanatel-nao-ter-resolver-peleja.htm