Centro Universitário de Brasília - UniCEUB

Faculdade de Ciências Jurídicas e Sociais -

FAJS Curso de Bacharelado em Direito

RITA MARIA BATISTA PERES

DIREITO À PRIVACIDADE NA TRANSFERÊNCIA INTERNACIONAL DE DADOS SENSÍVEIS

BRASÍLIA

2023

RITA MARIA BATISTA PERES

DIREITO À PRIVACIDADE NA TRANSFERÊNCIA INTERNACIONAL DE DADOS SENSÍVEIS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Ricardo Victor Ferreira Bastos

BRASÍLIA

2023

RITA MARIA BATISTA PERES

DIREITO À PRIVACIDADE NA TRANSFERÊNCIA INTERNACIONAL DE DADOS SENSÍVEIS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Ricardo Victor Ferreira Bastos

BRASÍLIA, 31 DE MARÇO DE 2023

BANCA AVALIADORA

Professor Orientador

Professor Avaliador

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus por ter me guiado em todos os passos e momentos da minha vida, me permitindo alcançar o sucesso em mais essa etapa de minha trajetória que apenas se inicia.

Agradeço especialmente aos meus queridos pais, Darcneice e Jorge, por me apoiarem nesse sonho, sempre me fornecendo amparo, carinho e preenchendo-me com um amor incondicional ímpar, eles que nunca me deixaram sequer pensar em desistir, sempre apostando no meu potencial e me ensinando no processo valores que moldaram a mulher e profissional que me tornei hoje.

Agradeço ao meu melhor amigo e namorado, Samuel Matos, por ter sido meu porto seguro em meio a tantas tormentas e angústias, sempre companheiro e resiliente nesse processo tão único e desafiador.

Agradeço ao meu orientador Prof. Ricardo Victor Ferreira Bastos, por cada dose de paciência, gentileza, empatia, compreensão e estímulo que despendeu comigo nesse caminho de desenvolvimento intelectual.

Aos meus amigos, que, do início ao fim do curso, compartilharam dos desafios enfrentados na jornada acadêmica, sempre com muita perseverança, ânimo e amizade, que me possibilitaram acreditar que eu era capaz de obter belas conquistas com louvor.

Por fim, quero agradecer ao Centro Universitário de Brasília - UNICEUB e ao seu corpo docente, que demonstraram comprometimento com a qualidade e excelência do ensino.

RESUMO

O presente trabalho de conclusão de curso pretende aproximar e realizar uma breve análise sobre os conceitos de privacidade, transferência internacional de dados e seus desdobramentos. Assim como, aprofundar-se nos contextos históricos de surgimento e disseminação da privacidade, até a sua disseminação no cenário jurídico do Brasil, e em seu impacto na outorga da recente Lei Geral de Proteção de Dados, principal regulamentação do tratamento de dados no país. Após, examinou-se como o Brasil tem se comportado no exercício da disciplina da proteção de dados, gênero no qual a sistemática da transferência internacional de dados, recorte dessa pesquisa, está inserido. A seguir, aprofundou-se o estudo sobre o regime atual de transferência internacional de dados no meio globalizado internacional e sob circunstâncias nacionais, com o escopo de expor o regime de transferência internacional de dados solidificado na ordem jurídica nacional, e, os contornos normativos desse potencial de normas, apontadas. Concluiu-se, então, que o regime jurídico de transferência internacional de dados ainda não está finalizado e estruturado, mas sim em vias de construção, e que esse tipo de operação não seria possível sem respeitar o direito à privacidade dos dados dos titulares. Por meio dessa análise, a presente pesquisa se propõe a averiguar em um caso real de vazamento de dados, se a LGPD encontra-se apta a garantir aos titulares dos dados que recaem sob sua tutela a efetiva proteção contra medidas ineficazes de segurança no procedimento de transferência internacional desses dados, sob a ótica da aplicação dos normativos brasileiros, onde o direito à privacidade e à proteção de dados representa um relevante desafio no âmbito jurídico, o qual requer maior robustez para suprir as lacunas frente ao meio digital em constante modificação e atualização. A metodologia adotada para o desenvolvimento da investigação debruçou-se na abordagem lógico-dedutiva e em um estudo de caso relativo ao vazamento de dados da empresa norte-americana Equifax. Quanto às técnicas de pesquisa, recorreu-se às espécies bibliográfica e documental, com base no estudo de fontes doutrinárias, legislativas e jurisprudenciais, nacionais e estrangeiras.

Palavras-chave: privacidade; proteção de dados; transferência internacional de dados; LGPD; informação.

SUMÁRIO

1 INTRODUÇÃO

O direito à privacidade na transferência internacional de dados sensíveis é um tema de crescente importância e preocupação no cenário global atual. A era digital e o desenvolvimento exponencial das tecnologias de informação e comunicação têm facilitado a circulação e o armazenamento de grandes volumes de dados em escala mundial, incluindo dados pessoais e sensíveis. Essa realidade tem gerado questionamentos e desafios relacionados à proteção da privacidade dos indivíduos, uma vez que a livre circulação de dados pode expor informações confidenciais a usos indevidos ou mal-intencionados.

Dados sensíveis são aqueles que revelam informações intimamente ligadas à vida privada do indivíduo, como origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados biométricos, genéticos, relativos à saúde ou à vida sexual, entre outros. A transferência internacional desses dados pode ocorrer entre empresas, governos e outros atores, por vários motivos, como transações comerciais, cooperação internacional e compartilhamento de informações para fins de segurança.

Nesse contexto, garantir o direito à privacidade na transferência internacional de dados sensíveis é crucial para preservar a dignidade e a autonomia dos indivíduos, assim como para manter a confiança no ambiente digital. Para isso, diversos países têm adotado leis e regulamentações específicas, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil, que estabelecem regras e exigências para a coleta, processamento e transferência de dados pessoais, incluindo dados sensíveis, sendo essa última o foco da presente dissertação.

Além disso, é fundamental que seja exposta uma breve análise sobre o direito à privacidade, a transferência internacional de dados e como ambos estão sendo aplicados na atual conjuntura brasileira, após a edição da Lei Geral de Proteção de Dados, de maneira a contribuir para o debate e aprofundamento legislativo e doutrinário da temática a ser abordada, além de expor a aplicação prática destes.

Haja vista que, o debate sobre o direito à privacidade na transferência internacional de dados sensíveis envolve questões éticas, legais, políticas e tecnológicas, exigindo uma abordagem multidisciplinar e colaborativa entre os diversos atores envolvidos, a fim de alcançar um equilíbrio entre a livre circulação de informações e a proteção dos direitos fundamentais dos indivíduos.

Logo, a empresa de crédito norte-americana, Equifax, será alvo de estudo e aprofundamento teórico sobre a temática proposta, sob a ótica da atual jurisdição brasileira no recente caso de vazamento de dados pessoais em 2017.

2 IMPORTÂNCIA DA PRIVACIDADE

As delimitações conceituais são importantes para o reconhecimento e desenvolvimento dos Direitos Fundamentais de cada cidadão, referentes a sua privacidade, em uma realidade em que a informação tem grande valor. Por conta disso, passa-se a discorrer sobre o princípio da privacidade no âmbito do mundo digital e, consequentemente, da Lei Geral de Proteção de Dados.

2.1 O que é Privacidade

O termo “privacidade”, em sua determinação mais atual, base para o desenvolvimento do presente trabalho, foi estabelecido pelo legislador do Código Civil de 2002, elencou o termo à “*vida privada*”, como também disciplinada pela Constituição Federal de 1988, em seu artigo 5°, inciso X e regida pelo princípio da exclusividade.

Apesar de doutrinariamente não possuir uma denominação consensualmente pacificada, está constantemente relacionada como direito ao resguardo, ao recato, ao segredo, à vida ou esfera privada ou íntima, segundo o conceito de José Serpa. É, portanto, um modo específico de vivência pessoal, isolada, numa esfera reservada, sempre sem uma notória forma de participação de terceiros, seja pelo resguardo contra a ingerência ou molestamento malevo alheio, seja pela utilização da faculdade que se lhe é atribuída para razoável exclusão do conhecimento público, de dados, ações, idéias e emoções que lhe são peculiares.

Outro ponto de vista de extrema relevância, seria o de Milton Fernandes, em que a vida privada consistiria, em um direito do proibição à intervenção ou conhecimento de terceiro, um direito de oposição e de exclusão da divulgação da própria vida, um *privacy a um jus prohibitionis*.

Logo, há de se levar em consideração que a doutrina é, em sua maioria, sensível à necessidade de construir um sistema capaz de abarcar a amplitude da problemática da privacidade e, para tal, se utiliza dos múltiplos termos.

A base para a distinção do Constituinte brasileiro pode ser encontrada na teoria das esferas de Heinrich Hubmann, segundo a qual o sentimento de privacidade do indivíduo pode ser entendido a partir de um esquema de círculos

concêntricos, que representam diferentes graus de manifestação da privacidade, em que no núcleo observariamos a esfera da intimidade ou do segredo, em torno dela viria a esfera privada, e em envolto de ambos, encontrar-se-ia a esfera pessoal, de maneira mais ampla, que englobaria a vida pública do homem.

Portanto, apesar de tantos conceitos referentes à privacidade, entende-se que a definição mais adequada é a que ressalta a percepção de controle do indivíduo sobre as suas informações, em decorrência da existência de uma autonomia do seu titular na constituição de tal direito, existindo, então, um único direito para abranger todos os casos que se trata da proteção do indivíduo no aspecto de sua esfera privada. Diante de tal contexto, é possível concluir que o titular possui a faculdade de estabelecer as delimitações do exercício do seu direito à privacidade, .

Contudo, no campo digital, quanto à transferência de dados pessoais, disciplinados pela Lei Geral de Proteção de Dados, toma-se o termo “privacidade”, em stricto sensu, como o conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, aquilo a ser mantido em particular, escondido das vistas ou conhecimento de terceiros.

2.1.1 Direito à privacidade

O direito à privacidade surgiu como resultado de inovações e ferramentas tecnológicas, que permitiram o acréscimo de informações e divulgação de fatos relacionados à esfera privada do indivíduo, em um contexto doutrinário que foi efetivamente reconhecido pelo legislador no século XX. O indivíduo de uma forma ainda desconhecida. Nesse sentido, o artigo da Harvard Law Review de Warren e Brandeis “The Right to Privacy” sobre privacidade foi imprescindível para o desenvolvimento desse direito fundamental, principalmente em um contexto capitalista onde a propriedade privada é garantida mundialmente em diversas constituições.

O marco inicial ao direito à privacidade foi desenvolvido por Warren e Brandeis na qual vinculou o direito à privacidade a proteção à inviolabilidade da pessoa, dessa forma quebrando com as tradições de vincular a proteção da vida privada à propriedade. Os autores entenderam que o princípio da proteção pessoal, não impede que sejam adquiridos por roubos ou apropriação indébita, mas pode

impedir qualquer forma de publicação, não sendo caracterizado como o princípio da propriedade privada, mas se busca a proteção no princípio da inviolabilidade da personalidade.

Com o crescimento e a velocidade da circulação das informações, consequência do desenvolvimento exponencial da tecnologia de coleta de dados, os autores partem da necessidade de reconhecer o direito à privacidade na própria vida moderna e complexa, o que torna as pessoas mais sensíveis à publicidade, de modo que a solidão e a intimidade se tornam mais importantes para o indivíduo.

Deve-se notar que ao determinar os direitos de privacidade, Warren e Brandeis também tentaram definir suas limitações em termos de: I) O direito a publicidade não impede a publicação de dados de interesse geral; ii) Os direitos de privacidade não proíbem todas as comunicações privadas, como se isso acontecesse legalmente, como em um tribunal ou a Assembleia Legislativa, este direito não será violado; iii) A reparação não será exigível se o delito resultar de uma divulgação oral que não cause danos; iv) O consentimento do lesado impede a violação dos direitos; vi) Nenhuma violação deste direito é pretendida nem excluída.

Percebe-se que para Warren e Brandeis a proteção da privacidade é fortemente individualista desde o início, caracterizada pelo direito de estar só. É nesse sentido que há muito tempo é considerado como um direito burguês típico por causa de suas características jurídicas negativas proeminentes, como a exigência absoluta do Estado de abrir mão da esfera privada do indivíduo para garanti-la.

Como argumenta Doneda, é o contexto em que o sentido de privacidade está associado à imagem do mundo burguês, principalmente no meio judiciário. Isso porque os primeiros processos judiciais a admitir invasão de privacidade envolveram grandes celebridades, como o caso Rachel (a famosa atriz francesa Elisa Rachel Félix em 1858) e o caso de Benito Mussolini e sua amante Clara Petacci. (Itália, 1953).

Notavelmente, ao longo do século XX, a mudança do papel do Estado, combinada com revoluções tecnológicas, ajudou a mudar o significado e o alcance do direito à privacidade. De um direito de dimensão estritamente negativa e de conotação quase egoísta, passou a ser visto como condição prévia para o reconhecimento de outros direitos fundamentais. Dessa forma a invasão de privacidade deixou de ser um problema apenas as classes mais elitizadas e passou a atingir o público em geral.

O reconhecimento internacional da proteção à privacidade ganhou ênfase após a Segunda Guerra Mundial. Na qual a Declaração Universal dos Direitos Humanos de 1948 estipula em seu art. 12, além dos direitos à privacidade, honra e confidencialidade das comunicações, há as seguintes disposições: "A vida privada, a família, o domicílio ou a correspondência de qualquer pessoa, ou atentados à sua reputação. Toda pessoa tem direito à proteção da lei, livre de tais interferências e ataques."

A Convenção Americana sobre Direitos Humanos na Convenção Europeia para a Proteção dos Direitos Humanos e Liberdades Fundamentais, o Pacto Internacional sobre Direitos Civis e Políticos e a Convenção de San José da Costa Rica também preveem a proteção da privacidade em termos semelhantes.

O progresso do direito à privacidade continua a se adaptar às novas mudanças sociais trazidas pelas inovações tecnológicas das informações, que de forma pioneira, permite coletar e processar dados pessoais dos cidadãos. Além de ganhar caráter positivo e reconhecimento internacional, o direito à privacidade também se transformou na disciplina de proteção de dados pessoais, pois a informatização dos dados traz novos desafios ao ordenamento jurídico.

A ligação entre a proteção da privacidade e as informações pessoais surgiu a partir do momento em que a tecnologia permitiu o armazenamento e processamento rápido e eficiente de dados pessoais. Nesse contexto, não apenas o conteúdo da privacidade mudou, mas também seu vocabulário, que agora é chamado de privacidade da informação, "proteção de dados pessoais", "autodeterminação da informação" etc.

Desta forma, os ordenamentos jurídicos de alguns países começam a proteger, não só a privacidade, mas explicitamente os dados pessoais dos seus cidadãos, por entenderem que esses dados constituem uma projeção da personalidade de um indivíduo e são mesmo dignos de proteção constitucional.

2.1.2 Histórico do princípio da privacidade para a edição da LGPD no direito brasileiro

Cabe ainda, introduzir o arcabouço histórico do princípio da privacidade no Brasil, até que fosse estabelecida a Lei Geral de Proteção de Dados.

Inicialmente, o princípio foi, de fato, estabelecido e normatizado no Brasil, com o advento da Constituição Federal de 1988, em seu artigo 5º, inciso X, onde se prevê que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação", podendo ser indenizável caso seja violada. (BRASIL, 1988)

Em seguida, houve a concretização do Código de Defesa do Consumidor, Lei nº 8.078/1990, o qual regulamenta o direito à proteção dos dados pessoais, em seu artigo 43, adentrando na proteção dos aspectos pessoais nas mais diversas situações, assim como a Lei do Sigilo Bancário, Lei Complementar nº 105/2001, a qual virou uma garantia constitucional quanto a privacidade dos clientes.

Com o advento do Código Civil Brasileiro, no ano de 2002, a privacidade foi objeto de novas disposições, por exemplo na impossibilidade de transmissão ou renúncia desta, uma vez que é um direito da personalidade ou em seu artigo 21, que dispõe sobre a inviolabilidade da vida privada da pessoa natural, com a premissa de decretação de medidas necessárias, a fim de impedir ou fazer cessar quaisquer atos contrários.

No entanto, foi somente no ano de 2014, após os avanços tecnológicos se tornarem comuns no cotidiano dos indivíduos, que surgiu o Marco Civil da Internet, o qual disciplina sobre a privacidade na internet e proteção dos dados pessoais contido nela, não abarcando o tratamento de dados colhidos off-line ou ainda, por meio de redes privativas, Lei nº 12.965/2014, juntamente com o Decreto 8.771/2016. (COTS; OLIVEIRA, 2019, p. 38.)

Diante de tal marco histórico, foi editada a Lei Geral de Proteção de Dados, promulgada em 2018, mas com vigência apenas em 2020, com a ideia de assegurar a proteção das garantias voltadas aos direitos fundamentais humanos, principalmente no âmbito digital (PINHEIRO, 2020, p. 15.)

2.3 Aplicação no meio Digital

O avanço tecnológico, com o advento da internet, no último século, abalou toda a estrutura constituída em torno do direito à privacidade, tendo em vista que o ordenamento normativo brasileiro não estava apto a suprir as necessidades específicas do mundo digital, pois não havia regulamentação específica sobre o uso de sistemas de coleta e processamento de dados, de modo a prevenir ou reparar possíveis violações a esse direito, expondo a fragilidade dos sistemas de proteção à privacidade.

Ainda que o direito à privacidade seja reconhecido na Carta Magna e nos tratados internacionais, como um dos direitos fundamentais da pessoa humana, ela adquiriu novas particularidades na internet, visto que está relacionada com o controle, compartilhamento e uso das informações dos dados pessoais do indivíduo.

Segundo a linha de estudo do criminalista Paulo José da Costa Júnior, o avanço Técnico-Científico não abarcou mecanismos de controle do uso nocivo dessa tecnologia, evidenciando que esse processo de corrosão das fronteiras da intimidade e a invasão da vida privada tornou-se mais alarmante e inquietante. A corrente de pensamento do criminalista, ainda leva em consideração que a tecnologia da informação aumentou a coleta, o processamento e o uso de dados, e que essas mudanças quantitativas causam mudanças qualitativas, pois as novas tecnologias têm implicações para a vida privada, em seu equilíbrio, a liberdade pessoal, possibilitando riscos, antes inimagináveis, conforme exposto no trecho abaixo:

> *As conquistas desta era destinar-se-iam em tese a enriquecer a personalidade, ampliando-lhe a capacidade de domínio sobre a natureza, aprofundando o conhecimento, multiplicando e disseminando a riqueza, revelando e promovendo novos rumos de acesso ao conforto. Concretamente, todavia, o que se verifica é que o propósito dos inventores, cientistas, pesquisadores sofre um desvirtuamento quando se converte a idéia beneficente em produto de consumo. A revolução tecnológica, sempre mais acentuadamente, ganha um dinamismo próprio, desprovido de diretrizes morais, conduzido por um 'cientificismo' ao qual são estranhas e mesmo desprezíveis quaisquer preocupações éticas, metafísicas, humanísticas. Torna-se cega e desordenada, subtraindo-se ao controle até mesmo dos sábios, que a desencadeiam. (COSTA JUNIOR, 1995, p. 22.)*

Diante desses fatos, parece não haver dúvida quanto à necessidade de uma legislação específica de controle dos dados pessoais, de maneira a ser consolidada a segurança jurídica, mas sem reduzir os progressos científicos e seus impactos positivos na sociedade. No entanto, no contexto digital, o indivíduo defronta a perda da sua capacidade de percepção acerca dos ataques à sua privacidade, acreditando que a exposição dos fatos referentes à sua intimidade seja comum.

A sensação de submissão condicionada à Era Digital, que leva as pessoas a renunciarem a própria privacidade, uma redução da individualidade a meras identificações numéricas à espera de alguma utilidade econômica ou política, pode ser evitada através de uma regulamentação à captação, ao armazenamento, ao tratamento e à difusão de dados pessoaiS, como está sendo difundida nos demais países, principalmente os mais desenvolvidos.

No Brasil, se faz nítida a necessidade de uma regulamentação nacional que normalizasse o uso devido de dados pessoais, tendo em vista a prerrogativa constitucional de privacidade do cidadão, uma vez que o compartilhamento sem consentimento e a venda dos dados pessoais já estão sendo disseminados pelo mundo, em decorrência do aprimoramento e fácil acesso tecnológico. (AGOSTINELLI, 2018, p. 3)

Perante a natureza constitucional do direito à privacidade, presume-se que todo cidadão goza da garantia de ter suas informações pessoais protegidas e tratadas, por todo o ciclo de vida do tratamento, com a devida precaução fornecida pelas instituições e órgãos governamentais responsáveis. Logo, foi sancionada a Lei Geral de Proteção de Dados, a LGPD, que tem por finalidade, segundo o artigo de Oliveira, Toffoli e Prandi-Gonçalves (2019, p. 40):

> *[...] proteção de dados pessoais do cidadão; direitos do cidadão titular em possuir maior controle sobre o uso dos seus dados por qualquer empresa; segurança da informação e boas práticas de prevenção de vazamento de dados pessoais; comunicação de incidentes envolvendo vazamentos de dados pessoais e fiscalização do uso desses dados. Ou seja, a lei visa a estabelecer direitos fundamentais do cidadão.*

A internet expandiu o campo para discussões, alterando e ampliando as formas de interação e relacionamentos dentro da sociedade, uma vez que quebrou

as barreiras físicas e espaciais de comunicação, interação e pesquisa, propiciando um acesso ilimitado de informações. O ser humano, então, passa a viver conectado, dependente dessa tecnologia, “[...] o lugar onde quase tudo acontece [...]” e “[...] é lá que são criados e armazenados os dados mais particulares de cada um. É na internet que desenvolvemos e expressamos nossa personalidade e individualidade”, como exposto e sustentado por Greenwald (2014, p. 15).

Não há como negar os múltiplos benefícios decorrentes dessa informatização, porém também é um fato que o mundo digital é bastante complexo quanto à questão de controle e regulamentação, ensejando debates, no que diz respeito à privacidade, por ultrapassar a matéria física, já disciplinada e conhecida. De acordo com o entendimento de Thibes (2014, p. 35), na interação virtual não se tem certeza por quem está sendo notado, pois a cada dia estamos ainda mais imersos em uma sociedade onde somos constantemente vigiados, de maneira facilitada, ao passo que nos ambientes públicos tradicionais, é “possível guiar com maior segurança a interação pelos aspectos visíveis do cenário e dos observadores presentes”.

O alcance da internet é imensurável, o que é divulgado virtualmente pode ser potencialmente acessado por qualquer pessoa num piscar de olhos, ou seja, a facilidade e comodidade fornecida por esse novo meio é de fato atrativa, mas a viralização pode ser, ao mesmo tempo, extremamente perigosa. “O modelo viral de expansão significa que cada usuário pode compartilhar com vários outros uma informação, o que permite sua disseminação em progressão geométrica” (THIBES, 2014, p. 24-25).

Com a popularização da internet, para além da intensificação da invasão da privacidade, Bauman reproduz o pensamento de que a própria população passou a exercer um movimento de evasão da privacidade, enaltecendo a exposição deliberada de suas informações privadas, com sede de ser constantemente aceito e notado, para formar uma percepção ideal de felicidade. (THIBES, 2014, p. 47)

Portanto, não há como fugir dessa realidade emergente, haja vista que a tecnologia é o futuro da humanidade, já existe uma dependência quase que absoluta dos meios digitais em todas as áreas do conhecimento. Para enfrentar as ameaças desse novo mundo, é preciso que as autoridades responsáveis pela regulação da LGPD estejam à frente das possíveis situações a serem encaradas, impedindo que a internet continue a ser um local sem leis.

3 PANORAMA GERAL DA LGPD E A TRANSFERÊNCIA INTERNACIONAL DE DADOS

Tendo em vista a falta de elementos exemplificativos e ainda de difícil determinação de casos de transferência internacional de dados, se faz necessária a ponderação da temática, a fim de proporcionar um pequeno esclarecimento sobre o capítulo V da recente Lei Geral de Proteção de Dados, suas concepções e aplicabilidades.

3.1 O que é LGPD

A denominada LGPD, foi a sigla adotada para designar a Lei Geral de Proteção de dados, uma Lei Federal, Lei nº 13.709, a qual foi sancionada em 14 de agosto de 2018, a qual busca tutelar à vulnerabilidade do titular de dados pessoais, do tratamento ilegal destes dados realizado por pessoa, instituições e até mesmo na internet, de direito público ou privado, conforme disposto em seu art. 1.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018).

Ademais, possui como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e garantir a transparência do uso desses dados pessoais, partindo do pressuposto que todo dado pessoal tem relevância e valor, com foco na criação de um cenário que proporcione maior segurança jurídica aos cidadãos brasileiros, a partir da padronização de regulamentos e das práticas para promover a proteção aos dados pessoais, conforme os parâmetros internacionais pré-estabelecidos.

A lei determina o que são dados pessoais, além de estabelecer previsões específicas de regulação, tanto no meio físico quanto no digital, como também estipula os sujeitos envolvidos no tratamento dos dados e quais as suas atribuições, responsabilidades e penalidades no âmbito civil. Além disso, a LGPD deve ser observada, se a organização estiver em território brasileiro, ainda que a sede de

manipulação dos dados ou o centro de dados esteja localizado no Brasil ou no exterior, ou até mesmo se há o processamento de informações sobre pessoas, brasileiras ou não.

Ela também autoriza o compartilhamento de dados pessoais com instituições internacionais e com outros países, desde que observados os requisitos nela estabelecidos, garantindo um efetivo controle por parte dos titulares sobre suas informações pessoais.

3.2 Tratamento de Dados Pessoais

Pela determinação *"tratamento de dados pessoais*", entende-se ser toda e qualquer operação realizada com dados pessoais, como, por exemplo, é possível inferir da coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração desses dados.

Todas as hipóteses contempladas para eventual tratamento dos dados pessoais, estão dispostas ao longo do artigo 7° da Lei Geral de Proteção de Dados, para que seja, de fato, efetivada a proteção de dados, desde que tenham sido obtidos em território nacional e a atividade do tratamento tenha como finalidade a oferta ou o fornecimento de bens e/ou serviços, ou seja, o tratamento não se aplica às pessoas naturais que tenham fins exclusivamente particulares e não econômicos.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial,

> administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018).

Os dados são tratados por agentes, que podem ser denominados como controladores, aquele a quem cabe tomar as decisões sobre o tratamento dos dados, isto é, elabora relatórios de impacto e descrição de como ocorrem as operações, e operadores, quem realiza o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. Esses agentes devem manter os registros das operações de tratamento de dados pessoais que realizarem, principalmente, quando não for exigido o consentimento para tal tratamento, o legítimo interesse.

Nesse sentido, o tratamento ocorre através de cinco etapas, sejam elas: a análise dos fundamentos legais; a avaliação das bases legais; o ajuste do tratamento conforme os requisitos para aquela categoria específica de dados; a identificação dos critérios do uso compartilhado de dados; e, a verificação do término do tratamento, à luz da LGPD.

A primeira etapa consiste em confirmar se os princípios e direitos aos usuários estão sendo observados, estabelecendo critérios para selecionar os dados a serem coletados. Para a certificação, são divididos quatro grupos de princípios, de acordo com os objetivos que visam atender, segundo o art. 6° da LGPD. O primeiro grupo consiste em determinar a finalidade, a adequação e a necessidade do tratamento de dados, verificando se os propósitos são legítimos, explícitos e se foram informados ao titular, se existe uma compatibilidade do tratamento com as finalidades que foram passadas ao titular dos dados, e, se houve uma limitação da abrangência, proporcionalidade e não excessividade em relação à finalidade do tratamento destes.

> 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. (BRASIL, 2018).

Em seguida, há o princípio do livre acesso, como sendo uma garantia de consulta facilitada e gratuita sobre a maneira, a duração e a integralidade do tratamento dos dados do titular, juntamente com a qualidade e transparência dos dados, garantindo aos titulares clareza, precisão, atualizações e a relevância destes dados. Consequentemente, estão presentes os princípios da segurança, prevenção e não discriminação, correspondentes a adoção de medidas técnicas e administrativas aptas a previnir quaisquer danos, acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão em virtude do tratamento de dados. No final da primeira etapa, é possível visualizar os princípios da responsabilização e prestação de contas, em que o agente demonstrará a utilização de medidas eficazes e seguras para cumprir o tratamento de dados, conforme as normas de proteção previstas em lei.

Ainda na primeira etapa, é preciso uma análise minuciosa se os direitos dos usuários estão sendo seguidos à risca durante o ciclo de vida desses dados, em conformidade com os princípios citados, por meio do direito de acesso aos dados, onde existe a desimpedida possibilidade de alteração dos dados em detrimento da vontade, haja vista que a manifestação livre, informada e inequívoca, para uma finalidade determinada, é fundamental para o tratamento dos dados. Já com relação ao direito de acesso a informação sobre o uso dos dados, é imprescindível que o titular do dado tenha plena ciência de onde estão os dados, com quem e de que forma estão sendo compartilhados, o que nos leva ao tratamento automatizado destes, uma produção de um perfil comportamental, que possibilita promover decisões destinadas ao perfil do usuário, que, de alguma forma, repliquem os seus interesses.

Quanto à avaliação das bases legais da LGPD, na segunda etapa, são equivalentes as diretrizes que autorizam a atividade pelo controlador, ao passo que seja possível realizar a coleta dos dados com ou sem o consentimento do titular dos dados, evidenciado no art. 7° da Lei em questão. As principais bases legais são o tratamento de dados mediante consentimento do titular e por interesses legítimos do controlador ou de terceiro.

O consentimento, diante do expresso no art. 5°, inciso XII, da LGPD, é a livre, informada e inequívoca manifestação de vontade do titular ao tratamento de seus dados para um fim específico. Portanto, para que o consentimento seja exercido sem vícios, é necessário o conhecimento de todas as informações sobre o uso desses dados, de forma que esteja ciente das suas finalidades e determinações.

> Art. 5º Para os fins desta Lei, considera-se: XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; (BRASIL, 2018).

O interesse legítimo do controlador está estritamente ligado a um fim determinado do uso do dado pessoal, sem que viole o direito de privacidade do titular, ainda que não seja preciso a obtenção de seu consentimento, aliás, somente quando a obtenção do consentimento for inviável. Para tal, deve-se respeitar as expectativas do titular, seus direitos e liberdades fundamentais, tratar somente aqueles dados realmente essenciais, adotar medidas para garantir a transparência

desses modos e informar o titular sobre as hipóteses de tratamento que estão sendo aplicadas para o uso daqueles dados.

Na terceira etapa, são averiguados os requisitos gerais e específicos para certificar se a coleta e o processamento dos dados estão se dando de maneira correta.Os critérios gerais equivalem as bases legais, são a base para fazer operações com os dados sensíveis, explicitadas anteriormente, enquanto os específicos, se não tratados devidamente, podem levar a discriminação de dados do titular, ou seja, a realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Dessa forma, as hipóteses de tratamento dos dados sensíveis estão disciplinadas no art. 11 da LGPD, inicialmente, na vertente de haver o consentimento para o tratamento, onde é registrada a manifestação da vontade do titular, juntamente com a explicação sobre como serão tratados e as situações em que seria indispensável o uso do dado, dando o titular ciência do conhecimento do tratamento e suas possíveis consequências.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro;f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.(BRASIL, 2018).

Ainda no mesmo artigo, são dispostas as hipóteses em que o tratamento dos dados sensíveis ocorrerá sem o consentimento do titular, quando se tratar do

interesse público, da proteção à vida e à segurança do próprio titular dos dados, ou quando estiver relacionado aos dados de crianças e adolescentes, que são incapazes e relativamente incapazes, respectivamente, de consentir livremente, envolvendo, assim, uma série de limitações. No que tange o tratamento de dados das crianças e dos adolescentes, é importante frisar que os dados dados deles, somente poderão ser operados uma única vez, por não poderem ser armazenados ou repassados a terceiros, sem que haja o consentimento expresso de algum responsável legal.

Os critérios de uso compartilhado dos dados, são identificados na quarta etapa do tratamento de dados, onde o usuário deve estar atento às definições e os requisitos para a execução, conforme o art. 5°, inciso XVI da LGPD, ficando visível uma preocupação quanto ao uso com fim econômico. Dentre os requisitos para o compartilhamento dos dados, o usuário deve compreender que é fundamental que haja o seu consentimento, este deve ter o livre acesso às informações sobre o compartilhamento dos seus dados, sendo, além disso, vedada a comunicação ou o uso compartilhado dos dados sensíveis entre os controladores, com o objetivo de auferir vantagem econômica, relacionados à saúde. As exceções, que permitem o compartilhamento dos dados, estão expressas na referida lei.

> 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; (BRASIL, 2018).

Por último, é visualizado como se dá o procedimento para o encerramento do tratamento de dados e as hipóteses para a autorização da conservação desses. Ao tratar do término do tratamento de dados, é relevante observar se a finalidade foi atingida, se os dados ainda se fazem necessários para o alcance de um fim específico. Assim, o procedimento se encerra no fim do período estipulado, quando o titular comunicar a revogação do seu consentimento para a continuidade do tratamento ou quando a autoridade nacional competente determinar, e, se o agente responsável pelo tratamento retirar, anonimizar ou bloquear os dados, o mesmo

deve se dar com todas as entidades jurídicas que partilhem desses dados.

A preservação dos dados somente está legitimada nos casos em que haja um estudo sobre eles, por um órgão de pesquisa habilitado; quando houver a transferência a um terceiro; até mesmo em decorrência do uso exclusivo do controlador; ou que a lei assim determine a obrigação da conservação, se encerrando, portanto, o ciclo do tratamento dos dados pessoais.

3.3 A Transferência Internacional de Dados

Conforme demonstrado no capítulo anterior, com o avanço tecnológico e expansão das barreiras internacionais, houve um aumento da preocupação, por parte dos países, com o armazenamento de dados pessoais e a facilidade de transferência destes dados, sem o devido cuidado. Desse modo, a LGPD, em função da manutenção das relações internacionais com o Brasil, disciplinou em seu normativo a transferência internacional de dados.

Assim, a Lei Geral de Proteção de Dados disciplinou inicialmente no artigo 5°, inciso XV a conceituação legal referente à transferência internacional de dados, a qual refere-se ao movimento de dados pessoais de um país para outro ou para uma organização internacional da qual o país é membro, sendo uma espécie do gênero “tratamento de dados”, diante da disposição do inciso X do mesmo artigo mencionado, enquanto no inciso XVI, elencou-a na modalidade de “uso compartilhado de dados”, conforme anteriormente mencionado e abarcado pelo advogado Raphael Oliveira. (OLIVEIRA, 2021, p. 127)

> 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; (BRASIL, 2018).
> [...]
> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;; (BRASIL, 2018).

Ademais, a Transferência Internacional de Dados é uma forma de compartilhar informações entre países de forma eficiente, segura e rápida. Um

avanço tecnológico que tem sido usado por diversas empresas, instituições e governos para compartilhar documentos, dados e conhecimento entre países, permitindo que informações sejam compartilhadas de forma oportuna e segura. Ela, por conseguinte, permite compartilhar grandes volumes de dados de forma rápida e segura, uilizando de criptografia para proteger os dados.

No entanto, tal transferência internacional de dados não pode vir a ser comparada com um mero acesso à internet, uma vez que estaríamos banalizando a aplicação da conceituação e do próprio regime jurídico, fato esse que culminaria em uma violação com as situações disciplinadas nas hipóteses do artigo 7° da LGPD. Nesse sentido, advogado Raphael Oliveira, ainda se posiciona alegando que:

> A definição legal, contudo, não é suficiente para posicionar os contornos do instituto, porquanto como ressalta a doutrina, a transferência internacional pode compreender sistemáticas de fluxos transfronteiriços descritas a partir de diversos sentidos, ultrapassando, pois, a perspectiva estritamente territorial que ilustra a circulação (tratamento) de um dado para um país terceiro ou organização internacional, como parâmetro insculpido pelo Regulamento Geral Europeu de Proteção de Dados (art. 44º) e refletido no inciso XV do artigo 5º da Lei Geral de Proteção de Dados brasileira. (OLIVEIRA, 2021, p. 127)

A transferência de dados internacionalmente é um tema complexo que envolve questões legais, políticas e sociais. Sob a perspectiva da territorialidade, essa transferência envolve a circulação de dados para além das fronteiras nacionais, o que desafia as jurisdições das Nações e apresenta desafios para a proteção dos dados pessoais e a privacidade dos usuários.

Entretanto, essa perspectiva territorial não é suficiente para compreender a natureza das transferências internacionais de dados em um mundo cada vez mais digital, visto que os dados são criados e compartilhados de forma constante e instantânea em todo o planeta, sendo, assim, armazenados em servidores localizados em outros países. Ou seja, uma virtualização severa da informação e dos dados que acabam por ser armazenados em servidores e nuvens localizados em distintas regiões no mundo, apresentando ainda desafios para a proteção dos dados pessoais, privacidade e segurança cibernética.

Em virtude do apresentado, com a finalidade de uniformizar de certa forma o

conjunto de características presentes na transferência internacional, para distinguir o instituto de outras espécies de tratamento informacional, há classificação para tal, a qual está contemplada no documento internacional *First orientations on transfer of personal data to third countries,* publicado pelo antigo Working Party 29, atual European Data Protection Board, para iluminar a então Diretiva 95/46 da União Europeia, a respeito da transferência de dados para países terceiros*,* que denomina-se de transferência direta e indireta. (OLIVEIRA, 2021, p. 129)

A transferência direta consolida-se com a comunicação e a transmissão de dados entre o titular do dado localizado em um país A com o controlador que está localizado no país B, sem que haja intermediários nessa operação. Enquanto a transferência indireta se subdivide em duas formas de operação de comunicação e envio dos dados, sendo a primeira de controlador para controlador, quando ocorre a materialização da relação entre agentes de tratamento de dados de uma mesma natureza, e, a segunda de um controlador para um operador, configurando uma relação entre agentes de tratamento importadores e exportadores, embora de natureza diversa, com a ressalva de sempre configurar a transferência entre países distintos.

Essa distinção conceitual que leva em consideração a territorialidade e o grau de comunicação entre os agentes de tratamento de dados é demasiado relevante para a conjuntura e relacionamento internacional, pelo fato de estabelecer a legislação, a competência jurisdicional, a responsabilidade de cada agente de tratamento, o rito de aplicação de sanções a serem aplicadas a cada caso concreto de acordo com suas especificidades.

Com base no exposto, de maneira ainda muito superficial, à luz do ordenamento brasileiro, foram levantados os aspectos essenciais da terminologia, a fim de definir brevemente que a transferência internacional de dados se trata de uma espécie do gênero atividade de tratamento de dados, onde um dado pessoal circulará entre os sistemas informacionais de armazenamento de um país soberano, através do comando de um agente de tratamento de dados, um controlador, para o domínio jurisdicional de um país terceiro ou organismo internacional.

3.3.1 *Casos Permissivos à luz do artigo 33 da LGPD*

O artigo 33 da Lei Geral de Proteção de Dados discorre especificamente sobre os casos passíveis de transferência internacional de dados, isto é, o legislador restringiu as hipóteses em que é permitida tal transferência, uma exceção, conforme redação do caput. Para tanto, há de se observar ao menos um dos requisitos do regime especial abarcado pelos incisos do artigo 33, para classificar as ocorrências de transferência internacional de dados, do ponto de vista técnico-jurídico conforme veremos a seguir.

Para que seja considerada legítima a transferência internacional de dados, à luz da LGPD, é necessário que tal ato ocorra para algum país ou organismo internacional que possa de fato proteger os dados de maneira adequada, como trata a Lei, devendo ser analisado pela ANPD. Esse ponto pode ser estritamente comparado ao modelo existente no Espaço Económico Europeu, em que a Comissão Europeia reconheceu certos países como de níveis adequados, como Suíça, Argentina, Japão, entre outros, sob a influência da GDPR, que é um regulamento geral europeu sobre a privacidade e a proteção dos dados pessoais, o qual seria utilizado para embasar a análise para a adequação no Brasil.

Assim, no primeiro inciso do artigo, o legislador intencionalmente expande o rol taxativo para organismos internacionais, equivalentes às pessoas jurídicas de direito internacional público, que, assim como os países, forças governamentais, poderão ser protegidos pela LGPD, por necessitarem de exercer comunicações para as atividades das entidades. Enquanto no segundo inciso, são determinadas as formas de garantias de cumprimento dos princípios, direitos do titular e do regime de proteção de dados, que deverão ser melhor especificados e chancelados por parte da Autoridade Nacional - ANPD - ou seja, será mais um ponto de atenção e semelhança com o modelo europeu, pois ainda carecem de estudo em território brasileiro para a melhor forma de implementação.

Por conseguinte, é garantido no inciso terceiro que os órgãos públicos de inteligência, de investigação e persecução não serão inviabilizados pelas regras contidas na Lei Geral de Proteção de Dados, enquanto no inciso quarto garante-se “a prevalência do direito à vida e da integridade física, o qual não pode ser mitigado por questões relativas à limitação do fluxo de dados pessoais.” (MALDONADO;

Blum, 2020)

No inciso quinto, abarca-se a possibilidade genérica de autorização da transferência pela autoridade nacional, ou seja, pela ANPD, que assim como no direito europeu seria aplicado para situações não habituais. Ao passo que os incisos sexto e sétimo, correspondem, respectivamente, aos compromissos assumidos em acordos de cooperação internacional sobre limitações para o fluxo de dados internacionalmente, e, quando houver a necessidade de execução de políticas públicas ou atribuições legais do serviço público. Isto é, uma restrição da Administração Pública para transferir dados internacionalmente, podendo apenas quando se fizer necessário viabilizar a execução anteriormente citada.

Ao tratar do consentimento específico do titular do dado, o inciso oitavo esclarece a imprescindibilidade de destacar a finalidade de transferência internacional da operação, além de não ser um mero consentimento conforme expresso no artigo 5°, inciso XII da própria LGPD, como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018), terminologia reforçada pelo artigo 8°, §4°. Todavia, para que se enquadre no consentimento da transferência internacional de dados, é preciso que haja um nível maior de robustez, formalidade e clareza do titular, em detrimento do risco que tal ação pode ocasionar, como já aplicado para o tratamento de dados pessoais sensíveis, mas acrescido de informações específicas do caráter internacional da operação de transferência de dados internacionalmente.

> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. (BRASIL, 2018).

É ressaltado no livro “Lgpd: Lei Geral de Proteção de Dados Comentada”, escrito por Viviane Maldonado e Renato Blum, em seu capítulo V, que:

> Portanto, ao contrário do que pode parecer à primeira vista, o consentimento para transferência internacional de dados não é uma via fácil do agente de tratamento para legitimar o ato, mesmo porque, além de específico (destacado), a manifestação precisa ser “livre” (regra geral sedimentada pela LGPD). Isso significa que o

> consentimento não deve ser condição para fornecimento de bens, produtos ou serviços, sendo que, na ocasião de sua obtenção, deve sempre haver a possibilidade de recusa, pelo titular. Além disso, devemos lembrar que o consentimento, em regra, pode ser revogado a qualquer momento pelo titular e, não bastasse, sua forma de obtenção é comumente passível de questionamento. Some-se a tudo isso o fato de que transferências internacionais de dados, normalmente, são decorrentes de decisões de negócio ou de necessidades relativas à infraestrutura tecnológica dos agentes de tratamento, as quais não se sujeitam, obrigatoriamente, à vontade do titular.

Em seguida deparamo-nos com o inciso nono, dispositivo elencado às hipóteses previstas nos incisos II, V e VI do artigo 7° da LGPD. Assim, quando for necessário cumprir as obrigações legais ou regulatórias pelo controlador; executar algum contrato ou realizar procedimentos preliminares relacionados ao contrato do qual o titular faz parto, à pedido deste; ou em caso de exercício regular de direitos em processo judicial, administrativo ou arbitral, relativos à constituição do corpo probatório, nestes casos a transferência internacional de dados será permitida.

Por fim, o parágrafo único do artigo 33° da LGPD contempla duas perspectivas nas quais a primeira se refere às pessoas jurídicas de direito público, presentes no parágrafo único do art. 1° da Lei 12.527/2011, e a segunda às pessoas jurídicas de direito privado. Enquanto as pessoas jurídicas de direito público podem dispensar as outras medidas de proteção na transferência internacional de dados em caso de ser considerado adequado o grau de proteção de dados, quando provocada a Autoridade Nacional de Proteção de Dados, às pessoas jurídicas de direito privado possuem abertura com base na referida lei para provocar a ANPD, para que também seja avaliado o nível de adequação da proteção de dados pessoais designada pelo país ou organismo internacional, observando cautelosamente, com base nos históricos legislativos, o emprego do termo “responsável” da LGPD na transferência internacional de dados sensíveis, o qual corresponde ao papel do controlador.

4 A TRANSFERÊNCIA INTERNACIONAL DE DADOS DENTRO DO DIREITO À PRIVACIDADE NA PRÁTICA

Após as considerações teóricas apontadas acima, será brevemente analisado a seguir como o direito à privacidade se aplica na transferência internacional de dados pessoais, principalmente frente ao caso da Equifax, e, as aplicações do que foi visto anteriormente e as consequências do caso, supondo-se ocorrido na conjuntura brasileira.

4.1 A importância da Transferência Internacional de Dados frente à Privacidade

A transferência internacional de dados é um tema fundamental no contexto da privacidade e proteção de dados pessoais, pois envolve a movimentação de informações sensíveis entre diferentes países e jurisdições, que podem ter leis e regulamentações distintas para a proteção de dados pessoais, como já demonstrado nos capítulos anteriores.

Nesse teor, a transferência internacional de dados é essencial para a manutenção da economia globalizada e para o funcionamento de diversas atividades empresariais, incluindo a prestação de serviços de tecnologia da informação e comunicação, a pesquisa e desenvolvimento científico, e a cooperação internacional entre organizações. Todavia, o direito à privacidade está intrinsecamente conectado a essa transferência, haja vista que deve ser realizada com a proteção da privacidade dos titulares dos dados, garantindo que as informações pessoais não sejam acessadas, utilizadas ou divulgadas sem o consentimento específico e informado de seus proprietários.

Segundo Joseph, Cannataci, Relator Especial da ONU sobre a Privacidade, ainda é um desafio crescente estabelecer a transferência de dados pessoais entre países, perante a uma economia global interconectada, sendo preciso o esforço conjunto dos governos, empresas e sociedade civil para encontrar soluções equilibradas que protegem a privacidade dos indivíduos nesse processo tão delicado. Para Daniel Castro, diretor do Centro de Inovação de Tecnologia da Informação da Fundação Tecnologia da Informação e Inovação, a transferência de dados transfronteiriça é uma questão crítica para as empresas globais que precisam compartilhar informações entre diferentes regiões geográficas, mas também é uma

questão crítica para os governos que precisam garantir a privacidade dos dados pessoais de seus cidadãos.

Para isso, é importante que os países tenham leis e regulamentações que garantam um nível adequado de proteção de dados pessoais, estabelecendo requisitos e padrões mínimos para a coleta, processamento, armazenamento e transferência de dados pessoais. Além do mais, as empresas que realizam tal operação devem adotar medidas de segurança adequadas para proteger as informações dos titulares, como criptografia, anonimização e pseudonimização de dados.

Portanto, a Lei Geral de Proteção de Dados é um grande passo para o Brasil na inserção e adequação frente a tantas regulamentações internacionais já existentes, como o Regulamento Geral sobre Proteção de Dados, na União Europeia, e, o Marco Civil da Internet. Porém, a lei precisará ainda passar por aprimorações para cobrir as lacunas existentes e que vierem a ser identificadas futuramente, sendo pauta para inúmeras discussões no ambiente empresarial brasileiro, com a intenção de trazer benefícios comerciais e econômicos no fluxo internacional de dados.

Diante do exposto, a privacidade é essencial para a efetiva realização da transferência internacional de Dados, já que tudo se encontra inserido no contexto globalizado e empresarial, mas de forma segura, de acordo com os dispositivos legais, com responsabilidade, respeito à privacidade dos titulares dos respectivos dados pessoais, garantindo a segurança tecnológica e jurídica tanto na transmissão, no uso e movimentação dessas informações, conforme pode ser vislumbrado no caso apresentado a seguir.

4.2 Caso de vazamento dos dados na Transferência Internacional de Dados

A Equifax, fundada em 1899, com sede em em Atlanta, Georgia, EUA, é uma empresa de serviços de informação de crédito americana que fornece soluções de informação sobre crédito e análise para ajudar empresas e consumidores a tomarem decisões sobre crédito e finanças. Ademais, coleta informações de crédito e histórico de pagamento de consumidores e empresas em todo o mundo e fornece acesso a essas informações para empresas, governos e outras organizações que precisam avaliar o risco financeiro e de crédito.

Além de serviços de informação de crédito, a Equifax também fornece soluções

de prevenção de fraudes, gestão de portfólio, marketing e análise de dados, operando em 24 países distribuídos pela América, Europa e a região da Ásia-Pacífico.

A empresa ganhou destaque em 2017 quando sofreu um grande vazamento de dados, em que revelou que informações pessoais de cerca de 143 milhões de pessoas haviam sido comprometidas em um ataque cibernético. As informações incluíam nomes, endereços, datas de nascimento, números de Seguro Social e, em alguns casos, números de cartão de crédito. Sendo considerado um dos maiores na história dos EUA, além de ter um impacto significativo na confiança do público em relação à segurança de dados.

O vazamento foi amplamente divulgado pela mídia internacional e levou a investigações por parte das autoridades regulatórias em vários países. A Equifax enfrentou críticas significativas por sua resposta inicial ao vazamento e por não ter implementado medidas adequadas de segurança de dados.

O caso se iniciou em março de 2017, onde a Apache Foundation publicou uma atualização que corrigiria a vulnerabilidade apresentada na plataforma Apache Struts (CVE-2017-5638), uma estrutura de aplicativo de código aberto que oferece suporte ao aplicativo da Web do portal de disputas online. Contudo, hackers exploravam a vulnerabilidade para dominar os aplicativos desenvolvidos por meio da plataforma, fato esse que levou o US-CERT a emitir um alerta de segurança avisando as empresas dos EUA sobre essa falha e seus riscos (EQUIFAX, 2017).

Nesse contexto, a equipe de TI da Equifax emitiu um comunicado por e-mail, para uma lista de endereços da empresa, porém ela estava desatualizada, visto que não incluía todos os administradores de sistemas, levando a uma atualização incompleta dos servidores. Assim, os hackers descobriram uma versão vulnerável do Struts onde obtiveram as credenciais de acesso das informações estritamente confidenciais dos clientes.

Logo os invasores iniciaram as consultas aos bancos de dados, chegando a um repositório de dados com informações pessoais de identidade, como nomes de usuário e senhas não criptografadas, os quais possibilitaram a eles o alcance de 48 bancos de dados.

> Depois de fazerem a extração, os dados foram baixados em arquivos pequenos, com protocolos padrão web criptografados, para fazer com que o tráfego de rede parecesse normal. Os dados foram filtrados durante 76 dias. Isso só foi descoberto em 29 de julho de

> 2017, durante as verificações de rotina do status operacional e da configuração dos sistemas de TI. (BRITO, 2018)

Após a verificação das atividades suspeitas, a equipe de segurança contratou uma empresa de segurança cibernética, a Mandiant, para apurar de maneira mais abrangente o impacto da invasão, onde foi constatado que cerca de 143 milhões de informações pessoais foram violadas, uma infração direta e clara à privacidade dos usuários.

A empresa trabalhou em estreita colaboração com as autoridades para investigar a origem do vazamento e implementar medidas de segurança adicionais para evitar futuros vazamentos, como também sofreu várias ações judiciais e multas regulatórias em relação ao vazamento.

Em 2019, a Comissão Federal de Comércio dos EUA (FTC) multou a Equifax em 575 (quinhentos e setenta e cinco) milhões de dólares por não proteger os dados dos consumidores. A multa foi a maior já aplicada pela FTC em um caso de privacidade de dados. Outrossim, em 2020, a empresa foi intimada a pagar 700 (setecentos) milhões de dólares para resolver ações judiciais civis e criminais relacionadas ao vazamento de dados.

A empresa também incitou críticas por sua resposta inicial ao vazamento e por não ter implementado medidas de segurança de dados. O incidente levou a mudanças nas políticas de segurança e privacidade de muitas empresas de tecnologia, que se concentram em utilizar atualmente a criptografia e outras medidas para proteger a privacidade dos usuários. Certamente, o incidente teve um impacto significativo na confiança do público em relação à segurança de dados e levou a uma série de mudanças regulatórias em todo o mundo para fortalecer a proteção de dados pessoais.

4.3 Aplicação da jurisdição brasileira no caso de vazamento de dados na transferência internacional

O sistema de proteção de dados brasileiro recebeu grande influência das regulações estrangeiras, como evidenciado nos capítulos anteriores, porém o tratamento jurídico, ainda que instituído, não encontra-se juridicamente aperfeiçoado para lidar com total segurança e autonomia das questões relacionadas à transferência internacional de dados. Apesar de não possuir ainda jurisprudências

consolidadas perante o assunto com o advento da nova lei, observa-se que a temática passa a ser abordada para quanto da desconfiguração do instituto em caso concreto, como no julgado do Tribunal Regional do Trabalho da 4° Região:

> [...] A defesa refuta e não se pode presumir, diante da falta de provas, a ocorrência de transferência de dados internacionais, fato extraordinário.
>
> Afasto o pedido 3.
>
> Sobre incidentes de segurança, a Portaria 11/2021 da ANPD trata no item 6, regulamentado com o seguinte conteúdo[2]:
>
> Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.
>
> O art. 47 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) determina que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito [...].

É evidente quando alegado no julgado que o caso não se trata de uma transferência internacional de dados, mas apenas de um descumprimento sistemático referente à proteção de dados por parte da reclamada, uma clara violação à privacidade e ao sigilo pelo compartilhamento indevido entre controladores e operadores, os quais não foram previamente indicados os encarregados, expondo sem necessidade os dados que se encontravam vulneráveis da reclamante.

Nesse sentido, diante do caso de vazamento internacional de dados da empresa de serviços de informação de crédito americana, Equifax, onde na transferência de informações entre suas bases locadas em múltiplos países, foi alvo de um ataque hacker que exportou informações de cunho notadamente pessoais e sensíveis, nota-se que se o ocorrido houvesse se situado nas relações jurídico-sociais brasileiras na contemporaneidade, isto é, após a outorga da Lei Geral de Proteção

de Dados, as tratativas seriam diferentes.

O ocorrido se enquadra notoriamente na hipótese prevista no parágrafo único, do artigo 33° da Lei Geral de Proteção de Dados, em que a pessoas jurídicas de direito privado em questão, caso o processo se iniciasse da base de dados alocada no Brasil, a instituição deveria ter provocado a ANPD, para que fosse avaliado o nível de adequação da proteção de dados pessoais para um outro país e do uso compartilhado dos dados sensíveis entre as filiais de operação, como a previsão do inciso primeiro e quinto do mesmo artigo indica, a fim de definir especificamente o controlador e os operadores, visto que não cabe à vontade de cada titular de dado submetido a Equifax, visto que são necessidades relativas à própria estrutura tecnológica dos agentes de tratamento que estão dispostos em países diversos.

Ademais, por ser uma pessoa jurídica de direito privado, seria estritamente recomendado que a empresa estabelecesse em seus contratos de adesão e outras negociações cláusulas-padrão contratuais específicas para esse tratamento e armazenamento transfronteiriço dos dados dos clientes, de acordo com o disposto no inciso II, alínea “b” do artigo 33° da LGPD. Cabe ressaltar que as atividades deveriam estar particularmente vinculadas às hipóteses disciplinadas no artigo 7° do mesmo diploma legal, especialmente pelo controlador para o cumprimento da obrigação legal instituída na adesão dos serviços, conforme o inciso II.

No entanto, como a Equifax não se resguardou de todas as maneiras disponíveis, possibilitando que hackers invadissem o sistema, em decorrência da atualização incompleta dos servidores, fato esse que deixou a plataforma Apache Struts (CVE-2017-5638) ainda mais vulnerável, que levou ao vazamento de aproximadamente 143 milhões de dados sensíveis, esta poderia ser responsabilizada pelo dano gerado aos clientes.

Assim, a empresa haveria de ser sancionada e responder pelo atentado ao direito de privacidade de milhões de usuários. Contudo, as punições em razão das violações à LGPD podem não suprir o que se é esperado pela referida legislação, de maneira a assegurar realmente a proteção dos dados pessoais sujeitos aos tratamentos realizados pela Equifax, na análise proposta neste tópico.

O ponto de maior destaque, que deixa a desejar das sanções a serem estipuladas, é a limitação de até 50 milhões de reais aos valores das multas simples no Brasil, ou alcançando 2% do faturamento da empresa, pessoa jurídica de direito

privado, baseado no seu último exercício, excluídos os tributos, haja vista que entende-se que as multas devem ter um caráter coercitivo, a qual, mediante ameaça de excussão patrimonial, objetiva compelir o executado a realizar o fixado pelo juiz. Logo, para que os dados pessoais fossem realmente respeitados e tratados devidamente pelas grandes instituições jurídicas de direito privado, não deveria existir tal limite previsto no artigo 52 da LGPD.

De modo geral, a referida Lei estabelece uma série de sanções para assegurar que não haja o descumprimento das normas de proteção de dados pessoais, garantias satisfatórias tanto para empresas públicas quanto privadas, as quais requerem:

> [...] criteriosa apreciação da gravidade, da natureza das infrações, dos direitos pessoais afetados, a boa-fé, vantagem auferida e condição econômica do infrator, o grau do dano, a cooperação do infrator, a adoção de política de boas práticas e governança e a pronta adoção de medidas corretivas. (SILVA, ROSSI, NEVES, 2021, p. 3)

Dentre as outras sanções estipuladas, podemos referenciar a advertência, onde a empresa pode ser anunciada formalmente pelo órgão responsável pela fiscalização da LGPD; a publicização da infração, o que pode afetar a sua imagem perante o mercado; e, o bloqueio ou eliminação dos dados, em que a empresa será obrigada a bloquear ou eliminar os dados pessoais que foram objeto da infração, além de outras medidas que sejam necessárias para minimizar os danos causados aos titulares dos dados.

Em casos extremos, como o caso em questão, se for determinado assim em juízo, a empresa poderia ainda ser impedida de operar devido a incapacidade técnica para proteger os dados de seus clientes, ou seja, a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, além de ter a suspensão parcial ou total do funcionamento do banco de dado pelo órgão fiscalizador.

. Além disso, a empresa concomitantemente sofreria, não só as sanções estipuladas pela Lei Geral de Proteção de Dados, como também a responsabilidade civil pelos atos praticados, tendo em vista que na hipótese imaginária onde a situação tivesse se dado em um contexto brasileiro. A jurisdição estaria alocada

estritamente nos inciso II e III do artigo 21 do Código Civil, onde é sintetizado que compete à autoridade judiciária brasileira processar e julgar as ações em que no Brasil tiver de ser cumprida a obrigação ou o fundamento seja fato ocorrido ou ato praticado no Brasil.

> Art. 21. Compete à autoridade judiciária brasileira processar e julgar as ações em que: I - o réu, qualquer que seja a sua nacionalidade, estiver domiciliado no Brasil; II - no Brasil tiver de ser cumprida a obrigação; III - o fundamento seja fato ocorrido ou ato praticado no Brasil.(BRASIL, 2018)

Em todo caso, a criação e entrada em vigor da Lei Geral de Proteção de Dados Pessoais é um avanço em nosso País, na medida em que representa um grande avanço para o Brasil, uma vez que coloca o país em sintonia com as melhores práticas internacionais de proteção de dados pessoais. A LGPD fortalece os direitos fundamentais de privacidade e autodeterminação das pessoas, o que é essencial para um mundo cada vez mais digital e conectado, beneficiando a economia brasileira, por criar um ambiente de confiança para o tratamento de dados pessoais e estimular a inovação e o desenvolvimento de novos negócios no setor de tecnologia da informação.

A proteção adequada de dados pessoais é crucial para evitar abusos e fraudes dentro do meio digital e suas movimentações, garantindo a segurança e transparência das relações sociais, isto é um vislumbre da comunidade internacional em busca de caminhos e modelos jurídicos inovadores para fortalecer esta proteção.

Isso mostra, portanto, a importância da adoção das medidas de proteção de dados por toda e qualquer entidade nacional ou internacional, uma vez que a informação se tornou um dos bens mais preciosos na sociedade contemporânea, o ambiente social no qual se concretizou a ideia de privacidade informacional, onde cada indivíduo deve possuir o controle de como seus dados estão sendo geridos, e, as instituições devem primar pela segurança informacional e jurídica de seus usuários. Evitando, desta forma, um caso como o da Equifax diante de um cenário legitimamente brasileiro.

5 CONCLUSÃO

A presente pesquisa abordou anteriormente o modo como a privacidade, inserida em um contexto globalizado, em seu sentido stricto sensu, onde o titular dos dados possui a capacidade de estabelecer as delimitações quanto ao seu direito de tornar os seus dados públicos ou não, direito formalmente reconhecido, a partir da publicação do pioneiro artigo de Warren e Brandeis, impacta fortemente o atual modelo jurídico legal positivado pela Lei Geral de Proteção de Dados, com especial ênfase no regime específico desenhado pelo capítulo V, a Transferência Internacional de Dados.

O capítulo, nesse contexto, foi proposto para definir a transferência internacional de dados e seus demais desdobramentos, como espécie do gênero atividade de tratamento de dados, com o objetivo de representar a operação na qual um dado pessoal circulará a partir de um comando de um agente de tratamento de uma jurisdição nacional soberana, para o domínio jurisdicional de um país terceiro ou organismo internacional, segundo Raphael Oliveira. (2021, p. 209)

No entanto, se faz impossível desconsiderar que o direito à proteção de dados tem inovado e permanece modificando os espaços da tomada da decisão jurídica, apresentando cenários transnacionais, os quais em matéria de proteção de dados acelerou o processo de construção da norma jurídica por instâncias bilaterais, que baseiam-se nos instrumentos de cooperação jurídica internacional.

Com o avanço da sociedade sendo cada vez mais guiada por dados, a ideia de privacidade informacional está sendo moldada pela proteção dos direitos dos indivíduos de controlar seus dados pessoais por meio da autodeterminação informativa. O conflito resultante da desigualdade de poder entre os detentores de dados e aqueles que os manipulam é a causa do problema de privatividade na atualidade, desequilíbrio social esse que pode facilmente resultar em violação do princípio da privacidade. Portanto, a proteção rigorosa dos dados pessoais sensíveis dentro da transferência internacional é uma ferramenta crucial para alcançar a segurança jurídica pretendida.

É nesse sentido que a investigação de um mecanismo que recebeu pouquíssima disciplina legislativa, buscou compreender como e com qual profundidade os diplomas internacionais pertinentes adotaram a lógica para que a operação fosse

positivada, e como a experiência deles, especialmente do sistema Europeu, determinou o modo como esses mecanismos serão tratados no território brasileiro. Diante dessa nova Ordem Informacional, uma sociedade baseada em informações, responsável por proporcionar o surgimento e desenvolvimento do direito à proteção de dados.

Perante ao evidenciado, ficou evidente que o ordenamento jurídico brasileiro estabeleceu um regime de transferência internacional de dados. Contudo, uma análise das diversas normas que regulam o intercâmbio de informações além das fronteiras do país revela que esse conjunto de regras ainda não está completamente consolidado, definido ou finalizado, mas sim em processo de construção.

Assim, para que esse conjunto de normas e princípios, que têm como objetivo regular a transferência de dados transfronteiriços à luz da ordem jurídica brasileira, possa estar em conformidade com os preceitos constitucionais e legais previstos, de maneira a resguardar o direito à privacidade dos titulares dos dados, não pode apenas configurar uma ficção jurídica de um processo estruturado para garantir resultados, caso toda a construção estatal seja operada com sucesso, é necessário que seja posto em prática, conforme sintetizado brevemente sobre as tratativas num caso de vazamento de dados como a da empresa norte-americana Equifax, sob a ótica do sistema jurídico brasileiro, na sua aplicação literal amoldada à situação hipotética.

Através do estudo das fontes doutrinárias, legislativas e jurisprudenciais, nacionais e estrangeiras acima referidos, é possível concluir, portanto, que além da aplicação das normas estipuladas, principalmente correspondendo às diretrizes do artigo 33 da Lei Geral de Proteção de dados, a Autoridade Nacional de Proteção de dados possui a obrigação de fiscalizar e propiciar a eficácia das normas de proteção de dados sujeitas à consolidação e ao seu bom desempenho.

Apesar da tutela constitucional e da existência de legislações sobre o tema, as práticas violadoras permanecerão em ascensão, impondo à ANPD e aos próprios legisladores o trabalho de suprir as lacunas da regulamentação, realizando maior apreciação quanto à temática proposta nesta pesquisa, uma vez que o Brasil sequer foi considerado um país de nível adequado em proteção de dados pelas outras Nações. Dessa maneira, espera-se que a ANPD seja ativamente atuante no procedimento de obtenção de uma decisão de adequação do Brasil pelas

autoridades europeias.

Ademais, se o Estado não for considerado adequado, em nível de proteção de dados, pela ANPD, outra solução plausível é a utilização de cláusulas contratuais-padrão, em que constem as obrigações das partes envolvidas na transferência internacional de dados, além dos direitos dos titulares dos dados a serem transferidos. Logo, observa-se que a ANPD enfrenta desafios quanto a regulação dos mecanismos de transferência internacional, visto que ainda não foi realizada uma análise do grau de proteção adequado de leis de outros países em relação à LGPD, nem disponibilizado um modelo oficial de cláusulas contratuais-padrão e tampouco validou as cláusulas contratuais específicas e as normas corporativas globais.

Portanto, a privacidade dentro da transferência internacional de dados sensíveis, há de ser pauta de futuros e importantes debates no ambiente empresarial e acadêmico brasileiro, pois se a temática fosse introduzida aos pensadores de Direito atuais, poderíamos chegar a soluções que acompanhem as contínuas evoluções tecnológicas, trazendo, assim, benefícios comerciais, econômicos e maior segurança nas movimentações de informações transfronteiriças.

A exemplos de medidas a serem adotadas, é possível depararmos com a utilização de criptografia, como técnica para transformar as informações em um código indecifrável, assim como a celebração de acordos e tratados internacionais, a fim de estabelecer regras claras para a transferência internacional de dados, garantindo maior proteção dos dados dos titulares frente a uma uniformização de parâmetros legais, ou seja, a adoção de padrões, sanções mais severas e boas práticas de segurança da informação pela comunidade internacional como uma forma efetiva de proteger os dados dos titulares durante a transferência internacional, evitando, assim, que os dados sejam expostos sem permissão.

REFERÊNCIAS

AVILA, Ana Paula Oliveira ; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, v. 4, n. 3, p. 167-200, 2017. Disponível em: https://www.scielo.br/j/rinc/a/kdqYTvJ7GWsS75twG6f37Bc/?format=pdf&lang=pt. Acesso em: 06 jun. 2022.

BARROS, Mariana. Tratamento de dados na LGPD: O que é e Como Fazer?. **Legalcloud**. 2020. Disponível em: https://legalcloud.com.br/tratamento-de-dados-lgpd/. Acesso em: 25 jun. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 maio 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#:~:text=Art.%201%C2%BA%20Esta%20Lei%20disp%C3%B5e,da%20personalidade%20da%20pessoa%20natural. Acesso em: 15 maio 2022.

BRITO, Paulo. Um ano de invasão da Equifax. Entenda como aconteceu. **CISO Advisor**. 2018. Disponível em: https://www.cisoadvisor.com.br/um-ano-de-invasao-da-equifax-entenda-como-aconteceu/. Acesso em: 20 mar. 2023.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Scielo**. Sequência: Estudos Jurídicos e Políticos, v. 38, n. 76, p. 213-240, 2017. Disponível em: https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?format=html. Acesso em: 09 jun. 2022.

COSTA JUNIOR, Paulo José da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

CUBELLS, Pablo Andrade. **Multa coercitiva (Astreintes)**: do CPC 1973 ao CPC 2015. 2015. 50 f. Monografia (Bacharelado em Direito) Universidade de Brasília - UNB. Brasília, 2015.

EQUIFAX INC. **Equifax divulga detalhes sobre incidente de segurança cibernética e anuncia mudanças de pessoal**. 2017. Disponível em: https://investor.equifax.com/news-events/press-releases/detail/237/equifax-releases-details-on-cybersecurity-incident. Acesso em: 20 mar. 2023.

EQUIPE ÂMBITO JURÍDICO. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro: Da emergência de uma revisão conceitual e da tutela de dados pessoais. **ÂMBITO JURÍDICO**. 2008. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/privacidade-vida-privada-e-intimidade-no-ordenamento-juridico-brasileiro-da-emergencia-de-uma-revisao-conceitual-e-da-tutela-de-dados-pessoais/. Acesso em: 01 jun. 2022.

FERNANDES, Milton. **Proteção civil da intimidade**. São Paulo: Saraiva, 1977.

GUIMARÃES, Gabriel Stagni. **A importância da lei geral de proteção de dados pessoais em face do avanço tecnológico da sociedade:** a proteção dos dados pessoais como direito fundamental. 2021. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito da Pontifícia Universidade Católica de São Paulo, São Paulo, 2021.

JOELSONS, Marcela. Desafios atuais para a transferência internacional de dados pessoais no Brasil - Federasul. **Souto Correa Advogados**. 2022. Disponível em: https://www.soutocorrea.com.br/artigos/desafios-atuais-para-a-transferencia-internacional-de-dados-pessoais-no-brasil/. Acesso em: 24 mar. 2023.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados comentada**.** 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane; BLUM, Renato. Art. 33 - Capítulo V. Da Transferência Internacional de Dados - Lgpd: Lei Geral de Proteção de Dados Comentada | Jusbrasil Doutrina. **Jusbrasil**. São Paulo (SP): Editora Revista dos Tribunais. 2020. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/secao/1233940148/art-33-capitulo-v-da-transferencia-internacional-de-dados-lgpd-lei-geral-de-protecao-de-dados-comentada?utm_source=google&utm_medium=cpc&utm_campaign=doutrina_search_v3&utm_term=&utm_content=adgroup_dinamico&campaign=true&gclid=Cj0KCQiAq5meBhCyARIsAJrtdr7cgSLQr4UeDKH34R_qs5xD5TGz26j9W7ILRtNqxBImREWLGdaDkMwaAlEBEALw_wcB. Acesso em: 17 jan. 2023.

MARIA, José Serpa de Santa. **Direitos da personalidade e a sistemática civil geral**. Campinas: Julex, 1987.

MENDES Laura S. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. Universidade de Brasília - UNB Faculdade de Direito Departamento de Pós-Graduação. 2008. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf. Acesso em: 01 jun. 2022.

MINISTÉRIO PÚBLICO. **O que é a LGPD?: Lei Geral de Proteção de Dados**. Mpf (COLOCAR A DATA DE PUBLICAÇÃO). Disponível em: http://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd. Acesso em: 25 jun. 2022.

OLIVEIRA, Raphael Rodrigues Valença de. **Regime de transferência internacional de dados à luz da ordem jurídica brasileira**. 2021. 242f. Dissertação (Mestrado em Direito) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2021.

PILATI José; OLIVO; Mikhail Vieira C. **Um novo olhar sobre o direito à privacidade: o caso** Snowden e pós modernidade jurídica. Dialnet. Vol. 35, Nº. 69, 2014, p. 281-300. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=4934129. Acesso em: 30 maio 2022.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**. Comentários à Lei nº 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: comentários à Lei nº 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

RAMOS Cristina M. **O direito fundamental à intimidade e à vida privada**. E-gov. 2011. Disponível em: http://www.buscalegis.ufsc.br/revistas/files/anexos/33174-41996-1-PB.pdf. Acesso em: 01 jun. 2022.

RIO GRANDE DO SUL. Tribunal Regional do Trabalho Da 4ª Região. Vara Do Trabalho de Montenegro. **Ação Civil Coletiva 0020043-80.2021.5.04.0261**. Inadequação à Lei Geral de Proteção de Dados. Litigância de Má-fé. Autor: Sind Trab Nas Inds De Alimentação De Montenegro. Réu: Cooperativa Dos Citricultores Ecológicos Do Vale Do Cai Ltda. Relatora: Ivanise Marilene Uhlig de Barros. Sentença Publicada em: 13 jul. 2021. Disponível em: https://pje.trt4.jus.br/consultaprocessual/detalhe-processo/0020043-80.2021.5.04.0261/1#40302f5. Acesso em: 22 mar. 2023.

SILVA, Raphaela; ROSSI, Beatriz; NEVES, Nathalia. A aplicação de sanções administrativas pelo descumprimento da LGPD. **Consultor Jurídico.** 2021. Disponível em: https://www.conjur.com.br/2021-set-30/opiniao-aplicacao-sancoes-descumprimento-lgpd. Acesso em: 23 mar. 2023.

SOARES, Luciano. A Privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais. **Publica Direito**. (colocar o ano de publicação). Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/bh/luciano_soares_maia.pdf. Acesso em: 30 maio 2022.

VIEIRA, Tatiana M. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Editora SAFE. 2007. p. 1-326. Disponível em: http://www.egov.ufsc.br/portal/conteudo/pref%C3%A1cio-direito-privacidade-na-sociedade-da-informa%C3%A7%C3%A3o. Acesso em: 31 maio 2022.

WANG, Ping; JOHNSON, Christopher. **CYBERSECURITY INCIDENT HANDLING**: A CASE STUDY OF THE EQUIFAX DATA BREACH. Issues in Information Systems, v. 19, n. 3, p. 150–159, 2018. Disponível em: https://iacis.org/iis/2018/3_iis_2018_150-159.pdf.