UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO "PROFESSOR JACY DE ASSIS"
BACHARELADO EM DIREITO

VICTOR RODRIGUES NASCIMENTO VIEIRA

LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE DA TUTELA DOS DADOS PESSOAIS EM CASOS DE TRANSFERÊNCIA INTERNACIONAL

UBERLÂNDIA/MG
JUNHO DE 2019

VICTOR RODRIGUES NASCIMENTO VIEIRA

LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE DA TUTELA DOS DADOS PESSOAIS EM CASOS DE TRANSFERÊNCIA INTERNACIONAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade Federal de Uberlândia, Faculdade de Direito "Professor Jacy de Assis", como exigência parcial para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Thiago Paluma Gonçalves Rocha

UBERLÂNDIA/MG

JUNHO DE 2019

Neste momento tão especial da minha vida, em que finalizo mais um ciclo, não poderia deixar de agradecer a todos os que foram minha base e minha motivação diária. Agradeço aos meus pais, Kátia e Carlos Ernane. Agradeço à toda a minha família, especialmente aos meus avós, Neide e Hugo e à minha tia Valéria. Agradeço aos meus amigos que tornaram os meus dias menos densos e muito mais agradáveis.
Enfim, agradeço a todos que, de alguma forma, estiveram presentes nesta caminhada comigo. Muito obrigado!

RESUMO:

O tema desta monografia é a tutela dos direitos de liberdade, privacidade e livre desenvolvimento da pessoa natural em casos de transferência internacional de dados pessoais à luz da Lei nº 13.709, de 14 de Agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD). O objetivo geral deste estudo é investigar as hipóteses de transferência internacional de dados pessoais conferidas pela LGPD e os objetivos específicos são dois, quais sejam: identificar qual a legislação aplicável e identificar qual o órgão judicial competente para julgar casos de responsabilidade civil decorrentes da violação dos direitos dos titulares de dados pessoais. Até a edição da LGPD o Brasil tinha uma lacuna legislativa no que diz respeito, especificamente, à proteção e transferência internacional de dados pessoais. Entretanto, com a entrada em vigor da LGPD, 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, estará sujeita à imperatividade das leis brasileiras. Além disso, com a LGPD, o Brasil entrou para o time dos países que contam com um nível adequado em termos de proteção de dados pessoais. Deste modo, a partir da entrada em vigor da LGPD, o Brasil poderá, sem nenhum óbice jurídico, ser um país destinatário de dados pessoais oriundos de países que exigem um nível adequado de proteção. Com o advento da lei, os requisitos e as hipóteses para a transferência internacional de dados foram expressamente previstos. Assim, conforme art. 33 da LGPD, a transferência internacional de dados só será permitida em nove hipóteses, ressalvadas as exceções legais previstas no ordenamento jurídico brasileiro. Ademais, qualquer titular de dados pessoais contará com o respaldo dos princípios da finalidade, minimização da coleta e retenção mínima. Estes princípios dispõem que os dados deverão ser utilizados apenas para a finalidade específica para a qual foram coletados, devendo ser coletados somente os dados mínimos necessários para que se possa atingir tal finalidade, devendo ser imediatamente excluídos após atingida esta finalidade. Por fim, ressalte-se que o tema abordado envolve vários campos do Direito, bem como tratados e convenções estrangeiras e noções de Ciência da Computação. Ademais, a LGPD é extremamente recente, não entrou em vigor e ainda será enfrentada pelos tribunais e órgãos de defesa e proteção do consumidor, cabendo a estes interpreta-la e assegurar a tutela dos direitos de liberdade, privacidade e livre desenvolvimento da pessoa natural.

Palavras-chave: Lei Geral de Proteção de Dados. Transferência Internacional de Dados. Privacidade. Liberdade. Livre desenvolvimento da personalidade da pessoa natural.

ABSTRACT:

The theme of this undergraduate thesis is the protection of the rights of liberty, privacy and free development of the natural person in cases of international transfer of personal data under Law No. 13,709 of 14 August 2018, known as the General Data Protection Act (LGPD). Therefore, the main objective of this study is to investigate the hypotheses of international transfer of personal data conferred by LGPD and the specific objectives are two: identify the applicable legislation and identify which judicial body is competent to judge cases of civil liability arising from the infringement of the rights of the holders of personal data. Until the edition of LGPD Brazil had a legislative gap with regard, specifically, to the protection and international transfer of personal data. However, with the entry into force of the LGPD, any collection operation, storage, custody and processing of records, personal data or communications by connection providers and Internet applications, in which at least one of these acts occurs in national territory, will be subject to the imperativity of Brazilian laws. In addition, with LGPD, Brazil has joined the team of countries that have an adequate level in terms of protection of personal data. Thus, from the entry into force of the LGPD, Brazil can, without any legal impediness, may be a country that is a recipient of personal data from countries that require an adequate level of protection. With the advent of the law, the requirements and hypotheses for the international transfer of data have been expressly foreseen. So, according to art. 33 of the LGPD, the international transfer of data will only be allowed in nine hypotheses, except for the legal exceptions provided for in the Brazilian legal order. Moreover, any personal data subject will have the support of the principles of the purpose, minimisation of collection and minimum retention. These principles provide that the data should be used only for the specific purpose for which it was collected, only the minimum data necessary to achieve this purpose must be collected and immediately excluded after this purpose has been achieved. Finally, it should be pointed out that the theme addressed involves several fields of Law, as well as foreign treaties and conventions and notions of Computer Science. Moreover, the LGPD is extremely recent, has not entered into force and will still be faced by the courts and bodies of defence and consumer protection, and it is up to them to interpret it and ensure the protection of the rights of freedom, privacy and free development of the natural person.

Keywords: General Data Protection Law. International Data Transfer. Privacy. Freedom. Free development of the personality of the natural person.

LISTA DE QUADROS E FIGURAS

SUMÁRIO

INTRODUÇÃO

Este trabalho de conclusão de curso tem como tema a tutela dos direitos de liberdade, privacidade e livre desenvolvimento da pessoa natural em casos de transferência internacional de dados pessoais à luz da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de Agosto de 2018. Buscam-se, com o presente estudo, discutir as questões legais decorrentes das relações jurídicas transfronteiriças envolvendo usuários de internet e a gestão de seus dados pessoais em escala global.

A transferência internacional de dados é, na atualidade, um tema de vital importância, posto que, ao atravessar fronteiras, os dados são submetidos a distintas legislações de diferentes países, que podem nem mesmo dispor de leis que assegurem de forma adequada a tutela dos direitos dos titulares desses dados.

Hoje, os dados encontram-se em qualquer lugar, seja numa pesquisa no Google, numa compra no Ifood, num cadastro de perfil no Facebook ou na procura por um destino no Waze. Tudo que é feito virtualmente é convertido em dados que podem ser coletados em um país e transferidos a empresas de outros países, com fins comerciais e até mesmo políticos.

O volume de dados e as receitas geradas com o seu tratamento não deixam dúvida a respeito de sua importância social, econômica e política. Segundo a Wikibom, as grandes receitas do mercado de dados mundiais de software e serviços projetam-se para aumentar de US$ 42 bilhões (quarenta e dois bilhões de dólares) em 2018 para US$ 103 bilhões (cento e três bilhões de dólares) em 2027, alcançando a taxa de crescimento anual de 10,48% (COLUMBUS, 2019).

Diariamente, empresas multinacionais tratam dados em diversos países, inclusive no Brasil, devendo se sujeitar, portanto, a diferentes jurisdições que podem não gozar de uma legislação específica sobre proteção de dados pessoais. O Brasil, a título de exemplo, até a edição da Lei nº 13.709, de 14 de Agosto de 2018, tinha uma lacuna legislativa no que diz respeito especificamente à proteção e transferência internacional de dados pessoais. Entretanto, com a publicação da LGPD, 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, estará sujeita à imperatividade das leis brasileiras incidentes sobre quaisquer atos relacionados à transferência internacional de dados.

Trata-se de um momento legislativo ímpar para refletir a respeito dos distintos interesses em jogo. Se, por um lado, temos os interesses econômicos das empresas e políticos dos

governos no tratamento desses dados, de outro, temos os interesses sociais e os direitos dos indivíduos, usuários de internet e titulares relativamente à proteção de informações pessoais que circulam entre diferentes territórios, para além das fronteiras territoriais brasileiras.

Com efeito, o tema aqui abordado merece ser estudado, visto que os direitos à liberdade, privacidade e livre desenvolvimento da pessoa natural são direitos que emanam diretamente da dignidade da pessoa humana. Além disso, em uma sociedade globalizada como a nossa, cabe destacar o poder que a coleta e manipulação de dados confere a organizações e governos.

O uso intensivo de inteligência artificial e *machine learning*[1] para a aplicação em robôs inteligentes e ferramentas de *analytics*[2] pode transformar dados em vantagens econômicas e políticas, assim como instrumentos de coação e chantagem, na pior das hipóteses. Vivemos, pois, numa era em que o controle de dados é poder.

Destarte, tendo em vista a magnitude e importância dos direitos de liberdade, privacidade e livre desenvolvimento da pessoa natural, bem como as consequências desastrosas que a coleta, uso e comercialização de dados podem trazer, o estudo deste tema se faz deveras justificável.

Considerando o exposto até aqui, o presente trabalho possui o objetivo geral de investigar quais são as hipóteses de transferência internacional de dados pessoais conferidas pela LGPD e como objetivos específicos identificar qual a legislação e a competência judicial aplicáveis aos casos de responsabilidade civil decorrentes da violação dos direitos dos titulares de dados pessoais.

Em apertada síntese, pontua-se que a metodologia foi dividida em um método de abordagem e um método de procedimento. Nessa ordem de ideais, o método de abordagem (ou técnica de pensamento)[3] adotado foi o hipotético-dedutivo que parte das considerações gerais acerca dos institutos de direito tratados neste estudo, correlacionando-os, para chegar a uma

---

[1] O *machine learning,* aprendizado de máquina ou aprendizagem automática, no português, é uma tecnologia que possibilita que os computadores possam agir e decidir sozinhos, baseando-se em dados em vez de seguirem à risca uma programação para realizar uma determinada tarefa. O *machine learning* se vale do reconhecimento de padrões nos dados com que têm contato e são projetados para aprender e melhorar ao longo do tempo quando expostos a novos dados (MATOS, 2017).

[2] Ferramentas de *analytics* são softwares que realizam o trabalho de coletar, armazenar e interpretar grandes volumes de dados.

[3] Aqui, com o intuito de se fazer uma diferenciação entre os termos que serão utilizados, se fazem necessários alguns esclarecimentos. O primeiro deles é de que foram usados como sinônimos os termos "técnica de pensamento" e "método de abordagem", visto que os autores que tratam dessa seara científica acabam divergindo na adoção do termo. Isso posto, quando fazemos menção à técnica de pensamento (ou método de abordagem) estamos fazendo menção a uma abordagem mais ampla, dos fenômenos naturais e sociais, de modo que este pode ser discriminado em indutivo, dedutivo, hipotético-dedutivo e dialético.

conclusão particular, baseada em fatos supostos. Quanto ao método de procedimento[4], esta monografia foi inspirada no método experimental, que consiste no conjunto de processos utilizados para a verificação de uma hipótese (MARCONI; LAKATOS, 2003).

Por fim, salienta-se que, por se tratar de uma legislação nova que ainda não entrou em vigor, este estudo não tem a pretensão de esgotar o tema tratado. Entretanto, busca-se, com este trabalho de conclusão de curso, contribuir para a discussão acadêmica e compartilhar os conhecimentos adquiridos ao longo de seu desenvolvimento.

[4] Com este termo, busca-se referir às etapas mais concretas do estudo, que tem finalidade mais restrita, em termos de explanação geral dos institutos jurídicos e menos abstrata se comparada ao método de abordagem. Os métodos de procedimento mais conhecidos são o histórico, o comparativo, o monográfico, o estatístico, o tipológico, o funcionalista e o estruturalista.

1. LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018)

A LGPD regulamenta o uso, a proteção e a transferência de dados pessoais em território nacional, em âmbito público ou privado. O seu objetivo é garantir um efetivo controle por parte dos titulares sobre suas informações pessoais. A LGPD, entre outras disposições, exige consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados.

Isso posto, com o fim de adentrar ao tema deste estudo, neste capítulo serão abordados o histórico e o âmbito de aplicação da LGPD bem como o conceito e classificação dos dados pessoais e os requisitos para o seu tratamento.

1.1 Histórico

No ordenamento jurídico brasileiro, a proteção de dados pessoais foi inicialmente admitida como princípio relativo ao uso da Internet, expressamente consagrado pela Lei nº 12.965, o Marco Civil da Internet. Em vigor desde 23 de junho de 2014, o Marco Civil da Internet foi reconhecido como legislação pioneira no mundo e estabeleceu, em seu artigo 3º, inciso III, a elaboração de lei específica para a proteção de dados, o que só aconteceu em 10 de julho de 2018, data em que a LGPD foi aprovada.

O Marco Civil da Internet foi regulamentado no ano de 2015, por meio do Decreto Lei nº. 8771, o qual manteve e complementou as diretrizes de privacidade e liberdade de expressão, sendo possível depreender de seu conteúdo a preocupação com "uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes" (BRASIL, 2014).

A LGPD se originou do Projeto de Lei da Câmara de nº 53, de 2018, de iniciativa do Deputado Federal Milton Monti (PR/SP). Durante o período de trâmite, foram realizadas duas consultas públicas em que houve mais de 2.500 contribuições de atores nacionais e internacionais (AGÊNCIA SENADO, 2018). A lei foi sancionada em 14 de agosto de 2018, publicada no Diário Oficial da União em 15 de agosto de 2018 e republicada parcialmente no mesmo dia em edição extra. A LGPD, originalmente, previa uma *vacatio legis* de 18 meses, entretanto foi alterada para 24 meses com a edição da Medida Provisória Nº 869/2018.

O contexto no qual o projeto de lei foi aprovado explica a sua rápida tramitação nas casas legislativas. A matéria foi votada em regime de urgência no Plenário, depois de ter sido

aprovada em maio de 2018 na Câmara e em julho de 2018 na Comissão de Assuntos Econômicos (CAE) do Senado. Um dos motivos da urgência na tramitação foi o fato de o projeto de lei ter sido fruto da aglutinação de outras propostas[5] que há anos vinham tramitando paralelamente sobre o tema. O outro motivo diz respeito aos escândalos de privacidade envolvendo o Facebook, a Cambridge Analytics, o *Brexit* [6] e o Serviço Federal de Processamento de Dados (Serpro).

A Cambridge Analytics era uma empresa privada britânica de consultoria comercial e política que fora criada em 2013. Desde sua criação, ela tinha a finalidade principal de atuar em campanhas eleitorais, coletando, tratando e analisando dados de usuários de redes sociais, principalmente o Facebook. Por meio da análise dos dados pessoais e do comportamento dos usuários nas redes, a empresa identificava o público-alvo de suas ações e direcionava propagandas para essas pessoas, com o intuito de arrebanhar eleitores para determinados candidatos (RONCOLATO, 2018).

A Cambridge Analytics ficou famosa por sua atuação na campanha eleitoral do atual presidente dos Estados Unidos, Donald Trump, e também por suas ações no *Brexit*. Ela foi acusada de coletar, usar e vender indevidamente dados de milhões de estadunidenses bem como de viralizar[7] *fake news*[8] com o fim de formar opiniões e moldar o pensamento dos usuários da internet (RONCOLATO, 2018).

No Brasil, um caso análogo que também chamou a atenção, foi o suposto esquema de venda de dados pessoais de brasileiros pelo Serviço Federal de Processamento de Dados (Serpro). Segundo reportagem do site de notícias G1, dados como endereço, nome da mãe, sexo e data de nascimento de inscritos no Cadastro de Pessoa Física (CPF) e Jurídica (CNPJ) estavam sendo comercializados por até R$ 273 mil (MARQUES, 2018).

Desde então, quem temia ter as suas atividades vasculhadas no uso da internet ou quem simplesmente não queria se expor nas redes e nem compartilhar seus dados pessoais passou a se sentir inseguro e desconfiado. Esse quadro de insegurança e desconfiança ocorre, sobretudo,

---

[5] O PL 53/2018 tramitou em conjunto com o PLS 330/2013, que já tramitava em conjunto com os PLS 131/2014 e com o PLS 181/2014.

[6] *Brexit* foi o termo utilizado para definir o processo de saída do Reino Unido da União Europeia que se iniciou com um referendo realizado em 2016 e que, até o início de junho de 2019, ainda encontrava-se em trâmite. A palavra Brexit é fruto da união das palavras do idioma inglês "Britain" que significa Bretanha, de Grã-Bretanha, e "exit" cuja tradução para o português é "saída".

[7] Viralizar é um termo comumente utilizado nas redes sociais e significa espalhar, dissipar-se rapidamente.

[8] *Fake News* é um neologismo, ou um termo novo, derivado da língua inglesa, que é utilizado para se referir a notícias falsas, notícias criadas que não correspondem com a realidade e que são comumente compartilhadas na internet.

porque há quem afirme que qualquer pessoa que tiver interesse e capacidade pode descobrir o que qualquer pessoa faz em seu computador ou *smartphone* (ELOLA, 2018).

O fato é que "a disseminação de informações de modo instantâneo entre milhões de pessoas não traz apenas benefícios. Como qualquer nova tecnologia, a Internet também criou oportunidades inéditas para a prática de atos ilícitos" (LEONARDI, 2005, p. 7). Entre esses atos ilícitos, podemos ter a violação de nosso direito de privacidade, assim como o uso indevido de nossos dados pessoais por corporações nacionais e internacionais bem como por órgãos governamentais.

Nessa ordem de ideias, o que se observa historicamente é que as inúmeras mudanças por que passou a humanidade forçaram o sistema jurídico a encontrar novas estruturas normativas para lidar com os riscos e com as oportunidades que as inovações propiciaram. Com a era da Internet das Coisas[9] não é diferente. O desenvolvimento tecnológico já ensejou a criação de diplomas normativos como o General Data Protection Regulation (GDPR,) ou Regulamento Geral de Proteção de Dados e o Marco Civil da Internet e também a escrita de livros sobre o assunto.

Diante desse quadro, a segurança de dados e a privacidade passaram a ser pautas recorrentes, recaindo uma pressão na classe política no sentido de regulamentar essas questões, já que não havia no país uma legislação com objetivo específico de tutelar os dados dos usuários e definir responsabilidades relativas ao tratamento destes, em que pesem as legislações esparsas, como o Código de Defesa do Consumidor (CDC), o Código Civil (CC) e a Constituição, que já traziam dispositivos de tutela de dados.

Esse cenário levou, portanto, à criação da LGPD, sancionada em 14 de agosto de 2018. O seu texto sofreu vetos do ex-presidente em exercício à época, Michel Temer, que alegou "vício de iniciativa" para vetar a criação da Autoridade Nacional de Proteção de Dados (ANPD). A ANPD seria um órgão independente que teria como atribuição fiscalizar a aplicação da lei. Contudo, esse órgão foi recriado, posteriormente, por meio da Medida Provisória nº 869,

[9] The Internet of Things (IOT), ou a Internet das coisas, descreve os muitos usos e processos que resultam de dar um endereço de rede a uma coisa, objeto, máquina ou equipamento e ajustá-los a sensores. Esses conjuntos de sensores, coisas e redes tornaram-se uma parte cada vez mais importante das experiências da Internet. Quando equipamos as coisas ao nosso redor com sensores e as conectamos a redes, elas ganham novos recursos, como os dispositivos que fazem as luzes das casas se apagarem sozinhas quando o morador sai de casa, a geladeira que detecta a falta de alimentos e faz compras online de forma autônoma, o sistema de refrigeração de uma casa que se aciona minutos antes do morador chegar em casa, para que a temperatura esteja ideal, os assistentes pessoais virtuais como a Alexa, da Amazon, entre muitos outros dispositivos.

de 27 de dezembro de 2018[10]. A lei entrará em vigor 24 meses após a sua publicação no Diário Oficial da União, ou seja, a partir de agosto de 2020.

1.2 Âmbito de Aplicação

A Lei em questão tem incidência ampla e se aplica, conforme seus arts. 1º e 3º, a pessoas naturais ou jurídicas, de direito público ou privado, independentemente do país de sua sede ou de onde estejam localizados os dados, desde que:

a) o tratamento de dados ocorra em território nacional;
b) o tratamento de dados tenha por objetivo a oferta ou o fornecimento de bens ou serviços no território brasileiro ou o tratamento de dados de indivíduos localizados no Brasil; e
c) os dados pessoais tenham sido coletados de indivíduos localizados no Brasil no momento da coleta.

Assim, qualquer uma das três hipóteses acima passa a exigir o consentimento expresso do usuário para que seus dados possam passar por uma operação de tratamento de dados.

A Lei se aplica aos dados disponíveis em meios digitais, virtuais e também em meios físicos, como fichas de cadastro de hospitais. Ademais, quando houver tratamento de dados, a aplicação da LGPD independe do segmento desenvolvido, seja indústria, comércio, prestação de serviços ou negócios, por exemplo.

Noutro giro, a LGPD, conforme seu art. 4º **não será aplicada em três hipóteses**, quais sejam:

a) ao tratamento de dados provenientes de fora do território nacional e que não sejam objeto (i) de comunicação ou uso compartilhado de dados com agentes de tratamento brasileiro; ou (ii) de transferência internacional com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei;

[10] A MP alterou também o Marco Civil da Internet com o fim de autorizar que pessoas jurídicas de direito privado controladas pelo Poder Público, como a ANPD, possam tratar dados de bancos de dados sobre segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão penal.

b) se os dados pessoais forem tratados exclusivamente para fins jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado, investigação e repressão de infrações penais; e
c) se os dados pessoais forem tratados por pessoa natural para fins exclusivamente particulares e não econômicos.

Além disso, a lei estabelece, claramente, os sujeitos envolvidos no tratamento dos dados e quais as suas atribuições, responsabilidades e penalidades no âmbito civil, que podem chegar à multa de 50 milhões de reais por eventual violação de direitos dos titulares dos dados.

1.3 Dados pessoais e suas definições

A LGPD, conforme inciso I do art. 5º, define como dado pessoal qualquer "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Além disso, conforme o mesmo art. 5º, a lei define o que é dado pessoal sensível, dado pessoal anonimizado, banco de dados e anonimização de dados, conforme se observa a seguir, *in literis:*

> **II - dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> **III - dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> **IV - banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> (...)
> **XI - anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; (BRASIL, 2018, grifos atuais)

Vemos, portanto, que temos três tipos de dados pessoais, os dados pessoais *lato sensu*, os dados pessoais sensíveis e os dados anonimizados.

Assim, temos que os dados pessoais *lato sensu* são informações relativas a uma pessoa física, identificada ou identificável, bem como ao conjunto de informações distintas que podem levar à identificação de uma determinada pessoa física. Nessa ordem de ideias, dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, porém que ainda podem ser utilizados para reidentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do LGPD.

Temos como exemplo de dados pessoais: o nome, sobrenome, apelido e data de nascimento de uma pessoa, um endereço de *Internet Protocol* (IP), os dados colhidos por um hospital que permitam identificar uma pessoa de forma inequívoca, fotos, imagens relativas às pessoas recolhidas através dos sistemas de videovigilância e a gravação de chamadas telefônicas quando informadas à pessoa. Além disso, conforme § 2º do art. 12 da LGPD, poderão ser igualmente considerados como dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Por outro lado, **não são** dados pessoais, por exemplo, o Número de Identificação do Registro de Empresas (NIRE) e um endereço de correio eletrônico de uma pessoa jurídica, como o seguinte: atendimento@empresa.com.br.

Os dados pessoais sensíveis, como demonstrado acima, são ligados, na sua maioria, a questões mais subjetivas e comportamentais, e, por terem maior potencial lesivo, caso violados, o seu tratamento deve observar regras mais rígidas.

Noutro giro, quando temos um dado que não pode identificar, de forma direta ou indireta, um indivíduo, temos o que a lei chama de dado anonimizado. Nos termos do artigo 12 da LGPD, os dados anonimizados estão excluídos do escopo de aplicação da lei. Isso porque, considerando que esses dados não identificam de forma direta ou indireta o seu titular, não têm potencial de lhe causar danos e, por conseguinte, não requerem a proteção da lei.

A anonimização é um dos procedimentos previstos na LGPD para assegurar proteção aos dados pessoais, devendo ser utilizada sempre que possível, como no caso de estudos em saúde pública. Os dados pessoais que tenham passado pelo processo de anonimização, de modo que o seu titular não é mais identificável, deixam de ser considerados dados pessoais. Contudo, para que os dados sejam verdadeiramente anonimizados e saiam do escopo de proteção da Lei, a anonimização tem de ser irreversível.

Por fim, vale destacar que o titular de um dado pessoal, conforme disposição do inciso V do art. 5º da LGPD, é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (BRASIL, 2018).

1.4 Requisitos para o tratamento de dados pessoais

Tratamento, por sua, vez, é definido pela lei no inciso X do art. 5º como 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.

As atividades que envolvem o tratamento dos dados deverão observar os seguintes princípios: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, minimização da coleta, retenção mínima, responsabilização e prestação de contas.

Entre esses princípios, um mais relevante é o da finalidade, por meio do qual os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares, juntamente com o princípio da minimização da coleta, isto é, somente devem ser coletados os dados mínimos necessários para que se possa atingir a finalidade, e o da retenção mínima, o qual determina a imediata exclusão dos dados, após atingida a finalidade para a qual eles foram coletados

O tratamento de dados pessoais, conforme disposição do art. 7º da LGPD, somente poderá ocorrer nos seguintes casos:

a) com o consentimento do titular;
b) para o cumprimento de obrigação legal ou regulatória pelo controlador;
c) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas;
d) para a realização de estudos por órgão de pesquisa, sem a individualizaç;ao da pessoa;
e) para a execução de contrato ou de procedimentos preliminares relacionados a um contrato;
f) para pleitos em processo judicial, administrativo ou arbitral;
g) para a proteção da vida ou da incolumidade física do titular ou de terceiro;
h) para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
i) 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;
j) para a proteção do crédito, nos termos do Código de Defesa do Consumidor (CDC).

O capítulo II da LGPD, nas seções II e III, elenca os requisitos e dispõe como se dará o tratamento de dados pessoais considerados sensíveis, que poderá ocorrer quando o titular ou

seu responsável legal consentir, de forma específica e destacada, para finalidades específicas ou sem o consentimento do titular, nas hipóteses do inciso II do art. 11 da LGPD

2 DIREITOS DOS TITULARES DOS DADOS PESSOAIS

Os direitos dos usuários contam com capítulo próprio no texto legal, qual seja o Capítulo III, sendo imperioso destacar o direito de acesso, que lhes garante a possibilidade de obtenção, mediante requisição, junto aos controladores, de todos os dados pessoais que estão sendo tratados, e, como consequência disso, os direitos de retificação e atualização, haja vista a obrigação dos agentes de mantê-los sempre corretos e atualizados.

Entre os direitos previstos no art. 18, destacamos o direito de o titular obter do controlador dos dados a qualquer momento a confirmação de existência de tratamento, a possibilidade de acesso, correção, anonimização, bloqueio, eliminação e portabilidade dos dados. São garantidos, ainda, ao titular o direito de informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e a possibilidade de revogar o consentimento dado para o tratamento dos dados.

Ademais, o objetivo fundamental da LGPD, consoante o seu art. 1º, é a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade ou pessoa natural, que também são o escopo deste estudo e serão objeto de subseções próprias, como se observa a seguir.

É imperioso destacar desde já que, como não há, em nossa Constituição, nenhum direito absoluto, os direitos aqui abordados, até mesmo os sigilos pessoais constitucionalmente tutelados, podem sofrer alguma restrição ou ponderação com outros direitos.

2.1 Livre Desenvolvimento da personalidade da pessoa natural

A noção de personalidade pode ser considerada sob dois aspectos. O seu aspecto subjetivo está relacionado à capacidade de as pessoas serem titulares de direitos e obrigações. Já no aspecto objetivo, a personalidade é vista como um conjunto de características e atributos da pessoa humana, objeto de proteção do ordenamento jurídico. Este último aspecto é que está intimamente ligado aos direitos da personalidade (SCHREIBER, 2013).

Os direitos da personalidade são aqueles inerentes ao homem, que são tidos como preexistentes ao seu reconhecimento por parte do Estado, essenciais à condição humana e fruto de uma contínua marcha de conquistas históricas.

No último século, o tema foi tratado sob diferentes denominações. A Assembleia Constituinte Francesa referia-se, na declaração de 1789, aos Direitos do Homem e do Cidadão.

A Declaração das Nações Unidas, de 1948, a seu turno, utiliza a expressão Direitos Humanos. A Constituição brasileira de 1988 reservou o seu Título II aos Direitos e Garantias Fundamentais.

Já o Código Civil, em seu segundo capítulo, em onze artigos (arts. 11 a 21), tutelou os direitos da personalidade, regulando o direito ao próprio corpo, o direito ao nome, o direito à honra, o direito à imagem e o direito à privacidade (SCHREIBER, 2013). A maior parte desses direitos tem previsão expressa no art. 5º da Constituição e, mesmo os não expressamente previstos, são consectários da dignidade humana, tutelada no art. 1º, inciso III da CF. Os direitos da personalidade, portanto, são direitos fundamentais.

Em que pese a variedade de termos, todos eles destinam-se a contemplar atributos da personalidade humana merecedores de proteção jurídica. A diferença está no plano de manifestação da personalidade humana, como se observa no trecho a seguir:

> Assim, a expressão direitos humanos é mais utilizada no plano internacional, independentemente, portanto, do modo como cada Estado nacional regula a matéria. Direitos fundamentais, por sua vez, é o termo normalmente empregado para designar "direitos positivados numa constituição de um determinado Estado". É, por isso mesmo, a terminologia que tem sido preferida para tratar da proteção da pessoa humana no campo do direito público, em face da atuação do poder estatal. Já a expressão direitos da personalidade é empregada na alusão aos atributos humanos que exigem especial proteção no campo das relações privadas, ou seja, na interação entre particulares, sem embargo de encontrarem também fundamento constitucional e proteção nos planos nacional e internacional (SCHREIBER, 2013, p. 13).

O valor tutelado é único, qual seja a dignidade da pessoa humana, independentemente do plano em que se encontram os direitos da personalidade. Hoje, portanto, a personalidade diz respeito a um valor que permeia todo o sistema jurídico com o fim de assegurar a proteção da pessoa ontologicamente considerada, reconhecendo, para tanto, os chamados direitos da personalidade.

Nessa ordem de ideias, o livre desenvolvimento da personalidade da pessoa natural diz respeito à liberdade na dinâmica do desenvolvimento das características e atributos da pessoa humana, que se concretiza por meio da possibilidade de a pessoa construir a sua própria biografia valendo-se de suas escolhas existenciais. A pessoa, como dona de sua vida, escolhe diariamente os rumos que tomará. Ao Estado a aos demais particulares cabe o respeito e a promoção dos meios para a realização dessas escolhas existenciais. Conforme destaca Moreira (2015, p. 10), "a liberdade de construção da personalidade permite a eleição dos planos de vida valorados pela própria pessoa como sendo uma vida boa e feliz".

Apesar de a Declaração Universal de Direitos Humanos reconhecer o direito ao livre desenvolvimento da personalidade da pessoa natural, não existe previsão expressa de sua tutela no sistema jurídico brasileiro. Entretanto, conforme mencionado acima, os direitos da personalidade são direitos fundamentais. Isso faz com que este direito esteja positivado "implicitamente por via dos princípios fundamentais constitucionais, nomeadamente o princípio da dignidade da pessoa humana, com especial aplicação do art. 5º, § 2º da Constituição Federal como cláusula de abertura para direitos fundamentais atípicos" (MOREIRA, 2015, p. 11).

Ademais, é importante ressaltar que, apesar de terem significados distintos, pessoa, personalidade e dignidade são construções inter-relacionadas, que se complementam e que contribuirão para justificar e reconhecer a existência de um direito ao livre desenvolvimento da personalidade no ordenamento jurídico brasileiro (MOREIRA, 2015).

Em suma, o direito ao livre desenvolvimento da personalidade "visa a tutela das decisões pessoais na formação dinâmica e em constante evolução da personalidade de cada pessoa humana, com ênfase nas suas dimensões de liberdade e de proteção dos direitos da personalidade" (MOREIRA, 2015, p. 11).

2.2 Liberdade

A liberdade, segundo o conceito do Dicionário Brasileiro da Língua Portuguesa Michaelis (2019, não paginado), é o "poder de agir livremente, dentro de uma sociedade organizada, de acordo com os limites impostos pela lei; é a faculdade que tem o indivíduo de decidir pelo que mais lhe convém". Sob o ponto de vista jurídico, a liberdade tem dois sentidos diversos, a liberdade positiva e a liberdade negativa:

> A **liberdade positiva** – também denominada de liberdade política ou liberdade dos antigos ou liberdade de querer – pode ser definida como a 'situação na qual um sujeito tem a possibilidade de orientar seu próprio querer no sentido de uma finalidade sem ser determinado pelo querer dos outros.
> A **liberdade negativa** – conhecida também como liberdade civil ou liberdade dos modernos ou liberdade de agir – é a 'situação na qual um sujeito tem a possibilidade de agir sem ser impedido, ou de não agir sem ser obrigado por outros'. Consiste, portanto, na ausência de impedimentos ou de constrangimentos. (NOVELINO, 2014, p. 475)

A Constituição de 1988 consagrou, ao lado do direito geral de liberdade, vários direitos de liberdade específicos, como o direito de liberdade de ação, o direito de liberdade de manifestação do pensamento, o direito de liberdade de consciência, de crença e de culto, o

direito de liberdade de comunicação pessoal, o direito de liberdade de exercício profissional, o direito de liberdade de informação, o direito de liberdade de locomoção, o direito de liberdade de reunião e o direito de liberdade de associação.

O direito de liberdade de ação nada mais é do que a expressão da autonomia da vontade. Nesse sentido, a liberdade de agir é conferida pela Constituição da República, quando esta, no inciso II do seu art. 5º, determina que ninguém será obrigado a fazer ou a deixar de fazer algo senão em virtude de lei. Com esse dispositivo constitucional, o indivíduo está protegido do arbítrio estatal, no sentido de que só estará obrigado a fazer aquilo que for determinado por lei que foi elaborada respeitando o devido processo legislativo constitucional e desde que seu conteúdo não afronte direitos fundamentais.

O direito de liberdade de manifestação do pensamento está previsto nos incisos IV, V e IX do art. 5º da CF, que dispõem o seguinte:

> CF, art. 5.°, IV – é livre a manifestação do pensamento, sendo vedado o anonimato; V– é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; [...] IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; (BRASIL, 1988)

O texto constitucional garante, portanto, a proteção da exteriorização da opinião e veda a censura prévia. A tutela à manifestação de pensamento se dá nas suas mais variadas formas, sejam em mensagens faladas, escritas, gestos, imagens, expressões e até mesmo no silêncio.

O direito de liberdade de consciência, de crença e de culto, previsto no inciso VI, do art. 5º da CF, garante a inviolabilidade da "liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias" (BRASIL, 1988). A diferença entre liberdade de consciência, crença e culto é explicada didaticamente pelo constitucionalista Marcelo Novelino no trecho a seguir:

> A **liberdade de consciência** consiste na adesão a certos valores morais e espirituais, independentes de qualquer aspecto religioso, podendo se determinar no sentido de crer em conceitos sobrenaturais propostos por alguma religião ou revelação (teísmo), de acreditar na existência de um Deus, mas rejeitar qualquer espécie de revelação divina (deísmo) ou, ainda, de não ter crença em Deus algum (ateísmo).
> Como pode ser observado, o âmbito de proteção da liberdade de consciência abrange a **liberdade de crença**. Esta, por sua vez, é garantida inclusive em entidades civis e militares de internação coletiva, nas quais a Constituição assegura a prestação de assistência religiosa (CF, art. 5.°, VII). No âmbito das Forças Armadas, o serviço de assistência religiosa está disciplinado na Lei 6.923/1981. Nas entidades hospitalares públicas e privadas, bem como nos estabelecimentos prisionais civis e militares, a prestação de assistência religiosa está regulamentada pela Lei 9.982/2000.
> A **liberdade de culto** é uma das formas de expressão da liberdade de crença, podendo ser exercida em locais abertos ao público, desde que observados certos limites, ou em

> templos, aos quais foi assegurada a imunidade fiscal (CF, art. 150, VI, b). (NOVELINO, 2014, p. 478)

O direito de liberdade de comunicação pessoal prevê a inviolabilidade do sigilo da correspondência e das comunicações telegráficas e telefônicas e também de dados, conforme inciso XII do art. 5º da Constituição. É importante ressaltar que a comunicação telefônica consiste na "transmissão, emissão, receptação e decodificação de sinais linguísticos, caracteres escritos, imagens, sons, símbolos de qualquer natureza veiculados pelo telefone estático ou móvel (celular)" (BULOS, 2010, p. 176). No entanto, há autorização expressa da própria Constituição para a interceptação das comunicações telefônicas quando decorrente de ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (CF, art. 5.°, XII).

A forma e as hipóteses nas quais as interceptações telefônicas poderão ser determinadas judicialmente estão regulamentadas na Lei 9.296/1996, cujos dispositivos se aplicam também à interceptação do fluxo de comunicações em sistemas de informática e telemática (Lei 9.296/1996, art. 1.°, parágrafo único), por exemplo, mensagens enviadas por correio eletrônico, por SMS e WhatsApp.

A liberdade de comunicação pode ser vista sob o ponto de vista positivo (que diz respeito à liberdade de transmitir e receber comunicações) e negativo (que assegura o direito de não transmitir e não receber comunicações). É a liberdade de comunicação que assegura, por exemplo, que a abertura de correspondência por pessoa diversa do destinatário viola o sigilo de correspondência. O sigilo, a seu turno, tem o fim de proteger o conteúdo das comunicações privadas contra qualquer ingerência indevida em qualquer momento que seja, durante a transmissão da mensagem ou depois.

O direito de liberdade do exercício profissional de qualquer trabalho, ofício ou profissão também é uma das garantias constitucionais, entretanto condicionada ao atendimento das qualificações profissionais que eventualmente uma lei federal estabelecer, conforme inciso XIII do art. 5º e inciso XVI do art. 22, ambos da CF.

A liberdade de informação, a seu turno, abrange os direitos de informar, de se informar e de ser informado e tem previsão expressa nos incisos XIV e XXXIII do art. 5º e art. 220, ambos da CF. Vejamos, *in literis:*

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
> [...]
> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
> § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.
> § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística. (BRASIL, 1988)

A liberdade de locomoção, prevista na CF, art. 5.°, XV, está relacionada à liberdade física do homem e engloba, além do direito de ir e vir, o de permanecer, sendo cabível *habeas corpus* em casos de violação efetiva do direito, bem como em casos de ameaça à liberdade do indivíduo.

O direito de liberdade de reunião, nos termos do art. 5º, XVI da CF, significa que todos podem reunir-se pacificamente, sem armas, em locais abertos ao público, independentemente de autorização, desde que não frustrem outra reunião anteriormente convocada para o mesmo local, sendo apenas exigido prévio aviso à autoridade competente. O direito de reunião, segundo Masson (2016, p. 251) "possui significante abrangência, já que compreende não apenas ao direito de organizar e convocar a reunião, mas também o de participar ativamente, debatendo e apresentando ideias, vez que os integrantes não precisam se limitar ao direito de ouvir".

O direito de liberdade de associação está previsto constitucionalmente no art. 5º, incisos XVII a XXI, e tem o fim de assegurar a plena liberdade de associação, a impossibilidade de alguém ser obrigado a se associar, ou a se manter associado, a desnecessidade de autorização do estado para se criar uma associação e a proibição de interferências estatais no funcionamento dessas associações.

É importante ressaltar que, para que haja uma associação, é necessário um agrupamento de pessoas com objetivos comuns e com estabilidade, não sendo relevante o modo como se dará o contato entre os seus integrantes, se pelas mídias sociais, reuniões presenciais ou telefonemas.

2.3 Privacidade

O direito à privacidade é um dos bens jurídicos mais importantes do ser humano e "confere ao indivíduo a possibilidade de conduzir a sua própria vida da maneira que julgar mais conveniente, sem intromissão da curiosidade alheia" (NOVELINO, 2014, p. 497).

O direito à privacidade é um Direito Humano e também um Direito Fundamental. Esse bem jurídico conta com a proteção jurídica da Declaração Universal dos Direitos Humanos em seu art. 12 a nível internacional e da Constituição Federal a nível nacional, sem contar a legislação infraconstitucional e outros tratados internacionais.

A Constituição no inciso X, art. 5º, protege a privacidade, garantindo a inviolabilidade da "intimidade, da vida privada, da honra e da imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

Há, segundo Gilmar Mendes, quatro meios básicos de se violar a privacidade, quais sejam:

> (i) intromissão na reclusão ou na solidão do indivíduo; (ii) exposição pública de fatos privados; (iii) exposição do indivíduo a uma falsa percepção do público (*false ligth*), que ocorre quando a pessoa é retratada de modo inexato ou censurável; (iv) apropriação do nome e da imagem da pessoa, sobretudo para fins comerciais (MENDES; BRANCO e COELHO, 2010, p. 471).

Tendo por referencial a teoria das esferas, adotada pela doutrina e jurisprudência alemãs, pode-se estabelecer uma variação do grau de proteção à privacidade de acordo com a área da personalidade afetada. As esferas delineadas pela teoria estão relacionadas às experiências definidoras da identidade dos indivíduos e são divididas em três espécies, quais sejam:

> A **esfera da publicidade** compreende os atos praticados em local público com o desejo de torna-los públicos. Não basta apenas que o ato seja praticado em local não reservado (elemento espacial), exige-se um elemento volitivo interno: a renúncia. Esta pode ser expressa (como a que ocorre nos programas televisivos de reality show) ou tácita (pessoas públicas em eventos públicos, como shows, comícios, noite de autógrafos, entrega de prêmios e solenidades em geral), mas somente será válida se ocorrer de forma casuística e temporária ("não exercício"). A esfera da publicidade compreende, ainda, fatos pertencentes ao domínio público ou informações passíveis de serem obtidas licitamente.
> A **esfera privada** abrange as relações do indivíduo com o meio social nas quais não há interesse público na divulgação. Abrange, por exemplo, informações fiscais ou bancárias.
> A **esfera íntima** se refere ao modo de ser de cada pessoa, ao mundo intrapsíquico aliado aos sentimentos identitários próprios (autoestima, autoconfiança) e à sexualidade. Compreende informações confidenciais e segredos pessoais, como, por exemplo, as anotações constantes de um diário. (NOVELINO, 2014, p. 468-468)

O direito à privacidade compreende o direito à intimidade, o direito à vida privada, o direito à honra, o direito à imagem, os sigilos pessoais (do domicílio, de correspondência, de dados em geral, de dados bancários, fiscais, telefônicos) e o sigilo das comunicações (telegráficas e telefônicas).

O direito à intimidade é o núcleo mais restrito da privacidade e, conforme Masson (2016, p. 2018), "compreende as relações e opções mais íntimas e pessoais do indivíduo, compondo uma gama de escolhas que se pode manter ocultas de todas as outras pessoas, até das mais próximas". Um exemplo de violação ao direito à intimidade é o acesso, sem consentimento, às comunicações telefônicas de um indivíduo.

O direito à vida privada, mais abrangente do que o direito à intimidade, "abarca as relações pessoais, familiares, negociais ou afetivas, do indivíduo, incluindo seus momentos de lazer, seus hábitos e seus dados pessoais, como os bancários e os fiscais" (MASSON, 2016, p. 219).

O direito à honra pode ser visto sob o ponto de vista objetivo ou subjetivo e está ligado à ideia de reputação, bom nome e boa fama que um indivíduo tem, bem como ao sentimento próprio de dignidade. Nesse sentido, o direito à honra objetiva "consiste na reputação do indivíduo perante o meio social em que vive" (NOVELINO, 2014, p. 469). Já a honra subjetiva está ligada à estimação que o indivíduo tem de si mesmo. Em caso de violação à honra, o indivíduo tem assegurada a indenização por danos morais.

O direito à imagem é a tutela conferida ao indivíduo no sentido de impedir a captação e difusão de sua imagem física, sem o seu consentimento. A imagem física, segundo Masson (2016, p. 219), "inclui qualquer representação gráfica do aspecto visual da pessoa ou dos traços característicos da sua fisionomia".

Vemos, portanto, que não é preciso que haja ofensa à estimação pessoal ou à reputação do indivíduo, basta que haja coleta e difusão da imagem física do titular sem o seu consentimento (mesmo que seja para enaltecer a pessoa), ressalvado o direito de informar e as circunstâncias fáticas e jurídicas que excepcionam a necessidade de o indivíduo consentir. Este é o entendimento do STF:

> Para a reparação do dano moral não se exige a ocorrência de ofensa à reputação do indivíduo. O que acontece é que, de regra, a publicação da fotografia de alguém, com intuito comercial ou não, causa desconforto, aborrecimento ou constrangimento, não importando o tamanho desse desconforto ou desse constrangimento. Desde que ele exista, há o dano moral, que deve ser reparado, manda a Constituição, art. 5º, X (RE 215.984, relatado pelo Min. Carlos Velloso, 21 Turma, STF).

Conforme assinalado pelo Min. Raul Araújo, em decisão proferida pelo STJ, para se verificar a gravidade do dano sofrido pela pessoa cuja imagem é utilizada sem autorização prévia, devem ser analisados alguns aspectos, quais sejam:

> (i) o grau de consciência do retratado em relação à possibilidade de captação da sua imagem no contexto da imagem do qual foi extraída; (ii) o grau de identificação do retratado na imagem veiculada; (iii) a amplitude da exposição do retratado; e (iv) a natureza e o grau de repercussão do meio pelo qual se dá a divulgação.
> De outra parte, o direito de informar deve ser garantido, observando os seguintes parâmetros: (i) o grau de utilidade para o público do fato informado por meio da imagem; (ii) o grau de atualidade da imagem; (iii) o grau de necessidade da veiculação da imagem para informar o fato; e (iv) o grau de preservação do contexto originário do qual a imagem foi colhida (STJ – REsp 794.586, rel. Min. Raul Araújo 15.03.2012).

Além disso, são exceções ao direito de privacidade os fatos que envolvem atividades criminosas, bem como fatos noticiáveis, como catástrofes de grandes proporções.

O sigilo pessoal compreende o sigilo do domicílio, de correspondência, de dados em geral, de dados bancários, fiscais e telefônicos. O sigilo do domicílio é previsto no inciso XI do art. 5º da Constituição da seguinte forma: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial" (BRASIL, 1988). A noção de casa, sob o ponto de vista constitucional, indica "qualquer local delimitado que alguma pessoa ocupe com exclusividade, a qualquer título, inclusive de forma profissional" (MASSON, 2016, p. 220).

O sigilo de correspondência tem previsão expressa no inciso XII do art. 5º da Constituição, que dispõe o seguinte: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (BRASIL, 1988). Considerando que nenhum direito é absoluto, vale ressaltar que o sigilo de correspondência pode ser relativizado quando estivermos diante de questões de segurança pública ou em razão da utilização da inviolabilidade como escudo para a prática de atividades ilícitas.

O sigilo de dados em geral é relacionado àquelas informações que podem revelar aspectos da privacidade de determinado indivíduo e também tem previsão expressa no inciso XII do art. 5º da Constituição. Além da previsão constitucional, os dados aqui mencionados também contam com a proteção da própria LGPD. Esses dados são referentes às informações

telefônicas, bancárias e fiscais da pessoa, bem como à sua orientação sexual, crença religiosa e ao valor de sua remuneração.

O sigilo de dados bancários, previsto no inciso XII do art. 5º da Constituição, diz respeito às informações relativas às movimentações e posições financeiras de determinado indivíduo que se encontram sob a guarda de uma instituição financeira.

Os dados fiscais, segundo o entendimento de Masson (2016, p. 223), "podem ser definidos como as informações obtidas pelos agentes da Fazenda Pública, no exercício do ofício, referentes à posição econômica, financeira ou dos negócios e atividades do contribuinte e terceiros".

Os dados telefônicos são aqueles relativos aos registros dos números de telefones para os quais a pessoa fez ou recebeu ligações, incluídas as informações que dizem respeito à data, horário e duração da chamada.

O sigilo das comunicações compreende as comunicações telegráficas e telefônicas. Diferentemente do sigilo de dados, o sigilo das comunicações visa à tutela do seu conteúdo, do que foi veiculado por meio do telegrama ou telefone.

A Constituição no inciso XII do art. 5º também estabeleceu a inviolabilidade das comunicações telegráficas, que são as realizadas por meio de telegramas. Apesar dessa modalidade não ser muito utilizada atualmente, a sua tutela ainda continua.

As comunicações telefônicas, a seu turno, são aquelas realizadas por meio de telefones. A interceptação telefônica é a "a captação e gravação de conversa telefônica, no mesmo momento em que ela se realiza, por terceira pessoa sem o conhecimento de qualquer dos interlocutores" (MORAES, 2010, p. 59).

3 RESPONSABILIDADE CIVIL E SANÇÕES

A responsabilidade civil, se entendida numa visão ampla de obrigação de reparar um dano antijuridicamente causado a um terceiro, pode ser compreendida em duas modalidades. A primeira delas é a decorrente de danos resultantes do inadimplemento, má execução ou atraso no cumprimento de obrigações contratuais, denominada de responsabilidade contratual. A segunda, também chamada de responsabilidade civil extracontratual, diz respeito à obrigação de reparação de danos resultantes da violação de outros direitos alheios, como os direitos da personalidade.

A responsabilidade civil extracontratual é, portanto, diretamente ligada à violação de um direito. Assim, aquele que viola um direito e ocasiona dano a outrem será responsável pela reparação do dano causado. No Código Civil, a responsabilidade civil é fundada em dois conceitos, o de ato ilícito (art. 186) e o de abuso de direito (art. 187) da seguinte forma:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes. (BRASIL, 2002)

O ato ilícito, portanto, é aquele praticado em desacordo com a ordem jurídica, que ocasiona a violação de direitos e causa prejuízos a outrem. O ato ilícito pode ser penal, administrativo ou civil bem como pode acarretar dupla ou tripla responsabilidade, por exemplo, um crime ambiental que ofende os particulares (ilícito civil), a sociedade (ilícito penal) e é passível de sanções administrativas. A consequência do ato ilícito civil é a obrigação geral de reparar o dano, disposta no caput do art. 927 do Código Civil de 2002.

Além disso, existem situações em que se responde por terceiros, devendo existir uma conexão entre o responsável e o executor do ato. Há também a hipótese de dano causado por coisa da qual se é proprietário.

Por outro lado, nos moldes do art. 187 do CC, a noção de ato ilícito foi ampliada, para considerar como ilícito aquele ato que, originalmente é lícito, mas foi exercido fora dos limites impostos pelo seu fim econômico ou social, pela boa-fé objetiva ou pelos bons costumes.

Desse modo, para que exista a responsabilidade civil é necessária a conjugação de três pressupostos, quais sejam a conduta, o nexo de causalidade e o dano. A conduta pode ser ação

ou inação; comissiva ou omissiva[11]; própria[12] ou de terceiro[13]; lícita ou ilícita; derivada de fato, coisa, produto ou animal. O nexo de causalidade liga a conduta do agente ao dano sofrido pela vítima. Para que surja o dever se indenizar é preciso que o dano verificado seja consequência da ação ou omissão do agente. O dano é a lesão a um bem jurídico.

A LGPD, a seu turno, define a responsabilidade dos agentes de tratamento de dados, que são os controladores[14] e os operadores[15], pelos danos causados em razão do exercício da atividade de tratamento, de forma semelhante à sistemática do Código de Defesa do Consumidor (CDC), na seção III do Capítulo VI. A Lei, conforme art. 43, exime de responsabilidade os agentes quando provarem que: não realizaram o tratamento de dados em questão; que não houve violação à legislação; ou que houve culpa exclusiva do titular dos dados ou de terceiro pela ocorrência dos danos.

Conforme art. 42 da LGPD, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, será obrigado a repará-lo. A LGPD traz, ainda, previsão expressa de responsabilidade solidária dos operadores e controladores. Nesse sentido, conforme disposição do inciso I do §1º do art. 42, o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do controlador. Já os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, conforme inciso II do §1º do art. 42 da LGPD, respondem solidariamente.

O direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso, é assegurado àquele que reparar o dano ao titular dos dados consoante §4º do art. 42 da LGPD.

Nos termos do art. 44 da LGPD, será considerado irregular o tratamento de dados pessoais quando for inobservada a legislação ou quando não for fornecida ao titular a segurança que ele poderia esperar, levando-se em conta as seguintes circunstâncias: o modo pelo qual o tratamento é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

---

[11] Quando há um dever legal de agir e a pessoa não age.
[12] A pessoa responde por seus atos.
[13] A pessoa responde por atos de terceiros.
[14] Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
[15] Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

As seguintes sanções administrativas, entre outras, são aplicáveis aos agentes de tratamento de dados por violação às normas previstas na Lei, conforme art. 52: (i) advertência; (ii) multa de até 2% do faturamento do grupo econômico no Brasil no último exercício, limitada a R$ 50 milhões por infração; (iii) multa diária; (iv) publicização da infração após devidamente apurada e confirmada a sua ocorrência; (v) bloqueio de dados pessoais; (vi) eliminação dos dados pessoais.

4 TRANSFERÊNCIA INTERNACIONAL DE DADOS

Antes da edição da LGPD, o Brasil não era considerado uma referência para os setores produtivos que demandavam a transferência internacional de dados. Vale destacar que o Brasil foi um dos últimos países signatários[16] da Convenção das Nações Unidas sobre os Contratos de Compra e Venda Internacional de Mercadorias (CISG)[17].

O Marco Civil da Internet foi o primeiro diploma legislativo que começou a delinear os direitos dos usuários no que diz respeito à transferência internacional de dados. Antes da criação da LGPD, o Marco Civil da Internet se apresentava como a única lei infraconstitucional que estabelecia dispositivos que tratavam especificamente de dados pessoais nas redes. Vejamos o que dispõe a Lei N° 12.965/14, em seu art. 11:

> 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.
> § 1o O disposto no caput **aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.**
> § 2o **O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.**
> § 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4o Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo. (BRASIL, 2014)

Conforme dispõe o Marco Civil, é aplicável a legislação brasileira sobre qualquer ato relacionado à transferência internacional de dados, nas situações em que pelo menos um deles se materialize ou produza efeitos no território nacional. Além disso, mesmo que o tratamento de dados seja realizado por pessoa jurídica sediada em país estrangeiro, desde que esta oferte

[16] O Brasil aderiu à CISG em 2013, com vigência a partir de 1º de abril de 2014.
[17] A Convenção de Viena das Nações Unidas sobre Contratos de Compra e Venda Internacional de Mercadorias (CISG, na sigla em Inglês) é uma lei uniforme que rege as transações comerciais internacionais em matéria de compra e venda de mercadorias. Ela foi aprovada, no dia 10 de abril de 1980, por uma conferência diplomática que contou com a participação de 62 países. A CISG entrou em vigor no dia 1º de janeiro de 1988, para os seguintes estados: Argentina, China, Egito, Estados Unidos, França, Hungria, Itália, Iugoslávia, Lesoto, Síria e Zâmbia. (CISG, 2019)

serviço aos brasileiros ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil, é aplicável a legislação brasileira.

Entretanto, apesar de o Brasil ter o Marco Civil da internet como legislação pioneira no mundo no que diz respeito à governança da Internet, o país não dispunha de uma legislação que tratasse especificamente e pormenorizadamente de como se daria a transferência internacional de dados, problema que foi solucionado pela LGPD, em seu Capítulo V, como se observa a seguir.

4.1 Hipóteses e requisitos para a Transferência Internacional de dados

Os requisitos e as hipóteses para a transferência internacional de dados estão previstos no Capítulo V, art. 33 e seguintes da LGPD. Conforme art. 33 da LGPD, a transferência internacional de dados só é permitida em nove hipóteses que são tratadas nos nove incisos do referido artigo. Desse modo, entende-se que o rol do art. 33 é taxativo.

A **primeira hipótese**, prevista no inciso I do art. 33, é aquela que prevê a possibilidade de transferência de dados para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD. O critério aqui, portanto, é geográfico e leva em consideração os potenciais riscos a que os dados estão submetidos quando entrarem no país de destino.

A adequação do grau de proteção leva em conta a legislação doméstica de cada país bem como os tratados e convenções internacionais de que o Estado destinatário é signatário. Ademais, pela letra da lei, a hipótese prevista no inciso I não considera as providências que podem ser tomadas pela iniciativa privada para a proteção dos dados transferidos em nível internacional.

A **segunda hipótese** de transferência, prevista no inciso II do art. 33, ocorre quando o controlador dos dados oferece e comprova que garante o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de: (i) cláusulas contratuais específicas para determinada transferência; (ii) cláusulas padrão contratuais[18]; (iii) normas corporativas globais[19]; e (iv) selos, certificados e códigos de conduta regularmente emitidos.

[18] "São cláusulas típicas que estão contidas no acordo contratual e que se destinam a tutelar aspectos comuns aos contratos em geral" (DELECRODE, 2017).
[19] São normas que devem ser observadas por um mesmo grupo de empresas em países diferentes para transferirem dados pessoais de um local para outro.

O inciso II do art. 33 traz a **terceira hipótese**, que se dá nos casos de necessidade de cooperação jurídica internacional[20] entre órgãos públicos de inteligência, de investigação e de persecução, conforme os instrumentos de direito internacional. Essa hipótese rege, portanto, a transferência internacional de dados para fins de investigações conduzidas em outros Estados.

Essa hipótese é de fundamental importância, tendo em vista o crescimento do número de ocorrências de crimes cometidos na internet bem como a descentralização da rede e da hospedagem de serviços digitais em outros países. Com efeito, as características da internet (descentralização e distribuição por diversos Estados) impõem às autoridades grandes desafios quando se trata de investigar, julgar e punir uma conduta criminosa, sendo extremamente necessária a cooperação internacional. Isso porque a prova da materialidade e autoria de um crime pode encontrar-se em um computador que esteja a milhares de quilômetros de onde os efeitos do crime foram sentidos, ou de onde a conduta deve ser julgada.

A **quarta hipótese**, disposta no inciso III do art. 33, é a que prevê a transferência de dados quando estes forem necessários para a proteção da vida ou da incolumidade física do titular ou de terceiro, ainda que o nível de proteção de dados do local de destino seja inferior ao brasileiro. O dispositivo aqui mencionado visa à tutela da pessoa humana e deve ser visto como necessário à proteção da vida ou integridade física de brasileiros que se encontram em situação de perigo no exterior. Como exemplo de sua aplicação, podemos citar a transferência de registros médicos para um país onde o titular desses registros tenha sofrido um acidente e precisa do histórico médico para que seja feito o prognóstico adequado.

A **quinta hipótese** de transferência internacional é a que se dá com a autorização da autoridade nacional. Conforme já foi abordado anteriormente neste estudo, às vésperas do final de 2018, em 28 de dezembro, a Presidência da República editou a Medida Provisória (MP) nº 869/2018, que estabeleceu a criação da ANPD e alterou alguns outros pontos da LGPD.

A criação da ANPD tem o fim de adequar a legislação brasileira, no que diz respeito à proteção de dados, aos padrões internacionais, verificados, especialmente, no quadro da Organização para Cooperação e Desenvolvimento Econômico (OCDE) e em países da União Europeia (UE), onde as "autoridades" em questão foram criadas e já até entraram em operação. A ANPD será um órgão da Administração Pública Federal, vinculado à Presidência da República, terá autonomia técnica e a função de zelar, implementar e fiscalizar o cumprimento da LGPD.

[20] A cooperação jurídica internacional é uma maneira formal de solicitar a outro estado alguma medida judicial, investigativa ou administrativa necessária para um caso concreto em andamento.

A **sexta hipótese** ocorre quando a transferência resultar em compromisso assumido em acordo de cooperação internacional. Nesse sentido, vale destacar que, no cenário internacional, dois importantes tratados impõem ao país o dever de transferir dados a outros Estados, quais sejam a Convenção das Nações Unidas contra o Crime Organizado Transnacional e a Convenção das Nações Unidas Contra a Corrupção.

A Convenção das Nações Unidas contra o Crime Organizado Transnacional, também conhecida como Convenção de Palermo, foi promulgada por meio do Decreto nº 5.015, de 12 de março de 2004. Ela foi aprovada pela Assembleia-Geral da ONU em 15 de novembro de 2000, data em que foi colocada à disposição dos Estados-membros para assinatura, e entrou em vigor no dia 29 de setembro de 2003.

Em seu art. 18, a Convenção de Palermo regula a assistência judiciária recíproca, mencionando expressamente que essa assistência pode ser solicitada para fornecer informações, elementos de prova e originais ou cópias autenticadas de documentos. Vejamos, *in literis:*

> **Artigo 18**
> Assistência judiciária recíproca
>
> **1.** Os Estados Partes prestarão reciprocamente toda a assistência judiciária possível nas investigações, nos processos e em outros atos judiciais relativos às infrações previstas pela presente Convenção, nos termos do Artigo 3, e prestarão reciprocamente uma assistência similar quando o Estado Parte requerente tiver motivos razoáveis para suspeitar de que a infração a que se referem as alíneas a) ou b) do parágrafo 1 do Artigo 3 é de caráter transnacional, inclusive quando as vítimas, as testemunhas, o produto, os instrumentos ou os elementos de prova destas infrações se encontrem no Estado Parte requerido e nelas esteja implicado um grupo criminoso organizado.
>
> **2.** Será prestada toda a cooperação judiciária possível, tanto quanto o permitam as leis, tratados, acordos e protocolos pertinentes do Estado Parte requerido, no âmbito de investigações, processos e outros atos judiciais relativos a infrações pelas quais possa ser considerada responsável uma pessoa coletiva no Estado Parte requerente, em conformidade com o Artigo 10 da presente Convenção.
>
> 3. A cooperação judiciária prestada em aplicação do presente Artigo pode ser solicitada para os seguintes efeitos:
>
> a) Recolher testemunhos ou depoimentos;
>
> b) Notificar atos judiciais;
>
> c) Efetuar buscas, apreensões e embargos;
>
> d) Examinar objetos e locais;
>
> **e) Fornecer informações, elementos de prova e pareceres de peritos;**
>
> **f) Fornecer originais ou cópias certificadas de documentos e processos pertinentes, incluindo documentos administrativos, bancários, financeiros ou comerciais e documentos de empresas;**

> g) Identificar ou localizar os produtos do crime, bens, instrumentos ou outros elementos para fins probatórios;
>
> h) Facilitar o comparecimento voluntário de pessoas no Estado Parte requerente;
>
> i) Prestar qualquer outro tipo de assistência compatível com o direito interno do Estado Parte requerido.
>
> **4. Sem prejuízo do seu direito interno, as autoridades competentes de um Estado Parte poderão, sem pedido prévio, comunicar informações relativas a questões penais a uma autoridade competente de outro Estado Parte, se considerarem que estas informações poderão ajudar a empreender ou concluir com êxito investigações e processos penais ou conduzir este último Estado Parte a formular um pedido ao abrigo da presente Convenção.**
>
> 5. A comunicação de informações em conformidade com o parágrafo 4 do presente Artigo será efetuada sem prejuízo das investigações e dos processos penais no Estado cujas autoridades competentes fornecem as informações. **As autoridades competentes que recebam estas informações deverão satisfazer qualquer pedido no sentido de manter confidenciais as referidas informações, mesmo se apenas temporariamente, ou de restringir a sua utilização. Todavia, tal não impedirá o Estado Parte que receba as informações de revelar, no decurso do processo judicial, informações que inocentem um argüido.** Neste último caso, o Estado Parte que recebeu as informações avisará o Estado Parte que as comunicou antes de as revelar e, se lhe for pedido, consultará este último. Se, num caso excepcional, não for possível uma comunicação prévia, o Estado Parte que recebeu as informações dará conhecimento da revelação, prontamente, ao Estado Parte que as tenha comunicado. (...) (ONU, 2000, grifo do autor)

Conforme se observa no artigo 18, §2º, a transferência também poderá ocorrer quando o investigado ou processado for uma pessoa jurídica, o que foge ao escopo da LGPD, que tutela os dados pessoais.

Com efeito, o artigo 18, §4º da Convenção faculta aos Estados a possibilidade de transferir informações não solicitadas, quando acreditarem que esses dados poderão ajudar na condução de investigações e processos penais em curso em outros países.

A Convenção das Nações Unidas Contra a Corrupção (United Nations Convention against Corruption, UNCAC) foi promulgada em 31 de outubro 2003 e entrou em vigor em 14 de dezembro de 2005. No Brasil, foi aprovada por meio do decreto n.º 5.687, de 31 de janeiro de 2006. A convenção tem 71 artigos, separados em oito capítulos cujos mais importantes tratam dos temas da prevenção, penalização, recuperação de ativos e cooperação internacional.

O capítulo que trata da cooperação internacional destaca que todos os aspectos dos esforços anticorrupção carecem de cooperação internacional, tais como a assistência legal mútua na coleta e transferência de evidências e ações conjuntas de investigação e rastreamento.

Em seu art. 46, §1º, a UNCAC prevê que os Estados prestarão ampla assistência judicial, de forma recíproca, relativa às investigações, processos e ações judiciais relacionados com os delitos tipificados na própria Convenção. Como acontece com a Convenção de Palermo, a

UNCAC apresenta uma lista de possíveis pedidos de assistência judicial, entre os quais estão a apresentação de documentos judiciais, informações e elementos de prova e a entrega de documentos originais ou cópias, entre eles documentos públicos, bancários e financeiros.

Para aumentar a eficácia da aplicação da lei e estabelecer canais de comunicação para assegurar o intercâmbio rápido de informações sobre todos os aspectos dos crimes abrangidos pela convenção, os Estados Partes deverão cooperar entre si. Além disso, os Estados devem possibilitar a utilização de técnicas especiais de investigação, por exemplo, a vigilância eletrônica e outras formas de operações sigilosas, além de permitir a admissibilidade das provas obtidas por meio dessas técnicas nos tribunais.

A **sétima hipótese** é a prevista no inciso VII e dar-se-á quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 da LGPD, que prevê o seguinte:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), **deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público**, desde que:
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; (BRASIL, 2018).

O inciso VII tem o escopo de delimitar a margem de liberdade que tem o agente público, que poderá decidir pela necessidade de transferência de dados em consonância com a implementação de uma política pública e o cumprimento de obrigações legais, observada a publicidade da transferência. Com isso, o art. 33, VII, faz com que a transferência de dados para locais não seguros seja uma parte integrante do funcionalismo público, o que pode ameaçar a efetividade do inciso I do mesmo artigo.

A **oitava hipótese** ocorrerá quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades. Tal consentimento, nos termos do art. 5º, inciso XII, é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Conforme disposição do art. 7º da LGPD, o tratamento de dados poderá ser realizado quando houver consentimento do titular. Entretanto, consoante art. 8º, esse consentimento

deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Assim, parte-se do seguinte pressuposto: desde que as circunstâncias de uso e tratamento de dados sejam pormenorizadamente explicadas, o usuário, e titular dos dados, terá condições suficientes para autorizar ou não a transferência de suas informações pessoais.

Nessa ordem de ideias, é importante destacar o consentimento que se dá por meio dos famosos “Termos e Condições de Uso” e das “Políticas de Privacidade”. As informações sobre o tratamento de dados prestadas por meio desses termos ou políticas de privacidade, muitas vezes, são veiculadas no meio de textos volumosos, extremamente detalhados e recheados de termos técnicos, a exemplo dos termos usados nas redes sociais.

Fato é que os referidos “Termos e Condições de Uso” e as “Políticas de Privacidade” são deliberadamente ignorados pelos usuários. Assim, em que pese o fato de o usuário ter acesso às informações constantes dos referidos documentos, ele acaba escolhendo por ignorar as condições a que seus dados estão sendo submetidos. Com efeito, aceitar os termos não necessariamente significa que houve a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Ocorre que estudos demonstram que 91% dos usuários confirmam os termos de uso sem sequer ler seu conteúdo (MCDONALD; CRANOR, 2008, p. 565). Não é à toa que o número de usuários que não leem os termos de uso é grande. Isso porque, conforme destacado acima, os termos são complexos e longos. A título de exemplo, a leitura dos termos de uso dos oito principais serviços acessados na internet, como Google, Facebook e WhatsApp, demandaria aproximadamente quatro horas e meia (FOLHA TEC, 2017).

Ciente disso, em 2009, uma loja *online* britânica fez uma brincadeira com os seus clientes, colocando nos seus termos e condições de uso o seguinte: “Ao fazer uma compra neste site, você nos concede o direito intransferível, agora e para sempre, de propriedade da sua alma” (FOLHA TEC, 2017). É claro que a cláusula é abusiva e totalmente nula. Entretanto, ela chama a atenção para a importância de sabermos com o que estamos consentindo, quais os dados estamos disponibilizando *online* e para qual finalidade.

O problema aumenta com o aumento da oferta de aplicativos para smartphone e a capacidade de coleta de informação que os celulares têm. Uma coisa é certa, se o aplicativo é “grátis”, o preço está embutido nos dados que são coletados.

O livro "Terms of Service and Human Rights"[21] analisou contratos de 50 serviços disponibilizados na internet. Em 43 deles, uma eventual resolução de conflitos era delimitada a

[21] Termos de Serviço e Direitos Humanos, em tradução livre.

um lugar específico, normalmente a Califórnia. Treze deles proibiam ações coletivas. Ambas as situações poderiam ser entendidas como abusivas no Brasil e não teriam validade aqui, posto que a LGPD tem alcance extraterritorial.

A **nona e última hipótese** trata da possibilidade de transferência quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º, que prevê que o tratamento de dados pessoais somente poderá ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador; 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; ou 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) (BRASIL, 2018).

5 DIREITO COMPARADO: A PROTEÇÃO DE DADOS NA EUROPA

A União Europeia (UE) foi pioneira no que diz respeito ao controle e proteção dos dados pessoais ao criar a primeira normativa de caráter supranacional referente à privacidade e proteção de dados, qual seja a Diretiva[22] 95/46/EC[23]. A diretiva foi criada com o fim de harmonizar o grau de proteção existente nas leis nacionais e de assegurar o livre fluxo de informações pessoais entre os países membros da UE.

A diretiva foi aprovada em 24 de outubro de 1995, entrou em vigor três anos depois e, conforme seu artigo 1º, dispõe que os Estados Membros da EU devem assegurar em suas legislações domésticas, a proteção das liberdades e direitos fundamentais, especialmente à privacidade, no que tange aos dados pessoais (PARLAMENTO EUROPEU E CONSELHO, 1994).

O artigo 25 da referida Diretiva contém regra que acabou sendo fonte de problemas diplomáticos com países não membros da União Europeia. Isso porque a referida norma proíbe a transferência de dados pessoais de cidadãos europeus a países que não possuam "um nível de proteção adequado".

A adequação ao nível de proteção exigida na Diretiva é examinada levando-se em conta uma série de fatores, mas, sobretudo, as regras de direito em vigor no ordenamento jurídico do país para onde se pretende transferir os dados. Assim, para a Diretiva, a legislação de um Estado pode ser considerada adequada quando suas normas internas ou tratados e convenções internacionais que tenha subscrito se igualarem às normas da Diretiva, em termos de proteção de dados pessoais.

Considerando os problemas diplomáticos, ao longo dos anos 2000, a Comissão Europeia adotou, adicionalmente, o modelo de cláusulas contratuais padrão e regras corporativas vinculantes (ou *binding corporate rules*)[24], que não estavam previstas na Diretiva 95/46/EC, deixando espaço para a iniciativa privada estabelecer regulações privadas.

---

[22] A União Europeia, para alcançar os objetivos que estabeleceu por meio de Tratados, adota diversos tipos de atos legislativos, vinculativos ou não, aplicáveis a todos os países ou só a alguns países do bloco. Nesse sentido, temos que uma Diretiva é um ato legislativo que fixa um objetivo geral que todos os países da EU devem alcançar. Entretanto, cada país poderá criar a sua própria legislação para cumprir esse objetivo.

[23] A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, é datada de 24 de outubro de 1995 e é relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[24] Para um aprofundamento sobre o assunto, consulte Overview on Binding Corporate Rules. Disponível em: < https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en > Acesso em: 23 de maio de 2019

As normas corporativas vinculantes possibilitaram que empresas europeias e empresas localizadas fora do continente europeu definissem, de forma contratual, padrões de proteção de dados pessoais nas trocas transnacionais. Além das normas corporativas vinculantes, em casos de transferência internacional, as partes envolvidas poderiam recorrer também às cláusulas contratuais padrão[25] e às cláusulas específicas aprovadas pelos órgãos competentes.

Já em 2016, foi aprovado o Regulamento[26] nº 2016/679, de 27 de abril de 2016, relativo à proteção de dados pessoais. O regulamento, que passou a ser diretamente aplicável aos ordenamentos jurídicos dos países membros da UE a partir de 25 de maio de 2018, prevê regras sobre a transferência de dados para "países terceiros" e organizações internacionais (PARLAMENTO EUROPEU E CONSELHO, 2016).

Em 25 de maio de 2018 entrou em vigor na Europa a General Data Protection Regulation (GDPR) ou Regulamento Geral de Proteção de Dados, que estabelece as novas regras europeias em matéria de proteção de dados e se tornou um ponto de referência global, no que diz respeito à proteção de dados. O GDPR foi aprovado pelo Parlamento Europeu, com caráter uniformizador e manteve o mesmo modelo geral do critério da proteção equivalente da Diretiva 95/46.

O projeto começou a ser idealizado em 2012 para atualizar leis já existentes sobre proteção de dados e foi aprovado em 2016. O principal objetivo das regras é capacitar as pessoas e ajudá-las a obter um maior controle dos seus dados pessoais, o que já pode ser observado, uma vez que mais de dois terços dos europeus ouviram falar do regulamento e que as pessoas começam a exercer os seus novos direitos (COMISSÃO EUROPEIA, 2019).

Assim como ocorre com a LGPD, o GDPR considera dados pessoais qualquer informação que, isolada ou em conjunto com outras, sirva para identificar um usuário. Esses dados podem ser nome, endereço, e-mail, dados financeiros, endereço de IP, dados de navegação entre outros.

A GDPR deve ser observada por empresas europeias ou empresas que, independentemente de sua área de atuação, trabalhem com dados de cidadãos europeus, mesmo tendo sede em países que não estão dentro da União Europeia. Em caso de descumprimento das disposições do GDPR, as empresas estão sujeitas a multas em valores que variam de 2% a 4% de seu faturamento anual.

---

[25] Essas cláusulas-modelo devem ser utilizadas para transações comerciais e inseridas em contratos quando o responsável pelo tratamento dos dados não residir ou não tiver a base de suas operações em país integrante da União Europeia.

[26] O regulamento, por sua vez, é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da EU.

Com a entrada e vigor da GDPR, a coleta em massa de dados de qualquer internauta europeu só poderá ser feita com sua devida, expressa e inequívoca autorização que poderá, inclusive, ser revogada quando ele quiser. A GDPR também tem o objetivo de implementar termos de uso mais simples, claros e de fácil entendimento para qualquer indivíduo.

Apesar de a lei ter sido criada pela União Europeia, ela engloba toda e qualquer empresa que colete, armazene e processe dados de cidadãos europeus, independentemente de onde ela esteja sediada. Isso, em tese, significa que se uma pessoa tem uma loja virtual que envia produtos para o mundo inteiro e possui um único consumidor europeu, a regulação já pode ser aplicada em seu empreendimento.

A referida legislação tem seu alcance para além das fronteiras europeias, vinculando sua aplicação a empresas que possuam filiais em algum dos 28 países da União Europeia ou que ofereçam serviços a pessoas que ali se encontrem, prevendo, ainda, requisitos para que haja a transferência internacional de dados entre empresas.

Nesse sentido, vale destacar que antes da edição da LGPD, o Brasil não cumpriria os requisitos estipulados pela GDPR, por não oferecer um nível de proteção de dados pessoais adequado. Entretanto, hoje tanto a LGPD como a GDPR preveem a possibilidade de transferência internacional dos dados, desde que o país ou organismo internacional destinatário possua leis de proteção de dados com os mesmos padrões de segurança por ela assegurados; quando o controlador comprovar estar de acordo com os padrões da LGPD; em casos de cooperações jurídicas internacionais; proteção à vida ou incolumidade do titular ou terceiro, com autorização expressa do titular; ou em casos excepcionais previstos no corpo da lei.

Hoje, no que diz respeito à transferência internacional de dados na União Europeia e Brasil, temos o seguinte quadro:

Quadro 1 - Transferência Internacional de dados na LGPD e na GDPR

LGPD	GDPR
brasileira permite a transferência de dados pessoais para países ou órgãos internacionais que proporcionem grau de proteção de dados pessoais adequados ao previsto. A lei é breve quanto a este procedimento e elementos a serem considerados como adequados. A LGPD estabelece apenas diretrizes genéricas a serem observadas pelas autoridades nacionais e as hipóteses de transferência internacional estão previstas no art. 33 da LGPD.	rme disposição do GDPR, a transferência internacional dos dados pode ser realizada independente de autorização específica caso a comissão europeia reconheça que o país terceiro assegure um nível de proteção adequado. Não havendo nível de proteção adequado, a transferência internacional estará condicionada a garantias adequadas, que devem ser asseguradas pelo Agente. Todos os procedimentos e elementos que são levados em consideração pela Comissão para a autorização da transferência estão descritos na GDPR.

Fonte: o autor

Por fim, vale ressaltar que, assim como a LGPD, o GDPR possui alcance extraterritorial, uma vez que sua aplicabilidade se estende às empresas que tiverem filial na União Europeia e aos serviços prestados fora da UE por empresas que coletem dados de pessoas residentes lá ou em trânsito pelo velho continente.

6 CIBERESPAÇO E INTERNET

Antes de adentrar ao tema específico da definição da legislação aplicável e da competência judicial, alguns apontamentos sobre ciberespaço e internet são indispensáveis.

6.1 Ciberespaço

O termo ciberespaço é comumente associado à internet, porém, segundo Vesce (2019), o termo, que foi idealizado por William Gibson, surgiu em 1984, na sua obra Neuromancer, ou seja, muito antes da criação da rede mundial de computadores. Gibson define ciberespaço como um espaço existente no mundo da comunicação, um espaço virtual, portanto um espaço que não existe fisicamente. Nas palavras de Silvana Drumond Monteiro:

> O ciberespaço é definido como um mundo virtual porque está presente em potência, é um espaço desterritorializante[27]. Esse mundo não é palpável, mas existe de outra forma, outra realidade. O ciberespaço existe em um local indefinido, desconhecido, cheio de devires e possibilidades. Não podemos, sequer, afirmar que o ciberespaço está presente nos computadores, tampouco nas redes, afinal, onde fica o ciberespaço? Para onde vai todo esse "mundo" quando desligamos os nossos computadores? É esse caráter fluido do ciberespaço que o torna virtual. (MONTEIRO, 2008, p. 2)

Nesse meio, para que se possa construir uma fonte de relacionamento ou de troca de informações, não é necessária a presença física de um humano. O ciberespaço não se limita apenas a quem se conecta via internet. Ele é um ambiente onde ocorre a interação dos humanos com as tecnologias, ou seja, no uso de celulares, *pagers*, rádios, sistemas de bancos de dados, comunicações por mensagem eletrônica e on-line, televisão por satélite e os jogos e máquinas que se valem da realidade virtual, entre tantos outros.

No prefácio à edição brasileira (2003), o tradutor de Neuromancer, Alex Antunes, afirma que "o conceito criado por Gibson neste livro, o cyberespaço, é uma representação física e multidimensional do universo abstrato da 'informação'. Um lugar para onde se vai com a mente, catapultada pela tecnologia, enquanto o corpo fica para trás" (GIBSON, 2003, p.5-6). Para Gibson, na mesma obra, o ciberespaço é:

> Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos [...]. Uma

[27] Conforme Oliven (2006), a desterritorialização é um termo utilizado para designar fenômenos que se originam num espaço e que acabam migrando para outros. Desterritorialização, portanto, está intimamente ligada à ideia de desmaterialização, dissolução das distâncias, deslocalização de firmas ou debilitação dos controles fronteiriços (HAESBAERT, 2006, p. 67).

> representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade. (2003, p. 67).

Nesse sentido, podemos dizer que o ciberespaço é um local de disponibilização de informações possibilitado pelas novas tecnologias, especialmente, a internet. É um espaço aberto, virtual, fluído e navegável, que ainda não se conhece completamente e que apresenta vários desafios e incertezas.

Conforme destaca Monteiro (2008), o ciberespaço antecipa o futuro disruptivo que vemos nos filmes, nos romances, nas séries de ficção científica em que ocorre o fichamento de pessoas, tratamento de dados sem local definido, apagamento de memórias, ataques cibernéticos, tudo em tempo real.

Entretanto, fato é que a nossa sociedade já está imersa no ciberespaço e se utiliza desse campo para várias atividades, em que pese ainda não seja possível definir ou caracterizar as suas fronteiras e localização, ao contrário do que acontece com as fronteiras do território de um Estado, por exemplo.

Como exemplo da utilização do ciberespaço temos os serviços de *cloud computing*[28] e, entre estes, os serviços de armazenamento em nuvem[29]. Os serviços de armazenamento em nuvem disponibilizam um espaço virtual que pode ser utilizado para guardar qualquer tipo de arquivos, com a possibilidade de acessá-los de qualquer lugar com conexão à internet. Os mais famosos serviços de armazenamento em nuvem são o Dropbox, o OneDrive, o Google Drive e o iCloud.

Noutro giro, temos a definição proposta por Koepsell, que afirma que não há nada de estranho ou de muito especial no ciberespaço, mas que este "é apenas um meio composto de chips de silício, fios de cobre, fitas e discos magnéticos, cabos de fibra ótica e de todos os outros componentes de computadores, meios de armazenamento e redes que armazenam, transmitem e manipulam bits" (KOEPSELL, 2004, p. 125).

Esta definição proposta por Koepsell em muito se assemelha ao *backbone* ou espinha dorsal, que, como se verá a seguir, é a estrutura física propriamente dita, pela qual trafega a

---

[28] A *cloud computing* (ou computação em nuvem) é um termo amplo usado para dar nome a diferentes serviços relacionados à Tecnologia da Informação. Entre os mais famosos, temos o serviço de armazenamento em nuvem de e-mail, fotos, músicas, filmes, entre outros documentos e dados.

[29] O armazenamento em nuvem dispensa a necessidade de um armazenamento local, ou físico. Seja em um computador desktop, um notebook ou um smartphone, com o serviço de *cloud* não é necessário ter um *hard disk (HD), ou* disco rígido físico para guardar informações. Tudo fica guardado e disponível em um ambiente digital, a *cloud*, ou nuvem.

maioria dos dados transmitidos por meio da Internet, e é, em regra, composto de cabos de fibra ótica de alta velocidade.

Com efeito, discorrer ou conceituar o ciberespaço não é tarefa fácil em face de sua incipiência e da característica metamórfica de suas obras e, sobretudo, porque o virtual é o seu principal atributo. O ciberespaço, grosso modo, é uma grande máquina abstrata, onde se realizam trocas simbólicas, transações econômicas, comerciais, novas práticas comunicacionais, relações sociais, afetivas e, sobretudo, novos agenciamentos cognitivos[30].

Enfim, trata-se de um universo virtual proporcionado pelas redes de telecomunicações, sobretudo a Internet, cujo tamanho e dimensão são impossíveis de se visualizar; é um espaço móvel, paradoxal, um local invisível onde circulam conhecimentos, saberes e potências de pensamento; e, ainda, onde os dados pessoais dos indivíduos circulam diariamente, por isso a importância de se conhecer a nova noção de espaço que o ciberespaço propõe. Quanto a essa noção, Monteiro destaca o seguinte:

> Quanto à nova noção de espaço que o ciberespaço nos propõe, podemos afirmar que se trata de um local real, porém não físico. É um ambiente onde pessoas do mundo todo podem interagir sem estar, de fato, presentes. É um novo espaço de comunicação, representação e interação. O termo ciberespaço, em sua etimologia, já nos propõe essa nova noção: cyber-espaço, ou seja, um espaço diferente, cibernético, com novas possibilidades e implicações. (2008, p. 7)

Para Ianni (1995), a globalização tende a desenraizar as coisas, as pessoas e as ideias. Tudo tende a desenraizar-se: mercadoria, mercado, moeda, capital, empresa, agência, gerência, projeto, publicidade, tecnologia. Seria, portanto, segundo o autor, dessa forma que se desenvolveria o processo de desterritorialização, uma característica intrínseca da sociedade globalizada. Vejamos, nas palavras do autor:

> O conceito de desterritorialização aplica-se não apenas a óbvios exemplos, como corporações transnacionais e mercados monetários, mas também a grupos étnicos, lealdades ideológicas e movimentos políticos que atuam crescentemente em moldes que **transcendem fronteiras e identidades territoriais específicas**. A desterritorialização tem afetado as lealdades de grupos envolvidos em diásporas complexas, suas manipulações monetárias e outras formas de riqueza e investimento, bem como as estratégias de Estado. O debilitamento dos vínculos entre povo, riqueza e territórios, por sua vez, tem alterado a base de muitas interações globais significativas e, simultaneamente, **põe em causa a definição tradicional de Estado**. (IANNI, 1995, p. 93, grifos atuais).

Segundo Ianni (1995, p.169), "(...) o sujeito do conhecimento não permanece no mesmo lugar, deixando que seu olhar flutue por muitos lugares, próximos e remotos, presentes e

[30] Agenciamento é uma combinação de elementos heterogêneos dando origem a algo novo.

pretéritos, reais e imaginários". Partindo da ideia de que território[31] é um dos elementos que constitui os Estados, composto por uma porção física do planeta sobre o qual um país ele exerce a soberania, ou seja, é aquele espaço de estabilidade e organização, a ação de desterritorializar é uma ação de desordem, de fragmentação para buscar encontrar novos saberes, menos instituídos, adotando uma percepção diferenciada que está pronta para descobrir novas ideias além das previstas.

Diante das considerações acima e das definições e conceitos apresentados, podemos entender o ciberespaço como um mundo virtual, que rompe as fronteiras dos Estados nacionais, desterritorializado, onde temos à disposição variados meios de comunicação e interação em sociedade. É nesse universo virtual que estão presentes uma enorme gama de dados (entre eles dados pessoais) e informações dos mais variados tipos.

Também é no ciberespaço que estão presentes dispositivos de vigilância que monitoram as nossas ações e comunicações e as convertem em informações que farão parte de enormes bancos de dados e perfis computacionais que buscam antecipar preferências, tendências, escolhas, traços psíquicos ou comportamentais de indivíduos ou grupos, como ocorreu nas ações capitaneadas pela Cambridge Analítica nas eleições dos EUA e no *Brexit*. Quem nunca procurou por uma palavra no Google, como fone *bluetooth* e, ao abrir o Facebook, deparou-se com um anúncio da JBL de fones sem fio? Este autor já.

Com efeito, os diversos dispositivos digitais estão nos colocando em meio a formas sutis de controle e vigilância. Nesse sentido, interessantes são as considerações de Fernanda Bruno a respeito da vigilância no ciberespaço:

> Em primeiro lugar, trata-se de uma vigilância que não mais isola e imobiliza indivíduos em espaços de confinamento, mas que se aproxima ou mesmo se confunde com o fluxo cotidiano de trocas informacionais e comunicacionais. Uma vigilância que se exerce menos com o olhar do que com sistemas de coleta, registro e classificação da informação; menos sobre corpos do que sobre dados e rastros deixados no ciberespaço; menos com o fim de corrigir e reformar do que com o fim de projetar tendências, preferências, interesses. (BRUNO, 2006, p. 2)

Outro exemplo interessante é o do blogueiro iraniano Hossein Derakhshan que foi barrado ao tentar entrar nos Estados Unidos da América (EUA), depois que os oficiais de imigração fizeram uma pesquisa com seu nome no Google. A pesquisa teve como um dos resultados o blog do iraniano que fazia duras críticas ao governo estadunidense. O resultado não poderia ser outro, Hossein Derakhshan foi proibido de entrar nos EUA.

[31] É uma área certa e delimitada da superfície do planeta Terra, que contém a nação, dentro de cujas fronteiras o Estado exerce a sua soberania e jurisdição.

Estamos, portanto, diante de um quadro em que os sujeitos são, ao mesmo tempo, olhados e objetivados através de exames que irão constituir registros dos seus dados individuais (suas competências, evoluções, falhas, sintomas, características físicas e psíquicas, biografia, preferências políticas, orientação sexual etc.) e organizar campos comparativos que permitam classificar, formar categorias, estabelecer médias, fixar normas (Foucault, 1983a, p. 169).

Com efeito, não basta captar e documentar os dados e informações, é necessário classificar e produzir conhecimento, de modo a aumentar o poder social com a informação coletada. É ai que entra a participação dos *cookies* (ver item 6.2.4.6), dos bancos de dados, seus algoritmos e os perfis computacionais. De posse desse conhecimento, é possível utilizar os dados e informações para diversos fins (BRUNO, 2006), como a transferência internacional de dados com fins comerciais e políticos e o direcionamento de publicidade para os usuários da internet.

6.2 Internet

Feitas as considerações a respeito do ciberespaço, nesta subseção serão abordados o histórico e o conceito da rede mundial de computadores, mais conhecida como Internet. Além disso, será feita uma análise de cada um dos elementos que juntos dão forma a essa ferramenta de comunicação e proporcionam a interação instantânea entre usuários que se encontra a milhares de quilômetros de distância.

6.2.1 Histórico

A Internet proporcionou uma grande revolução nos meios de comunicação entre os mais diversos povos e culturas. Por ser um instrumento de alcance mundial de extrema praticidade, facilita a pesquisa acadêmica, auxilia no trabalho e contribui para o desenvolvimento humano, levando informação às áreas mais remotas e de difícil acesso do planeta. Entretanto, até chegar ao estágio atual, várias foram as etapas de aprimoramento e desenvolvimento desta tecnologia.

No fim da década de 1950, os Estados Unidos da América (EUA) criaram uma instituição de pesquisa, denominada de *Advanced Research Project Agency* ARPA, que fazia parte do Departamento de Defesa norte americano. Foi na ARPA que nasceu a internet, fruto do desenvolvimento de um programa militar das forças armadas estadunidenses que ganhou o nome da ARPANET.

O objetivo da instituição era implantar uma rede de comunicação entre os locais mais críticos do sistema da defesa dos EUA. Assim, o programa foi criado no ano de 1969 com o fim de tornar possível a comunicação e transferência de dados entre os seus usuários, como explica Marcel Leonardi:

> Este programa foi criado em 1969 com o objetivo de possibilitar a comunicação e transferência de dados entre seus usuários através de canais redundantes, de forma a garantir o funcionamento do sistema mesmo na hipótese de destruição de partes da rede em uma eventual guerra (LEONARDI, 2005, p. 12).

Assim, a ARPANET deveria ser forte o suficiente a ponto de continuar funcionando mesmo após ataques nucleares, com a consequente destruição de parte de sua rede. Portanto, o objetivo inicial era a comunicação interna, de modo que a ARPANET só passou a se conectar com redes externas a partir do ano de 1973.

O nome internet só veio à tona no ano de 1973 e foi fruto da pesquisa, na ARPA, do conceito de *internetworking,* que era a forma de conexão das várias redes. Com o início da comunicação externa, inclusive comunicação internacional, em meados da década de oitenta, a *National Science Foundation* dos EUA já havia criado a sua própria rede e em 1990 a ARPANET foi extinta (LEONARDI, 2005).

Já no Brasil, a internet foi lançada oficialmente apenas em 1989 e foi fruto do desenvolvimento da Rede Nacional De Pesquisa (RNP), uma iniciativa governamental do Ministério da Ciência e Tecnologia, com o apoio de fundações de pesquisa dos estados de São Paulo, Rio de Janeiro e Rio Grande do Sul.

6.2.2 Conceito

A Internet pode ser conceituada, de forma sintética, como a rede mundial (global ou internacional) de computadores conectados entre si, que possibilita a troca de informações de toda natureza. Vários são os conceitos formulados para tentar precisar o que seria a Internet, de modo que seria inviável relacionar todos. Entretanto, a título de conhecimento, é imperioso ressaltar a definição que alguns doutrinadores, órgãos governamentais bem como legislações pátrias formularam para este fenômeno.

A Agência Nacional de Telecomunicações – ANATEL, por sua vez, por meio da Nota Conjunta de junho de 1995, definiu a internet como o "nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos

necessários à comunicação entre computadores, bem como o 'software' e os dados contidos nestes computadores" (ANATEL, 1995).

O Marco Civil, em seu art. 5º, inciso I, define a internet como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para o uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes" (BRASIL, 2014).

Pedro Alberto de Miguel Asensio, a seu turno, observa que a Internet se traduz num "emaranhado mundial de redes conectadas entre si de modo a tornar possível a comunicação quase instantânea de qualquer usuário de uma dessas redes a outros situados em outras redes do conjunto, tratando-se de um meio de comunicação global" (ASENSIO, 2001, p. 27).

Segundo Carlos Tadeu Queiroz de Morais, a Internet pode ser definida como:

> A Internet é, portanto, uma rede mundial de computadores ou terminais ligados entre si, que tem em comum um conjunto de protocolos e serviços, de uma forma que os usuários conectados possam usufruir de serviços de informação e comunicação de alcance mundial através de linhas telefônicas comuns, linhas de comunicação privadas, satélites e outros serviços de telecomunicações. Com o surgimento da World Wide Web, esse meio foi enriquecido, o conteúdo da rede ficou mais atraente com a possibilidade de incorporar além de textos, imagens e sons. (MORAIS, 2012, p. 42).

Por fim, vale destacar que a palavra internet com o "i" minúsculo é resultado da contração de *interconnected network* (rede interconectada), que se refere a redes particulares de computadores interligadas entre si, sem relação alguma com a Internet mundial, propriamente dita (LEONARDI, 2011). Por fim, e como já destacado acima, ela não se confunde com o ciberespaço. De fato, a Web é o principal "local" do ciberespaço, seu principal edifício, podendo tomá-la como o centro de todas as possibilidades de interfaces.

6.2.3 Funcionamento

Para uma melhor compreensão do tema deste trabalho de conclusão de curso, é importante ter uma noção básica do funcionamento da internet, para que seja possível identificar a responsabilidade civil em casos de violação dos direitos dos titulares de dados pessoais. Nesse sentido, a supracitada norma conjunta da ANATEL definiu as características basilares do funcionamento da rede no Brasil. Vejamos:

> A Internet é organizada na forma de espinhas dorsais *backbones*, que são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade.

> Interligadas às espinhas dorsais de âmbito nacional, haverá espinhas dorsais de abrangência regional, estadual ou metropolitana, que possibilitarão a interiorização da Internet no País. Conectados às espinhas dorsais, estarão os provedores de acesso ou de informações, que são os efetivos prestadores de serviços aos usuários finais da Internet, que os acessam tipicamente através do serviço telefônico. Poderão existir no País várias espinhas dorsais Internet independentes, de âmbito nacional ou não, sob a responsabilidade de diversas entidades, inclusive sob controle da iniciativa privada (ANATEL, 1995).

Como podemos observar, a linguagem utilizada na definição é recheada de jargões e nomes técnicos próprios da área da computação que serão analisados separadamente a seguir. Em suma, o que se pode extrair do que foi dito acima é que existem vários computadores, conectados à internet, que compõe toda a rede. Os usuários desses computadores utilizam a rede, por meio de seu provedor de acesso, para se conectar à rede desse provedor. Esse provedor, a seu turno, está interligado a uma rede ainda maior, passando a fazer parte desta rede e assim sucessivamente. Graficamente, conforme figura 1:

Figura 1 - Backbone e Internet

Fonte: KOHN, 2014

Assim, temos que a Internet não é uma entidade física ou palpável, mas um emaranhado de pequenas redes compostas por um grupo de usuários, que se conecta a uma rede de maior abrangência. Essa conexão de uma rede regional a uma rede ainda maior possibilita a conexão entre usuários de diversos provedores de acesso, de qualquer rede do sistema. Vemos, portanto, que os dados pessoais dos usuários passam por um complexo emaranhados de redes para poder circular na Internet.

Com efeito, a troca de dados na rede, por meio dos serviços de internet, pode se dar de várias formas, como a *world wide web*, os mecanismos de busca como o Google, o correio eletrônico (*e-mail)*, os aplicativos de mensagens instantâneas, como o WhatsApp. Isso se dá porque qualquer usuário da rede pode se valer de vários meios de transmissão de informações, que podem ser utilizados para a difusão de dados, de modo que um meio será mais adequado

para a veiculação de um vídeo, enquanto outro meio será mais adequado para a transmissão de um simples texto.

O meio mais difundido e conhecido, sem dúvidas, é o *world wide web*, ou *web*, o famoso "www". A *web* nada mais é do que um grande número de dados armazenados em diferentes computadores de usuários do mundo todo. A *world wide web* pode se materializar num *web site* ou simplesmente site, ou sítio eletrônico.

Assim, para ter acesso às informações constantes de um site, o usuário terá que digitar um endereço (ou um conjunto de caracteres ordenado) de um determinado *web site* conhecido, de forma que localizará as informações e dados que busca. Grosso modo, é como se o usuário, por meio de seu computador, tivesse acesso a uma grande biblioteca, que na verdade é um conjunto de dados armazenados em um *web site* composto de várias páginas, cada uma destas correspondente a um endereço eletrônico.

O que torna viável a comunicação na internet é o *Transmission Control Protocol/Internet Protocol (TCP/IP)* [32] . Ele permite a comunicação entre diferentes computadores. É o Protocolo de Controle de Transmissão (TCP) que fraciona os dados a serem transmitidos e recebidos em pacotes. Na hora da transmissão, os dados são transmitidos em pequenos pedaços e na hora da recepção esses dados são reunidos novamente, formando, novamente, o dado, informação, texto originais que foram transmitidos.

O Protocolo de Internet (IP), a seu turno, atribui a cada pacote de dados o seu endereço de destino. Conforme o art. 5º, inciso III do Marco Civil da Internet, o endereço IP é o "código atribuído a um terminal de uma rede para permitir a identificação, definido segundo padrões internacionais" (BRASIL, 2014).

A identificação do endereço IP nos permite saber de onde se originou determinada conexão e diz respeito, em regra, ao local de uma conexão e não a uma máquina específica. Assim, quando um usuário faz uma conexão à rede, a sua máquina recebe um endereço IP do Provedor de Acesso.

6.2.4 Provedores de Serviços de Internet

Na linguagem do dia a dia, é comum que ocorra a confusão entre os vários termos e expressão utilizados no meio da Ciência da Computação, de modo que, não raro, algumas palavras são utilizadas como sinônimos de outras, de forma imprópria. Assim, é comum a

[32] Protocolo de Controle de Transmissão/Protocolo de Internet.

confusão entre provedores de serviços de internet, provedores de *backbone,* provedores de acesso, provedores de correio eletrônico, entre outros.

Portanto, para uma melhor compreensão sobre o tema, cada um destes termos será conceituado e explicado. Para isso, partiremos da premissa de que o **Provedor de Serviços de Internet é o gênero**, **do qual se originam as demais, espécies, quais sejam: provedores de *backbone*, acesso, correio eletrônico, hospedagem e conteúdo**. Cada um destes é uma atividade completamente distinta, entretanto, que pode ser prestada por uma mesma empresa a um mesmo usuário.

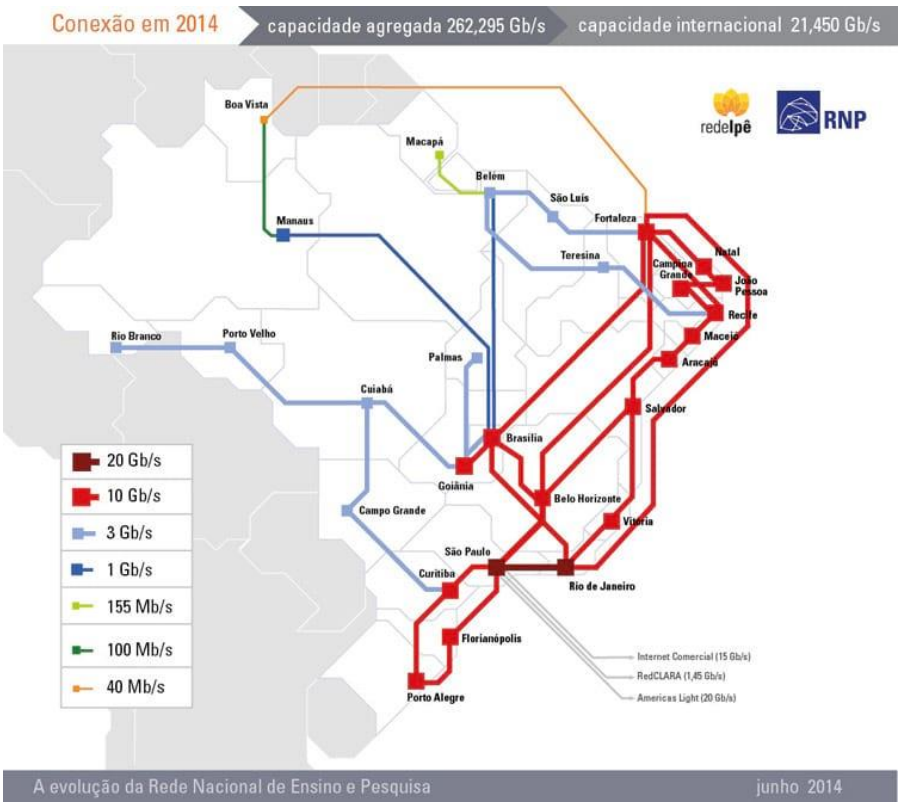
Nesse sentido, sob o ponto de vista jurídico, temos que o Provedor de Serviços de Internet é a pessoa (natural ou jurídica) que oferece os serviços relacionados à Internet.

6.2.4.1 Provedor de backbone

O *backbone,* ou espinha dorsal, é a estrutura física propriamente dita, pela qual trafega a maioria dos dados transmitidos por meio da Internet, e é, em regra, composto de cabos de fibra ótica de alta velocidade. Assim, o Provedor de *Backbone*, é a pessoa jurídica que efetivamente detém as estruturas físicas de rede aptas a veicular uma enorme quantidade de informações.

Os Provedores de *backbone* são constituídos basicamente de roteadores de tráfego interligados por circuitos de alta velocidade, consoante a Nota Conjunta de 1995 da ANATEL. Em suma, o *backbone* é um **conjunto de pontos físicos** de internet que veiculam dados entre diversos usuários. Abaixo podemos ver uma figura ilustrativa do *backbone* da Rede Nacional de Ensino e Pesquisa, o primeiro *backbone* nacional, fundado em 1997:

Figura 2 - O backbone brasileiro



Fonte: MULLER, 2015

O primeiro Provedor de *backbone* brasileiro foi a Rede Nacional de Pesquisa (RNP) e dela dependeu o desenvolvimento da Internet no Brasil até que as empresas privadas conseguissem criar e disponibilizar novas estruturas parecidas. **O provedor de *backbone* oferece conexão à rede, vendendo o acesso à sua infra-estrutura a outras empresas**, que a seu turno, revendem o acesso ou hospedagem para os usuários finais. Assim, o usuário final, que se conecta à rede por meio de um provedor de acesso, raramente tem contato direto com o provedor de *backbone* (LEONARDI, 2005).

Os principais provedores de *backbone* existentes no Brasil são a Embratel, a Rede Nacional de Pesquisa (RNP), a Oi, Algar Telecom, entre outros. São essas as empresas que, efetivamente, detêm a conexão com o sistema de cabeamento de transporte de dados (LEONARDI, 2005).

6.2.4.2 Provedor de Acesso

Conforme mencionado acima, o usuário final se conecta à rede por meio de um provedor de acesso à Internet, que é a pessoa jurídica que fornece serviços de conexão. Essas pessoas jurídicas, que normalmente são empresas, podem ter o seu próprio *backbone* ou dispõe de um acesso a um *backbone* de terceiros. A Rede Nacional de Ensino e Pesquisa (RNP) define provedor de Acesso da seguinte forma:

> O provedor de acesso é aquele que se conecta a um provedor de backbone através de uma linha de boa qualidade e revende conectividade na sua área de atuação a outros provedores (usualmente menores), instituições e especialmente a usuários individuais, através de linhas dedicadas ou mesmo através de linhas telefônicas discadas (RNP, 1996, p. 7).

O provedor de acesso, portanto, pode ser comparado a um varejo, cujo produto vendido é o acesso à Internet, disponibilizando conexões de largura de banda menor, mas suficiente para a demanda de seus clientes. O provedor de *backbone,* a seu turno, analogamente, atende o atacado fornecendo conexões com largura de banda maior devido ao volume de dados que recebem de seus clientes e tem como principal função interconectar outras redes e assim permitir o "trânsito" de informações de uma rede para outra.

Assim, o objeto do acordo entre o consumidor final e o provedor de acesso é a atribuição, ao usuário, de um endereço de IP, para que ele possa se conectar à Internet. Notamos, portanto, que aqui existe uma relação de consumo entre provedor de acesso e usuário, celebrada, usualmente, por meio de contratos de adesão, relação esta regida pelo Código de Defesa do Consumidor.

Os principais provedores de acesso à internet brasileiros são a Oi, a Algar Telecom, a Vivo, a Net Virtua, a GVT, entre outros. Um provedor de acesso, portanto, tem como principal serviço prover conexão à Internet para algum usuário externo, residencial ou corporativo. Esse meio de acesso físico é o que permitirá a conexão dos equipamentos dos usuários aos demais serviços disponíveis na Internet.

Nesse sentido, temos que o acesso à Internet implica duas atividades, quais sejam, o serviço de telecomunicação, que é a ligação entre a casa do usuário e um ponto da operadora de telecomunicações, e posteriormente a atividade de conexão a Internet propriamente dita.

6.2.4.3 Provedor de correio eletrônico

O Provedor de Correio Eletrônico, a seu turno, é a pessoa jurídica que fornece serviços de envio de mensagens de um usuário a seus destinatários, por meio do uso de um nome de usuário e senha exclusivos. Os provedores de correio mais populares são Gmail (Google), Yahoo e Hotmail (Microsoft). Grosso modo, são as pessoas jurídicas que fornecem o serviço de e-mail.

6.2.4.4 Provedor de Hospedagem

Conforme definição de Marcel Leonardi, "provedor de hospedagem é a pessoa jurídica que fornece o serviço de armazenamento de dados em servidores próprios de acesso remoto, possibilitando o acesso de terceiros a esses dados" (LEONARDI, 2005, p. 25). Vemos, portanto, que são dois serviços. Um é o serviço de armazenamento de dados. O outro é o serviço de acesso de terceiros a estes dados, conforme o que foi avençado.

Grosso modo, o que o provedor de hospedagem faz é ceder um espaço em disco rígido de acesso remoto, bem como o acesso do conteúdo armazenado a terceiros, por meio de um contrato de *hosting* (contrato de hospedagem). Entretanto, esse acesso a terceiros pode ser concedido à qualquer pessoa ou apenas a usuários determinados. Parellada, citando Lorenzetti, define o contrato de *hosting* da seguinte forma:

> O hosting é um contrato mediante o qual o prestador de serviço concede ao seu co-contratante gratuitamente ou por um pagamento de um preço em dinheiro o direito ao alojamento de arquivos informáticos em um servidor (que pode ser próprio do prestador ou só gozar de um direito de uso sobre ele) que ficam à disposição do público. Existem, portanto, duas relações diversas: a do alojamento do arquivo (entre o prestador e o introdutor da página) e a de acesso à informação (do público ao servidor), conectadas assim ao introdutor, interessando-lhe a extensão do público. Por sua vez, o prestador pode fazê-lo sobre hardware próprio ou alheio, com software próprio ou alheio e com combinações dessas modalidades, como sobre hadware próprio e com software alheio e inversamente (PARELLADA, 1999, p. 168 apud LORENZETTI, 2000 p. 446-447).

Conforme destaca Leonardi (2005, p. 25), os provedores de hospedagem também podem "oferecer serviços adicionais, tais como locação de equipamentos informáticos e de servidores, registros de nomes de domínio, cópias periódicas de segurança do conteúdo do *website* armazenado, entre outros". Entretanto, esses serviços adicionais não são necessários para que o provedor seja considerado de hospedagem.

Como podemos observar, a Internet depende da inter-relação de todos estes provedores para que exista e funcione. Assim, os serviços prestados pelos provedores de hospedagem são indispensáveis para a existência dos provedores de conteúdo, próximo tópico deste estudo, visto que, necessariamente, terão que utilizar os seus serviços para disponibilizar informações na rede.

Por fim, importante destacar que o provedor de hospedagem não controla o conteúdo que é armazenado nos seus discos rígidos, seja qual for o grau de complexibilidade dos serviços armazenados. Em nosso país, os provedores de hospedagem mais conhecidos são o UOL Host e a Localweb.

6.2.4.5 Provedor de Conteúdo ou de informação

Como se observa em boa parte da literatura jurídica a respeito do tema, usualmente as expressões "provedor de informação" e "provedor de conteúdo" são utilizadas como sinônimos, embora, a rigor, não sejam. A esse respeito, discorre Marcel Leonardi:

> O ***provedor de informação*** é toda pessoa natural ou jurídica responsável pela criação das informações divulgadas através da Internet. É o efetivo autor da informação disponibilizada por um provedor de conteúdo. O ***provedor de conteúdo*** é toda pessoa natural ou jurídica que disponibiliza na Internet as informações criadas ou desenvolvidas pelos provedores de informação, utilizando para armazená-las servidores próprios ou os serviços de um provedor de hospedagem. Dessa forma, o provedor de conteúdo pode ou não ser o próprio provedor de informação, conforme seja ou não o autor daquilo que disponibiliza. (LEONARDI, 2005, p. 27, grifos no original)

Conforme a legislação de regência, ou seja, o Marco Civil da Internet, o **Provedor de Conteúdo** disponibiliza na internet as informações criadas ou desenvolvidas pelos provedores de informação. Os provedores de conteúdo podem usar servidores próprios ou os serviços de um provedor de hospedagem para armazená-las, conforme destacado acima. A título de exemplo, os provedores de conteúdo podem ser pessoas naturais que mantêm um blog pessoal ou então grandes portais de imprensa. Finalmente, o **Provedor de Informação** é o autor de fato da informação veiculada.

6.2.4.6 Navegador de internet

Os navegadores de internet, também chamados de *browsers*, são *softwares* que possibilitam o acesso do usuário à diversos sites. O navegador possui uma interface gráfica que inclui botões de navegação, uma barra de endereços e uma barra de status.

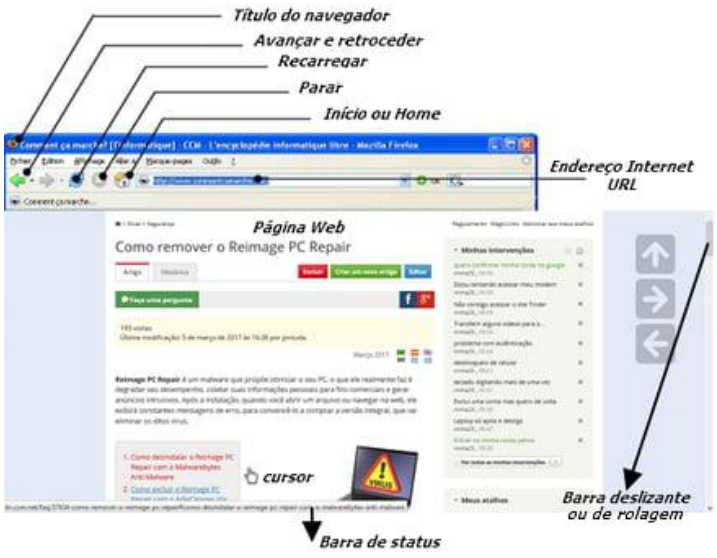
Como exemplo de navegadores de internet, temos o Internet Explorer e o Google Chrome. A maioria das interações na Internet ocorre por meio de um navegador que permite que o usuário tenha acesso às páginas disponibilizadas na *World Wide Web*.

Com efeito, a *World Wide Web*, é o nome específico do sistema de documentos que pode ser acessado com um navegador, que se comunica através do provedor de acesso. Grosso modo, a *web* é o conjunto de páginas que podem ser acessadas com o navegador de preferência do usuário. Conforme explica Hautsch:

> Fechar o Internet Explorer (IE) não significa "fechar a internet". Você estará conectado à internet assim que o seu modem começar a se comunicar com o computador central da operadora que você escolheu, não quando abrir o IE. Este é somente um programa de navegação (navegador) que possibilita acessar páginas hospedadas nos computadores ao redor do mundo. (2009)

Para acessar qualquer site, o usuário deverá digitar o *Uniform Resource Locator* (URL), ou simplesmente endereço, correspondente na barra de endereços do seu navegador, como se observa na imagem a seguir:

Figura 3 - Navegador e URL



Fonte: PILLOU, 2017

Existem, basicamente, três maneiras de navegar na internet. A primeira é quando o usuário conhece o endereço do site que deseja visitar, bastando digitar o URL na barra de endereços e validar pressionando a tecla Enter ou clicar no botão de validação do próprio navegador. A segunda é quando o usuário está procurando uma informação para obter o endereço de um site. Como o usuário não dispõe do URL, é preciso fazer uma pesquisa nos motores de busca como o Google, Bing, Yahoo, para encontrar as informações procuradas, com a ajuda de palavras-chaves. E a terceira é quando o usuário navega na internet sem um objetivo definido, entrando numa página da Internet e seguindo os links que aparecem (PILLOU, 2017).

Com efeito, importante salientar que "ao visitar websites, os usuários são 'carimbados' de forma a facilitar o reconhecimento em caso de novo acesso, o que se dá por meio dos '*cookies*', sendo possível, dessa forma, inferir suas preferências de consumo" (LEME, 2019). Os *cookies* são responsáveis por guardar as preferências e dados dos usuários, como informações de login, senhas e acessos realizados pelos titulares dos dados (FURUTANI, 2018). Nas palavras de Gabriel Gugik,

> Basicamente, um Cookie é um arquivo de texto muito simples, cuja composição depende diretamente do conteúdo do endereço Web visitado. Por exemplo, a maioria do sites armazenam informações básica, como endereços IP e preferências sobre idiomas, cores, etc. Contudo, em portais como o Gmail e o Hotmail, nomes de usuários e senhas de email também fazem parte dos Cookies. (GUGIK, 2008)

Assim, por meio dos *cookies*, é possível mapear as preferências de um usuário, conforme o seu comportamento na internet. Com efeito, os dados que são disponibilizados nestes acessos à internet são ferramentas valiosas para a promoção de bens de consumo por meio da publicidade.

Nesse sentido, Leme (2019, p. 11) destaca a chamada "publicidade comportamental online, a qual é a responsável por identificar padrões de consumo, personalizando as ofertas apresentadas aos internautas de acordo com seus acessos". Com o mapeamento do comportamento do usuário, é possível a personalização da publicidade que lhe será apresentada ao acessar novamente a internet (BIONI, 2019, p. 19). Nas palavras de Carolina da Silva Leme:

> Em termos mais práticos, o mapeamento dos registros de acesso possibilita que o usuário realize uma pesquisa de uma viagem a ser realizada pelo seu celular e, ao acessar sua rede social via computador lhe apareça uma publicidade acerca do site de viagens e do destino consultados. (LEME, 2019, p. 11)

Apesar das facilidades que os *cookies* apresentam, estes também trazem ônus, por exemplo, uma invasão à privacidade dos usuários, sendo de fundamental importância verificar quais dados são atualmente coletados pelos serviços mais utilizados por usuários brasileiro, a fim de analisar se essa coleta está de acordo com o Marco Civil da Internet e com a Lei Geral de Proteção de Dados, que entrará em vigor no próximo ano.

7 A DEFINIÇÃO DA LEGISLAÇÃO APLICÁVEL E DA COMPETÊNCIA JUDICIAL NOS CASOS DE RESPONSABILIDADE CIVIL DECORRENTE DA VIOLAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

Com o fenômeno da globalização, houve o aumento das relações que possuem caráter internacional, como acontece nos casos de transferência internacional de dados. A consequência desse fenômeno foi o fato de que estas relações passaram a acarretar efeitos além das fronteiras territoriais, sendo de suma importância a definição do efetivo contorno da competência internacional dos Estados para julgar tais litígios.

Conforme destacado acima, são inúmeros os direitos dos titulares de dados, as formas de violá-los, bem como os sujeitos que podem violá-los. Ademais, as hipóteses de transferência internacional de dados são taxativas. Dito isso, é necessário que o titular dos dados saiba a quem recorrer em uma eventual situação de transferência não prevista na lei ou no caso de responsabilidade civil decorrente da violação da proteção de seus dados numa operação de tratamento e transferência internacional.

Nesse sentido, para que seja possível a tutela efetiva dos seus dados, o usuário precisa ter claro qual é o local de ajuizamento de uma eventual ação judicial, bem como qual é a lei aplicável aos casos de ajuizamento de ação no Brasil, hipóteses que serão abordadas a seguir.

Antes de delimitar o local de ajuizamento da ação, é importante relembrar, de modo sucinto, o que é jurisdição e o que é competência. Nesse sentido, temos que a jurisdição é o poder de aplicar a lei ao caso concreto e a competência é a medida desta jurisdição.

A competência e a jurisdição mantêm um relacionamento tão estreito que, por vezes, acabam sendo confundidas, ou tratadas como um único instituto do Direito. Isto se dá até pelo fato de que a competência é o limite da jurisdição, ou, como prefere Alvim (2015), a competência nada mais é do que “a medida da jurisdição”.

Nesse sentido, a competência é a quantidade de jurisdição, assinalada pela lei, ao exercício de cada órgão jurisdicional. Assim, as restrições ao exercício da jurisdição provêm da lei, que traça os limites dentro dos quais a jurisdição pode ser exercida. Não fosse assim, qualquer juiz poderia apreciar e consequentemente julgar qualquer matéria ou litígio que a ele se apresentasse.

7.1 Local do ajuizamento da ação

Conforme destacado acima, a jurisdição é demarcada e limitada pela competência. Sendo assim, cada juízo só pode julgar aquelas causas que estão compreendidas em seu âmbito jurisdicional, delimitado pela lei, visto que, fora desses limites, é incompetente.

Nesse viés, surgiu também a necessidade de se delimitar a competência no âmbito internacional, que ficou determinada no Título II do Livro II (arts. 21 a 41) do Código de Processo Civil (CPC). É neste título que o CPC trata das hipóteses em que a Justiça Brasileira é competente para julgar uma demanda, sem excluir a possibilidade da referida causa ser julgada pela Justiça Estrangeira.

No Brasil, a jurisdição nacional limita-se ao território nacional[33] e se manifesta consoante algumas circunstâncias previstas nos arts. 21 e seguintes do CPC. Registramos, nesse sentido, que a jurisdição da autoridade brasileira para processar e julgar ações pode se dar de maneira concorrente com as autoridades estrangeiras, ou pode se manifestar de maneira exclusiva.

A jurisdição concorrente está tratada nos arts. 21 e 22 do CPC. Vejamos o que dispõe o art. 21:

> 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.
> Parágrafo único. Para o fim do disposto no inciso I, considera-se domiciliada no Brasil a pessoa jurídica estrangeira que nele tiver agência, filial ou sucursal. (BRASIL, 2015)

O inciso I trata da hipótese do réu que tem domicílio no Brasil e se aplica independentemente de sua nacionalidade, bastando que seja domiciliado aqui.

Para que se compreenda o dispositivo, é necessário relembrar o que é domicílio, instituto jurídico que vem tratado nos arts. 70 e seguintes do Código Civil de 2002. O art. 70 do CC dispõe que "o domicílio da pessoa natural é o lugar onde ela estabelece a sua residência com ânimo definitivo" (BRASIL, 2002). Se, porém, a pessoa natural tiver diversas residências, onde, alternadamente, viva, considerar-se-á domicílio seu qualquer delas, conforme disposição do art. 71 do CC.

[33] Território nacional é a área que compreende todo o espaço terrestre, fluvial, marítimo e aéreo considerado por lei como território brasileiro.

Noutro giro, conforme versa o art. 72 do CC, quanto às relações concernentes à profissão, o lugar onde esta é exercida também é considerado domicílio. Além do mais, "se a pessoa exercitar profissão em lugares diversos, cada um deles constituirá domicílio para as relações que lhe corresponderem" (BRASIL, 2002).

Por fim, temos a hipótese do domicílio contratual, disposta no art. 78 do CC, versando que nos contratos escritos, poderão os contratantes especificar domicílio onde se exercitem e cumpram os direitos e obrigações deles resultantes (BRASIL, 2002).

Em se tratando de pessoa jurídica, além do que dispõe o par. único do art. 21 do CPC [34], é de se ressaltar o teor do inciso IV e §§ 1º e 2º do art. 75 do CC:

> Art. 75. Quanto às pessoas jurídicas, o domicílio é:
> (...)
> IV - das demais pessoas jurídicas, o lugar onde funcionarem as respectivas diretorias e administrações, ou onde elegerem domicílio especial no seu estatuto ou atos constitutivos.
> § 1o Tendo a pessoa jurídica diversos estabelecimentos em lugares diferentes, cada um deles será considerado domicílio para os atos nele praticados.
> **§ 2o Se a administração, ou diretoria, tiver a sede no estrangeiro, haver-se-á por domicílio da pessoa jurídica, no tocante às obrigações contraídas por cada uma das suas agências, o lugar do estabelecimento, sito no Brasil, a que ela corresponder**. (BRASIL, 2002, grifos atuais)

Vemos que o conceito de domicílio da pessoa jurídica é amplo e considera domiciliadas aqui, aquelas que, de algum modo, estiverem estabelecidas ou tenham representação no Brasil.

Quanto ao inciso II do art. 21 do CPC o elemento que atrai a jurisdição concorrente da autoridade judiciária brasileira é o local de cumprimento da obrigação. Nesse caso, não importa se o vínculo obrigacional foi estabelecido no exterior, ou entre estrangeiros, o que importa é que a obrigação tenha que ser cumprida em território brasileiro.

O inciso III do art. 21 do CPC, por sua vez, contem previsão ainda mais ampla acerca da jurisdição concorrente, dispondo que a autoridade judiciária brasileira será competente sempre que se tratar de causa oriunda de fatos ocorridos no Brasil ou então de atos aqui praticados. Assim, basta que a ação a ser ajuizada tenha como causa de pedir fato ocorrido no Brasil ou ato aqui praticado.

O art. 22 do CPC, por sua vez, trata das ações que versem sobre alimentos, sobre relações de consumo e sobre as hipóteses em que as partes optarem pela legislação brasileira, sendo competente a autoridade brasileira para todos estes casos.

---

[34] Considera-se domiciliada no Brasil a pessoa jurídica estrangeira que nele tiver agência, filial ou sucursal.

O inciso II do art. 22 cuida de ações em que se debatem as relações de consumo. Desse modo, tendo o consumidor domicílio ou residência no Brasil, há jurisdição brasileira concorrente para processar e julgar a ação.

O inciso III do art. 22, a seu turno, relaciona-se a situações em que as partes se submeteram expressa ou tacitamente à jurisdição brasileira. Nesta hipótese são irrelevantes, portanto, o aspecto territorial e a nacionalidade das partes.

O art. 24 do CPC, por sua vez, trata da ausência de litispendência entre ação ajuizada no Brasil e ação ajuizada no exterior. O referido artigo trata das hipóteses em que a jurisdição brasileira não é exclusiva, quais sejam as hipóteses dos arts. 21 e 22 do CPC, conforme observamos a seguir:

> Art. 24. A ação proposta perante tribunal estrangeiro não induz litispendência e não obsta a que a autoridade judiciária brasileira conheça da mesma causa e das que lhe são conexas, ressalvadas as disposições em contrário de tratados internacionais e acordos bilaterais em vigor no Brasil.
> Parágrafo único. A pendência de causa perante a jurisdição brasileira não impede a homologação de sentença judicial estrangeira quando exigida para produzir efeitos no Brasil. (BRASIL, 2015)

Além disso, temos a situação da cláusula de eleição de foro, prevista no art. 25 do CPC em que as partes de determinada relação contratual podem optar pela autoridade judiciária estrangeira para fins de resolução de conflitos eventualmente surgidos acerca deste contrato. Conforme disposição do art. 25, a autoridade judiciária brasileira é incompetente para processar e julgar ação quando houver cláusula de eleição de foro exclusivo estrangeiro em contrato internacional, arguida pelo réu na contestação.

O § 1ºdo artigo em análise, a seu turno, contém uma exceção: "Não se aplica o disposto no caput às hipóteses de competência internacional exclusiva previstas neste Capítulo" (BRASIL, 2015). As hipóteses de competência brasileira exclusiva são as previstas no art. 22 do CPC, que não interessam a este trabalho.

Por fim, temos o § 2º do art. 25 que prevê a possibilidade de rejeição da aplicação da cláusula de eleição de foro estrangeiro exclusivo, caso se trate de uma cláusula abusiva.

7.2 Lei aplicável aos casos de ajuizamento da ação no Brasil

Conforme já destacado neste trabalho, no mundo globalizado em que vivemos, as fronteiras virtuais entre países vão sendo rompidas pelas trocas comerciais, pelas novas tecnologias e pelo intercâmbio da força de trabalho, dando espaço a novas relações jurídicas.

Ocorre que estas novas relações jurídicas podem ensejar aparentes conflitos de leis no espaço, ou seja, para uma dada matéria podem, a princípio, existir diferentes normas jurídicas aplicáveis, envolvendo diferentes Estados, sendo de suma importância saber qual a norma aplicável ao caso concreto.

Com efeito, para se solucionar esse aparente conflito de normas, a LINDB determina qual será o direito aplicável para cada tipo de demanda pluriconectada, por meio das suas regras de conexão.

As regras de conexão são definidas pela lei do Estado (*Lex Fori)*. Entretanto, também é facultado às partes, envolvidas em um conflito de leis no espaço, definir o elemento de conexão, por meio da autonomia da vontade. Porém, para que isso ocorra, é preciso que tal possibilidade esteja expressamente descrita na *Lex Fori*. Ademais, os tratados internacionais também têm o condão de definir elementos de conexão, desde que tenham sido aceitos pelo Estado e incorporados ao seu ordenamento jurídico.

As principais regras de conexão vigentes no ordenamento jurídico brasileiro são de três tipos e dizem respeito ao estado das pessoas (elementos de conexão pessoais), a bens móveis ou imóveis (elementos de conexão reais) ao local de celebração ou execução do contrato (elementos de conexão conducistas). Para este trabalho, o que interessa são os elementos de conexão relativos ao local de celebração ou execução do contrato, no caso, o contrato internacional.

Os contratos internacionais[35] são aqueles firmados com pessoas ou organizações de diferentes países. A negociação de qualquer contrato internacional implica além das cláusulas que definem as condições negociais, também as cláusulas relativas à eleição de foro e da lei aplicável ao caso concreto.

Considerando que essas relações jurídicas envolvem duas ou mais partes domiciliadas em países diferentes, é necessário determinar qual o ordenamento jurídico aplicável ao caso concreto, em uma eventual ação judicial ajuizada no Brasil.

No Brasil aplica-se, em regra, como elemento de conexão o art. 9º da LINDB, que versa o seguinte:

> Art. 9o Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituirem.
> § 1o Destinando-se a obrigação a ser executada no Brasil e dependendo de forma essencial, será esta observada, admitidas as peculiaridades da lei estrangeira quanto aos requisitos extrínsecos do ato.

[35] Como exemplo de contratos internacionais temos os contratos de *franchising, factoring, leasing, letters, joint-venture*, de informática, de *catering*, de agência e de *know-how*.

> § 2o A obrigação resultante do contrato reputa-se constituida no lugar em que residir o proponente. (BRASIL, 1942)

Como podemos notar no dispositivo legal supracitado, não foi reconhecida a autonomia da vontade como elemento de conexão para se determinar a lei aplicável a um contrato internacional. Assim, em se tratando de contrato internacional, independentemente de as partes contratantes serem ou não nacionais do mesmo Estado e terem ou não o mesmo domicílio, aplica-se a lei do lugar do ato (art. 9º, caput, LINDB). Em outras palavras, onde se contratar, a lei local (territorial) regulará suas condições. Noutro giro, tratando-se de contrato internacional que venha a ser executado no Brasil e dependa de forma essencial (art. 9º, § 1º, LINDB), ele deverá obedecer à lei brasileira.

Cabe ressaltar que no Brasil há uma hipótese em que é possível que as partes escolham, de forma direta, a lei aplicável ao contrato internacional, que é por meio do instituto da arbitragem. Conforme disposição do §1º do art. 2º da Lei de arbitragem, "poderão as partes escolher, livremente, as regras de direito que serão aplicadas na arbitragem, desde que não haja violação aos bons costumes e à ordem pública" (BRASIL, 1996).

CONCLUSÃO

Como pudemos observar, o tema abordado, em que pese ser tratado especificamente em apenas quatro artigos da LGPD, quais sejam os artigos 33, 34, 35 e 36, envolve matérias de Direito Constitucional, Direito Civil, Direito Processual Civil, Direito Internacional, Direito do Consumidor, Direito Digital, tratados e convenções estrangeira e noções de Ciência da Computação. Além disso, a LGPD é extremamente recente, não entrou em vigor e ainda não foi enfrentada pelos tribunais pátrios, nem pelos órgãos de defesa do consumidor. Entretanto, algumas considerações sobre o tema já podem ser feitas.

A primeira delas é no sentido de que não seria absurdo dizer que os dados pessoais são o novo petróleo, tendo em vista o seu valor comercial, político e econômico. Desde os escândalos envolvendo a Cambridge Analytcs, o Facebook e o SERPRO e com a criação do GDPR e da LGPD fica patente a necessidade de atenção da sociedade para a questão do tratamento destes dados, incluindo aí a transferência internacional de dados pessoais.

É de se notar também que com a LGPD, o Brasil entra para o time dos países que contam com um nível adequado em termos de proteção de dados pessoais, podendo, portanto, ser um país destinatário de dados pessoais oriundos de países que exigem um nível adequado de proteção destes, como é o caso dos Estados da União Europeia. Entretanto, o que é considerado "nível adequado", ainda é controverso e carrega certo grau de subjetivismo, dando margem a diversas interpretações tanto na LGPD, como no GDPR.

Como foi destacado acima, antes da LGPD, o Brasil não dispunha de uma legislação específica sobre o tema. Notamos que o conceito de dado pessoal na LGPD é mais extensivo que o conceito adotado pelo Marco Civil da Internet, não se limitando a dados de subscrição ou nome, endereço, CPF, englobando, inclusive dados sensíveis, como orientação sexual e preferências políticas, como também dados biométricos.

A LGPD, no que diz respeito à sua abrangência, tem aplicação mais ampla que o Marco Civil da internet. Ela dispõe sobre o tratamento de dados pessoais, *online* e/ou *offline*, 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, estabelecendo regras e limites para empresas a respeito da coleta, armazenamento, tratamento e compartilhamento de dados.

Quanto aos direitos dos titulares de dados, como não há, em nossa Constituição, nenhum direito absoluto, os direitos de privacidade, liberdade e livre desenvolvimento da personalidade,

até mesmo os sigilos pessoais constitucionalmente tutelados, podem sofrer alguma restrição ou ponderação com outros direitos.

Outro ponto que chama atenção na lei é a questão da efetividade da anonimização de dados. Isso porque, em alguns casos, seria tecnicamente possível reverter o processo e reidentificar o titular dos dados, ainda que sem total certeza acerca da sua identidade. Por esse motivo, a LGPD estabelece que essa reversão deva se dar a partir do uso exclusivo de meios próprios ou de esforços razoáveis, considerando fatores objetivos, tais como o custo e o tempo necessários para a reversão desse processo, bem como a tecnologia disponível na ocasião da reversão.

Nesse sentido, para garantir o cumprimento da lei e mitigar o risco de vazamento, é recomendável que as empresas busquem padrões e técnicas de anonimização que garantam a irreversibilidade do processo ou pelo menos estabeleçam um maior grau de dificuldade, a ponto de não incentivar a sua reversão, dado o elevado custo e tempo para atingir esse objetivo ou o controle de terceiros acerca das regras aplicáveis a esse processo.

Entretanto, é inegável o avanço em matéria de empoderamento dos titulares de dados pessoais, que passarão a ter maior controle sobre o tratamento de seus dados, haja a vista a ampla gama de obrigações que os controladores e operadores terão, bem como as vultosas multas que poderão ser aplicadas em casos de violações de direitos dos titulares assim que a lei entrar em vigor. Antes da edição da lei, a legislação específica sobre o tema era esparsa e apresentava lacunas, especialmente no caso da transferência internacional de dados.

Entretanto, com o advento da lei, os requisitos e as hipóteses para a transferência internacional de dados estão previstos no Capítulo V, art. 33 e seguintes da LGPD. Conforme art. 33 da LGPD, a transferência internacional de dados só é permitida em nove hipóteses que são tratados nos nove incisos do referido artigo. Desse modo, entendemos que o rol do art. 33 é taxativo, ressalvadas as exceções legais previstas no ordenamento jurídico brasileiro.

Ademais, além de haver hipóteses taxativas de transferência internacional, o titular dos dados ainda conta com o respaldo dos princípios da finalidade, minimização da coleta e retenção mínima, por meio dos quais os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares, devendo ser coletados somente os dados mínimos necessários para que se possa atingir a finalidade, e deverão ser imediatamente excluídos após atingida a finalidade pela qual eles foram coletados

Quanto ao aspecto transfronteiriço, a LGPD, no mesmo sentido do que já era disposto no art. 11 do Marco Civil da internet, também tem aplicação extraterritorial, sendo aplicável não só às empresas que tem estabelecimento no Brasil, mas também às empresas que oferecem

serviços no nosso país e tem sede fora ou então às empresas que tratem dados de pessoas localizadas no Brasil.

Para fins de verificar como é tratada a questão em outros países, a partir da comparação da LGPD com o GDPR, verifica-se, assim como a LGPD o GDPR possui alcance extraterritorial, uma vez que sua aplicabilidade se estende às empresas que tiverem filial na União Europeia e aos serviços prestados fora da UE por empresas que coletem dados de pessoas residentes lá ou em trânsito pelo velho continente.

Ademais, ambas as legislações impõem como requisito para a transferência internacional um nível de proteção adequado dos dados pessoais veiculados. Não havendo nível de proteção adequado, a transferência internacional estará condicionada a garantias adequadas.

No caso do GDPR, as garantias devem ser asseguradas pelo Agente. No caso da LGPD, ocorre quando o controlador dos dados oferece e comprova que garante o cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de cláusulas contratuais específicas para determinada transferência, cláusulas padrão contratuais, normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos.

Quanto à proteção efetiva dos dados pessoais no Brasil, na seara extrajudicial, hoje o trabalho de tutela é feito principalmente pelos órgãos de defesa do consumidor, como Procons e a Secretaria Nacional de Defesa do Consumidor, e pelo Ministério Público. A área é regida principalmente pelo Código de Defesa do Consumidor e pelo Marco Civil da Internet, passando a ser complementada pela LGPD.

Entretanto, com a entrada em vigor da LGPD, espera-se que a tutela dos titulares de dados seja concentradas na Autoridade Nacional de Proteção de Dados, que terá como atribuições o estabelecimento de padrões técnicos, a avaliação de cláusulas e jurisdições estrangeiras no que tange a proteção de dados, a determinação para a elaboração de Relatórios de Impacto, a fiscalização e aplicação de sanções, atividades de difusão e educação sobre a lei, bem como demais atribuições que visam a correta aplicação da lei e os princípios da proteção de dados pessoais como um todo.

Ademais, no âmbito judicial, a depender do caso concreto, conforme as normas que disciplinam o local de ajuizamento da ação e a lei aplicável ao caso, a ação poderá ser ajuizada no Brasil, podendo ser aplicável o ordenamento jurídico pátrio.

Além disso, vale reiterar que a LGPD tem incidência ampla e se aplica, conforme seus arts. 1º e 3º, a pessoas naturais ou jurídicas, de direito público ou privado, independentemente do país de sua sede ou de onde estejam localizados os dados, desde que o tratamento de dados

ocorra em território nacional; o tratamento de dados tenha por objetivo a oferta ou o fornecimento de bens ou serviços no território brasileiro ou o tratamento de dados de indivíduos localizados no Brasil; e os dados pessoais tenham sido coletados de indivíduos localizados no Brasil no momento da coleta.

No que tange aos dados a serem coletados pelas empresas, a LGPD é expressa quanto à necessidade. Isto é, as empresas deverão coletar os dados dos titulares que sejam necessários para a execução de suas finalidades, o que também se aplica à transferência de dados entre empresas, salvo em caso de "legítimos interesses do controlador", prevalecendo os direitos e liberdades fundamentais dos titulares.

Esse conceito de "legítimo interesse" foi importado do GDPR e, conforme o conceito de "nível adequado de proteção", suscita debate em razão de sua forma genérica. Nesse sentido, pode ser hipóteses diversas se encaixem na referida exceção, de modo que esta seja a regra no lugar do consentimento inequívoco do usuário.

Outra questão que pode ser controversa quando a lei entrar em vigor é a prevista no inciso VII do art. 33 da LGPD, que tem o escopo de delimitar a margem de liberdade que tem o agente público, que poderá decidir pela necessidade de transferência de dados em consonância com a implementação de uma política pública e o cumprimento de obrigações legais. Com isso, o art. 33, VII, faz com que a transferência de dados para locais não seguros seja uma parte integrante do funcionalismo público o que pode ameaçar a efetividade do inciso I do mesmo artigo.

É importante destacar, ainda, a sensibilidade do consentimento para coleta e transferência de dados. Conforme mencionado, este deve ocorrer de maneira prévia, gratuita, informada e inequívoca por parte de seu titular. Entretanto, conforme estudos citados neste trabalho 91% dos usuários confirmam os termos de uso de serviços de internet sem sequer ler seu conteúdo. Assim, em que pese o fato do usuário ter acesso às informações constantes dos referidos documentos, ele acaba escolhendo por ignorar as condições a que seus dados estão sendo submetidos.

Com efeito, aceitar os termos não necessariamente significa que houve a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Ademais, vale ressaltar o cenário de vigilância constante em que estamos inseridos. Nos exemplos mencionados neste trabalho, como o das publicidades direcionadas, já encontramos algumas das principais características dessa nova forma de vigilância, que, a título de exemplo, pode se dar por meio dos *cookies* que aparecem nos navegadores de internet. Esta não seria,

portanto, uma forma de violar o direito à privacidade do indivíduo nas redes? Qual é o dispositivo de vigilância que capta essas informações? Em que lugar do ciberespaço ele e os nossos dados pessoais se encontram? Os nossos dados estão sendo captados e transferidos internacionalmente sem o nosso consentimento? É possível precisar a que jurisdição estaria submetido o responsável por esse dispositivo de vigilância? São estas algumas das perguntas que a noção de ciberespaço acaba suscitando, tendo em vista a sua desterritorialização e virtualidade.

Com efeito, ao voltarmos a atenção para o ciberespaço e os dados pessoais que circulam nesse ambiente, nos deparamos com uma enorme ampliação das capacidades de coleta, registro, processamento e transferência de informações sobre indivíduos, possibilitada pela vigilância digital.

É justamente esse cenário que preocupa, visto que as mesmas tecnologias que ampliam as possibilidades de emissão, acesso e distribuição da informação tornam-se instrumentos de vigilância e controle. São essas mesmas tecnologias que possibilitaram o anonimato nas trocas sociais e comunicacionais, que se mostram eficientes instrumentos de identificação. A vigilância se confunde hoje com a própria paisagem do ciberespaço.

Por fim, vale destacar que no caso de uma violação de um direito de um titular de dados pessoais em uma operação de transferência internacional de dados alguns aspectos devem ser observados. O primeiro deles é identificar qual o direito do usuário foi violado. O segundo é identificar se a transferência efetuada está prevista nas hipóteses do art. 33 da LGPD. Após, é necessário verificar qual será o direito aplicável à hipótese conforme as regras de conexão da LINDB e as previsões da LGPD, bem como qual será o local de ajuizamento da ação, consoante o regramento trazido pelo CPC. Identificado o direito aplicável e o local de ajuizamento da ação, necessário identificar quais as sanções previstas para o tipo de violação ocorrida.

Portanto, com base no disposto no parágrafo anterior, se um dado foi coletado de um usuário de algum serviço de internet no Brasil, transferido a uma empresa estadunidense e nessa ocasião houve a violação de algum direito deste usuário, como o direito à privacidade, em que pesem eventuais disposições dos termos de uso desse serviço versarem que é aplicável a lei da Califórnia, será aplicável o ordenamento jurídico brasileiro para a tutela desses usuários, podendo ser a ação ajuizada no Brasil (art. 21, III do Código de Processo Civil), conforme as regras de conexão previstas no art. 9º da Lei de Introdução às normas do Direito Brasileiro (e tratadas na seção 7 deste trabalho), estando a empresa sujeita às sanções administrativas previstas no art. 52 da LGPD, por exemplo, multa de 50 milhões de reais, bem como poderá ser responsabilizada civilmente a reparar danos morais e materiais.

REFERÊNCIAS

Agência Senado (Ed.). **Projeto de lei geral de proteção de dados pessoais é aprovado no Senado.** 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/07/10/projeto-de-lei-geral-de-protecao-de-dados-pessoais-e-aprovado-no-senado>. Acesso em: 01 jun. 2019.

ALVIM, José Eduardo Carreira. **Teoria Geral do Processo**. 18. ed. Rio de Janeiro: Forense, 2015.

BIONI, BR. **Proteção de dados pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL, Decreto – **Lei nº. 4.657, de 4 de setembro de 1942** – Lei de Introdução às Normas do Direito Brasileiro. Disponível em http://www.planalto.gov.br/ccivil_03/decretolei/Del4657compilado.htm, último acesso em 28 de maio de 2019.

_____. **Constituição da República Federativa do Brasil**. Presidência da República, Brasília, DF, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 05 abril de 2019.

_____. **Lei n. 9.307 de 23 de setembro de 1996**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9307.htm> Acesso em: 28 mai 2019.

_____. Lei nº 10.406 de 10 de janeiro de 2002. **Código Civil**. Presidência da República, Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 22 maio 2019.

_____. **Lei nº 12.956, de 23 de Abril de 2014**. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Presidência da República, Brasília, DF. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 maio de 2019.

_____. Lei nº 13.105, de 16 de março de 2015. **Novo Código de Processo Civil**. Presidência da República, Brasília, DF, 16 mar 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: 22 maio 2019.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Presidência da República, Brasília. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 01 maio de 2019.

BRUNO, Fernanda. **Dispositivos de vigilância no ciberespaço**: duplos digitais e identidades simuladas. Fronteiras: estudos midiáticos, São Leopoldo, v. 8, n. 2, p.1-8, jan. 2006.

Disponível em: <http://revistas.unisinos.br/index.php/fronteiras/article/view/6129>. Acesso em: 25 maio 2019.

BULOS, Uadi Lammêgo. **Constituição Federal anotada**, 2010

CISG. Convenção de Viena das Nações Unidas sobre Contratos de Compra e Venda Internacional de Mercadorias. **A CISG.** 2019. Disponível em: <http://www.cisg-brasil.net/a-cisg>. Acesso em: 20 maio 2019.

COLUMBUS, Louis. **10 Charts That Will Change Your Perspective Of Big Data's Growth.** Disponível em: <https://www.forbes.com/sites/louiscolumbus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/#24847c762926>. Acesso em: 28 abr. 2019.

COMISSÃO EUROPEIA. **Regulamento Geral de Proteção de Dados**: um ano depois. 2019. Disponível em: <http://europa.eu/rapid/press-release_IP-19-2610_pt.pdf>. Acesso em: 23 maio 2019.

DELECRODE, Amanda. **Boilerplate Clauses (Cláusulas Padrão):** Common Law. 2017. Disponível em: <https://amandadelecrode.jusbrasil.com.br/artigos/467530295/boilerplate-clauses-clausulas-padrao?ref=topic_feed>. Acesso em: 01 jun. 2019.

ELOLA, Joseba. **É possível navegar pela Internet sem deixar rastros?** A luta pela privacidade é uma batalha perdida Qualquer um pode saber o que acontece no seu computador. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/04/10/tecnologia/1523373306_036349.html>. Acesso em: 05 jul. 2018.

FARIA, William Rodrigues de. **LGPD e GDPR:** 7 princípios que a Ti deve colocar em prática. 2019. Disponível em: <https://cio.com.br/lgpd-e-gdpr-7-dicas-para-coloca-las-em-pratica-em-ti/>. Acesso em: 22 maio 2019.

FOLHA TEC (Ed.). **Leitura de 'termos e condições' de serviços na internet exige 4,5 horas.** 2017. Disponível em: <https://nic.br/noticia/na-midia/leitura-de-termos-e-condicoes-de-servicos-na-internet-exige-4-5-horas/>. Acesso em: 02 jun. 2019.

FOUCAULT, M. 1983a. **Vigiar e punir.** Petrópolis, Vozes, 272 p

FURUTANI, Karola. **Aprenda o que são Cookies e qual é a função deles no seu computador**. 2018. Disponível em: <https://www.meupositivo.com.br/doseujeito/tendencias/o-que-sao-cookies/>. Acesso em: 02 jun. 2019.

GIBSON, Willian. **Neuromancer**. São Paulo: Aleph, 2003

GUGIK, Gabriel. **O que são Cookies?** 2008. Disponível em: <https://www.tecmundo.com.br/web/1069-o-que-sao-cookies-.htm>. Acesso em: 02 jun. 2019.

HAESBAERT, R. **Concepções de território para entender a desterritorialização**. In: SANTOS, M. et al. Território, territórios: ensaios sobre ordenamento territorial. 2 ed. Rio de Janeiro: DP&A, 2006. 43-70.

HAUTSCH, Oliver. **Dicas para internautas de primeira viagem**. 20099. Disponível em: <https://www.tecmundo.com.br/web/2558-dicas-para-internautas-de-primeira-viagem.htm>. Acesso em: 02 jun. 2019.

IANNI, O. A desterritorialização. In: _____**A sociedade global**. Rio de Janeiro: Civilização Brasileira, 1995. p. 89-105.

KOEPSELL, David R. **A ontologia do ciberespaço**: a Filosofia, a lei e o futuro da propriedade intelectual. São Paulo: Madras, 2004.

KOHN, Ricardo. **Acesso à internet no Brasil.** 2014. Disponível em: <https://rrupta.wordpress.com/2014/05/22/acesso-a-internet-no-brasil/>. Acesso em: 20 nov. 2018.

LEME, Carolina da Silva. **Proteção e tratamento de dados sob o prisma da legislação vigente**. Revista Fronteiras Interdisciplinares do Direito, [s.l.], v. 1, n. 1, p.178-197, 9 maio 2019. Portal de Revistas PUC SP. http://dx.doi.org/10.23925/2596-3333.2019v1i1a10.

LEMOS, André. **Ciberespaço e Tecnologias Móveis:** Processos de Territorialização e Desterritorialização na Cibercultura. Bauru: CompÓs, 2006. Disponível em: <http://www.compos.org.br/data/biblioteca_531.pdf>. Acesso em: 25 maio 2019.

LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet.** São Paulo: Juarez de Oliveira, 2005.

_____. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

MARQUES, Marília. G1. **MP do DF aponta suposto esquema de venda de dados pessoais de brasileiros pelo Serpro.**2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/mp-do-df-aponta-suposto-esquema-de-venda-de-dados-pessoais-de-brasileiros-pelo-serpro.ghtml>. Acesso em: 29 abr. 2019.

MASSON, Nathalia. **Manual de Direito Constitucional.** 4. ed. Salvador: Juspodivm, 2016.

MATOS, David. **Conceitos Fundamentais de Machine Learning.** 2017. Disponível em: <http://www.cienciaedados.com/conceitos-fundamentais-de-machine-learning/>. Acesso em: 09 jul. 2018.

MCDONALD, AM.; CRANOR, LF. **The Cost of Reading Privacy Policies**. Journal of Policy for
Information Society, Vol. 4, 2008

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet; COELHO, Inocêncio Mártires. **Curso de Direito Constitucional**. 51 ed. São Paulo: Saraiva, 2010.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa.** São Paulo: Melhoramentos, 2019. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/liberdade/>. Acesso em: 01 maio 2019.

MONTEIRO, Silvana Drumond. O Ciberespaço: o termo, a definição e o conceito. **Datagramazero**: Revista de Ciência da Informação, São Paulo, v. 8, n. 3, p.1-20, jul. 2007. Disponível em: <http://www.brapci.inf.br/_repositorio/2010/01/pdf_31a590c998_0007547.pdf>. Acesso em: 25 maio 2019.

MORAES, Alexandre de. **Curso de Direito Constitucional**. 26! ed. São Paulo: Atlas, 2010.

MORAIS, Carlos Tadeu Queiroz de. **Conceitos sobre Internet e Web** / Carlos Tadeu Queiroz de Morais, José Valdeni de Lima [e] Sérgio R. K. Franco. – Porto Alegre: Editora da UFRGS, 2012.

MOREIRA, Rodrigo Pereira. **Direito ao livre desenvolvimento da personalidade:** Caminhos para a Proteção e Promoção da Pessoa Humana. 2015. 291 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal de Uberlândia, Uberlândia, 2015.

MULLER, Nicolas. **O que é um backbone?** 2015. Disponível em: <https://www.oficinadanet.com.br/post/14168-o-que-e-um-backbone>. Acesso em: 20 nov. 2018.

NOVELINO, Marcelo**. Manual de Direito Constitucional.** 9. ed. São Paulo: Método, 2014**.**

OLIVEN, R. G. **Território, fronteiras e identidades**. In: SCHULER, F.; BARCELLOS, M de A. (Org.) Fronteiras: arte e pensamento na época do multiculturalismo. Porto Alegre: Sulina, 2006. p. 157-166.

ONU. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS**, 1948. Disponível em: < http://www.onu.org.br/img/2014/09/DUDH.pdf> Acesso em : 05 jul 2018.

ONU. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Convenção das Nações Unidas contra o Crime Organizado Transnacional**, 15 novembro 2000. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm >. Acesso em: 21 mai. 2019.

ONU. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Convenção das Nações Unidas contra a Corrupção**, 31 outubro 2003. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5687.htm >. Acesso em: 21 mai. 2019.

PARELLADA, Carlos. **La responsabilidad civil por los daños a terceros ocasionados por el contenido de Páginas Web em Internet**, in Revista de responsabilidad civil y seguros, la

ley, no. Dec. 1999, apud LORENZETTI, Informática, cyberla, e-commerce, tradução de Edson Bini, in Direito & Internet – Aspectos Jurídicos Relevantes, coordenado por Newton De Lucca e Adalberto Simão Filho, Bauru: Edipro, 2000, p. 446

PARLAMENTO EUROPEU E CONSELHO, Diretiva 2016/680, de 27 de abril de 2016, relativa à proteção de dados singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680> Acesso em 23 de maio de 2019.

_____. **Diretiva 94/46/CE**, 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoas e à livre circulação desses dados. Disponível em: < https://publications.europa.eu/pt/publication-detail/-/publication/7901bc34-f83d-4a58-ae31-7efcc784d58a/language-pt/format-PDF/source-search >. Acesso em: 21 mai. 2019.

PILLOU, Jean-françois. **O navegador web.** 2017. Disponível em: <https://br.ccm.net/contents/832-o-navegador-web>. Acesso em: 02 jun. 2019.

RE 215.984, relatado pelo Min. Carlos Velloso, 21 Turma, STF

RNP. Rede Nacional de Ensino e Pesquisa. **Guia do Usuário:** Internet/Brasil. 1996. Disponível em: <https://memoria.rnp.br/_arquivo/documentos/rpu0013d.pdf>. Acesso em: 20 nov. 2018.

RONCOLATO, Murilo. **O uso ilegal de dados do Facebook pela Cambridge Analytics**. E o que há de novo. 2018. Disponível em: <https://www.nexojornal.com.br/expresso/2018/03/19/O-uso-ilegal-de-dados-do-Facebook-pela-Cambridge-Analytics.-E-o-que-h%C3%A1-de-novo>. Acesso em: 05 jul. 2018.

SCHREIBER, Anderson. **Direitos da Personalidade.** 2. ed. São Paulo: Atlas, 2013.

SCHWENZER, Ingeborg; PEREIRA, Cesar A. Guimarães; TRIPODI, Leandro (Org.). **Convenção das Nações Unidas sobre os Contratos de Compra e Venda Internacional de Mercadorias (CISG):** Convenção das Nações Unidas sobre os Contratos de Compra e Venda Internacional de Mercadorias (CISG). São Paulo: Marcial Pons, 2015.

SERASA EXPERIAN (Ed.). **A anonimização de dados na LGPD.** 2019. Disponível em: <https://www.serasaexperian.com.br/a-anonimizacao-de-dados-na-lgpd>. Acesso em: 01 maio 2019.

STJ – REsp 794.586, rel. Min. Raul Araújo 15.03.2012

VESCE, Gabriela E. Possolli. **Ciberespaço.** Disponível em: <https://www.infoescola.com/internet/ciberespaco/>. Acesso em: 25 maio 2019.

WAMBIER, Teresa Arruda Alvim et al. **Primeiros comentários ao novo código de processo civil***:* artigo por artigo. 2. ed. São Paulo: Revista dos Tribunais, 2016.

ZULIANI, Ênio Santarelli et al. **Responsabilidade Civil na Internet e nos demais meios de comunicação.** 2. ed. São Paulo: Saraiva, 2012.