JURISDIÇÃO E TRANSFERÊNCIA DE DADOS: DESAFIOS PARA A PROTEÇÃO DO DIREITO À PRIVACIDADE

WELLINGTON ANTONIO BALDISSERA*

* Bacharel em Direito pela Universidade Regional do Alto Uruguai e das Missões - Campus Erechim (2018). Mestrando em Direito pela Faculdade Meridional - IMED, na linha de pesquisa Efetividade Do Direito, da Democracia e da Sustentabilidade com bolsa na modalidade taxa CAPES/PROSUP. Pós-Graduando em Direito Administrativo pelo Complexo Educacional Renato Saraiva (CERS). Assessor Jurídico na área de Direito Público. Advogado-OAB/RS 112119.

RESUMO

Com a popularização da internet, vários fatos novos passaram a necessitar da tutela do direito, todavia, algumas dessas novas situações não eram tratadas com a atenção que merecem. A jurisdição em demandas envolvendo a proteção de dados na internet é um destes aspectos que precisou ser melhor analisado, tanto na esfera nacional quanto internacional. O objetivo geral deste estudo é a importância do estabelecimento de normas específicas sobre a jurisdição de transferência de dados para a preservação do direito à privacidade. E a principal conclusão que foi realizada a partir do que foi abordado no transcorrer do texto que a melhor opção seria a criação de um direito internacional de proteção de dados. O método utilizado nessa pesquisa é o monográfico e a técnica de pesquisa é a bibliográfica.

PALAVRAS-CHAVE

Internet; direito internacional; proteção de dados.

INTRODUÇÃO

Com os adventos das novas tecnologias surgem novas relações e conflitos que precisam ser resolvidos pelo direito. A popularização da internet trouxe um novo panorama para a nossa sociedade, trazendo à tona situações que até pouco tempo não recebiam atenção dos legisladores do nosso país e, inclusive não sendo apreciadas como deveriam pelo direito internacional.

A proteção dos dados pessoais é uma dessas novas demandas que o direito precisa se preocupar, alguns pontos conseguem ser cobertos pelo texto da Constituição Federal de 1988, diante das garantias que ela fornece em face da semelhança com fatos que já eram corriqueiros, antes desse assunto entrar em evidência.

Dessa relação, deriva diretamente as questões sobre a jurisdição e transferência de dados eletrônicos, seja numa perspectiva internacional ou nacional, diante da imprecisão tanto da legislação brasileira, ou de uma norma que abranja todos os países, para definir as competências de julgamento, tanto na esfera criminal quanto na civil, nos casos envolvendo estes conflitos.

O problema que se pretende responder com o presente estudo é: quais são os desafios para a preservação do direito à privacidade na definição da jurisdição de transferência de dados pessoais, tanto na esfera internacional quanto nacional?

O objetivo geral é demonstrar a importância do estabelecimento de normas específicas sobre a jurisdição de transferência de dados para a preservação do direito à privacidade. Como objetivos específicos, esta pesquisa apresenta: (i) definir um entendimento sobre o que é o direito à privacidade; (ii) apresentar conceitos e informações sobre o que são os dados pessoais e suas aplicações na internet; (iii) explicar sobre a jurisdição de dados pessoais na internet, na esfera internacional e na nacional e a relação existente com o direito à privacidade; (iv) demonstrar sugestões para solucionar as questões indefinidas sobre a jurisdição dos dados pessoais na internet.

O método de abordagem utilizado nesta pesquisa foi o hipotético- dedutivo, o método de procedimento foi o comparativo, o tipo de pesquisa tem natureza qualitativo-exploratória, e a técnica de pesquisa utilizada, é a pesquisa bibliográfica.

1. DIREITO À PRIVACIDADE NA CONSTITUIÇÃO FEDERAL DE 1988

Com o intuito de propiciar o melhor entendimento possível do objeto principal deste estudo, é imprescindível expor a concepção existente em nosso ordenamento sobre o que é o direito à privacidade, de uma forma mais abrangente, não focado especificamente na questão da proteção de dados, assunto que será tratado no capítulo seguinte, mas sim, na perspectiva apresentada na nossa Constituição Federal, em que eram observados os fatos que ocorriam na época de sua promulgação.

Obviamente, a sociedade brasileira sofreu várias mudanças desde a entrada em vigor da Constituição Federal de 1988, sendo que esta permanece em vigência até os dias atuais, dessa forma, não compreende todos os novos fatos que vieram a surgir com o advento das novas tecnologias, principalmente da internet, sendo um desafio para o direito brasileiro garantir a preservação dos dados pessoais de seus cidadãos que estão disponibilizados na rede.

O maior problema para definir o que é o direito à privacidade é que não existe um conceito preciso sobre, nem na doutrina, nem nas legislações, uma vez que há grandes divergências na doutrina e que, na Constituição Federal de 1988, não é utilizada expressamente a palavra privacidade, todavia, os direitos que são protegidos pelo inciso X do art. 5º da nossa Carta Magna, tem o objetivo de garantir o que pode ser considerado como os preceitos fundamentais para a privacidade do cidadão brasileiro, sendo que o seu teor diz que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (BRASIL, 1988)

Ainda, no inciso XII do art. 5º da Constituição Federal, é mencionado especificamente sobre a proteção de dados, evidentemente vista numa perspectiva diferente da dos dias atuais, mas que devido a possibilidade de interpretação e adequação da norma, garante a proteção dos dados pessoais de qualquer pessoa, tanto dos vinculados à internet quanto em outros

meios de comunicação, ou em outras situações mais específicas. No seu texto, está definido que:

> [...] 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).

Com relação a natureza desse direito, ele pode ser compreendido de várias formas: pode ser entendido como parte do chamado direito humano; como um direito fundamental, que para alguns doutrinadores, seriam classificações semelhantes, no entanto, cada uma possui sua peculiaridade, na visão do autor desta pesquisa e, inclusive, também pode ser entendido como um direito da personalidade da pessoa humana.

Diante do que foi supramencionado, convém fazer uma rápida conceituação do que seria cada uma das classificações apresentadas. Com relação aos direitos humanos, podem ser entendidos como:

> [...] aqueles que possuem relação com o direito internacional, por fazerem referência àquelas posições jurídicas que se reconhecem ao ser humano como tal, independentemente de sua vinculação com uma determinada ordem constitucional e, por isso mesmo, aspirando à validade universal, valendo para todos os povos e em todos os tempos, ou seja, revelando um caráter supranacional. (WENCZENOVICZ; BAEZ, 2016, p. 104-105).

Já os direitos fundamentais, têm uma profunda relação com os direitos humanos, pois todo titular de um direito fundamental, também é um ser humano. Esta categoria pode ser conceituada assim:

> Os direitos fundamentais podem ser conceituados como a categoria jurídica instituída com a finalidade de proteger a dignidade humana em todas as dimensões. Por isso, tal qual o ser humano, tem natureza polifacética, buscando resguardar o homem na sua liberdade (direitos individuais), nas suas necessidades (direitos sociais, econômicos e culturais) e na sua preservação (direitos relacionados à fraternidade e à solidariedade). (ARAUJO, 2005, p.109-110).

Na legislação brasileira, a maioria dos direitos fundamentais são encontrados no artigo 5º da nossa Constituição Federal atual, sendo que no inciso X, são definidos os direitos que necessitam ser garantidos para assegurar a privacidade do cidadão brasileiro, dessa maneira, sendo possível o entendimento de que a privacidade também pertence a este rol.

Todavia, existem algumas peculiaridades, que diferem o entendimento que há sobre direitos humanos do existente sobre direitos fundamentais, sendo a principal característica que os diferencia é que os direitos fundamentais estão positivados na Constituição de um Estado. Sobre isso:

> Evidentemente, direitos fundamentais e direitos humanos guardam estreita relação, na medida em que os direitos fundamentais são, na verdade, os direitos humanos positivados, garantidos pela Constituição e, portanto, representam um elenco de direitos considerados fundamentais para determinada sociedade. Assim sendo, se configuram no tal conjunto de faculdades e instituições que, em cada momento histórico, concretizam as exigências sociais, razão pelas quais, cada Estado tem seus direitos fundamentais específicos. ((WENCZENOVICZ; BAEZ, 2016, p. 104).

Por último, não se pode esquecer que a privacidade é um direito da personalidade da pessoa humana, que no direito brasileiro estaria inserido dentro dos direitos fundamentais, já que "os direitos da personalidade são os reconhecidos à pessoa humana considerada em si mesma e em suas projeções na sociedade. São inerentes à condição humana, por isso, declarados estão na Constituição." (DINIZ, 2017, p. 09).

Sobre o que foi supracitado, cabe demonstrar o seguinte comentário, que relaciona o direito à privacidade com o os direitos da personalidade:

> O ser humano, a par dos direitos patrimoniais e dos pessoais, tem direitos da personalidade, que são os direitos subjetivos, como diz Goffredo Telles Jr, da pessoa de defender o que lhe é próprio, ou seja, a identidade, a liberdade, a sociabilidade, a reputação, a honra, a imagem, a intimidade, a privacidade, a memória privada, a própria historia etc. Por outras palavras, os direitos da personalidade são direitos comuns da existência, porque são simples permissões dadas pela norma jurídica, a cada pessoa de defender um bem que a natureza lhe deu, de maneira direta e primordial. (DINIZ, 2017, p. 09).

Diante dos conceitos expostos fica clara a natureza do direito à privacidade, bem como a relação existente entre todas as classificações, uma vez que os direitos da personalidade da pessoa humana, estão inseridos no contexto dos direitos fundamentais, sendo esse último derivado dos direitos humanos.

A próxima questão a ser abordada é tentar conceituar o que seria este direito, sendo uma tarefa relativamente complicada, considerando todas as divergências existentes na doutrina, nunca tendo sido estabelecido um conceito que fosse aceito por todos, sem haver questionamentos.

Dessa forma, passam a surgir problemas no direito brasileiro diante desta indefinição deste conceito, de acordo com Marcel Leonardi (2011, p.47):

> A falta de clareza a respeito do que é privacidade cria complicações para definir políticas públicas e para resolver casos práticos, pois se torna muito complexo enunciar os danos ocorridos em uma situação fática, podendo dificultar ou mesmo inviabilizar sua tutela, principalmente diante da necessidade de seu sopesamento em face de interesses conflitantes, tais como a liberdade de manifestação de pensamento, a segurança pública e a eficiência de transações comerciais. A experiência de alguns países demonstra esse problema.

A dificuldade se dá em face de que não foi utilizada de forma expressa pelo legislador na Constituição Federal de 1988 a palavra privacidade, o que deixa várias dúvidas e aberturas no seu conceito, levando em conta que este seria o direito que nomeadamente envolve o direito à intimidade, à vida privada, honra e imagem, conforme consta na Carta Magna de nosso país, todavia, não apresenta nenhuma definição precisa, na lei, para o que seria cada um deles.

Diante dessa dificuldade em definir com precisão o que seria a privacidade, vem à tona a colocação de Vinicius Borges Fortes (2017, n.p.):

> Assim, a privacidade passou a ser considerada uma 'virtude extremamente escorregadia', intangível, sobre a qual é difícil estabelecer uma definição e eventuais mensurações. Significa dizer que um 'direito à privacidade' não é e não pode ser um estatuto imutável. Para diferentes pessoas possui

> sentidos diferentes em espaços de tempo diversos e está diretamente ligado com o que se compreende por anonimato.

Com a exposição dos problemas para definir um conceito para o objeto em estudo, é necessário apresentar, ao menos, um conceito para propiciar o melhor entendimento do assunto em tela, mesmo que, como já dito antes, nenhuma conceituação que venha a ser apresentada, consegue abranger toda a ideia de privacidade, sendo aceita por toda a doutrina, ou que ainda, não deixe margem para dúvidas. Entretanto, Celso Ribeiro Bastos (1997, p. 30), conceitua o direito à privacidade da seguinte maneira:

> [...]a faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhe o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano.

Diante dessa dificuldade da doutrina para conseguir definir o que é o direito à privacidade, é interessante demonstrar o pensamento de Leonardi (2011, p. 48) sobre essa questão:

> A doutrina pondera que é difícil de definir a privacidade, porque é "irritantemente vaga e evanescente" e que o fato mais surpreendente sobre o direito à privacidade é que "ninguém parece ter uma ideia clara do que ele é". Argumenta-se, ainda, que a palavra privacidade, tal como liberdade, "possui um sentido emotivo e ao mesmo tempo tão vago que, ainda que utilizada pelo ordenamento, não está ela definida, daí os problemas que se colocam na análise do assunto", e que "o inciso X do art. 5º chega a proclamar como invioláveis a 'intimidade' e a 'vida privada', mas não adianta qualquer elemento que possa conduzir a uma delimitação segura do direito elementar do indivíduo à privacidade".

É importante comentar que o direito à privacidade engloba três áreas diversas da vida do ser humano, na forma em que é aplicada atualmente, sendo que a necessidade dessa aplicação acaba por definir certas normas sociais, que precisam ser observadas por todas as sociedades, uma vez que é um direito inerente a qualquer cidadão, em qualquer época. Essa divisão deste direito é explicada por Vinícius Borges Fortes (2016, p. 103):

> Com efeito, a necessidade de privacidade individual ou em grupo, resultando em normas sociais, está virtualmente presente em todas as sociedades. Em uma gama de atividades, essas necessidades afetam basicamente três áreas da vida do ser humano: a privacidade individual, a intimidade do grupo familiar, a comunidade como um todo. As normas de privacidade para a sociedade são estabelecidas em cada uma dessas três áreas. Na primeira área, o indivíduo busca privacidade assim como busca companhia em suas interações diárias com outros indivíduos. Os limites são definidos para manter algum grau de distância em momentos cruciais da vida. No ambiente familiar, também são instituídas normas para os membros da família e do ambiente externo, de modo a proteger as atividades dentro do lar. Na terceira área, cerimônias e rituais significativos na sociedade são protegidos por regras de privacidade de cada grupo.

Apesar de toda a exposição realizada até o momento, é notório que vivemos numa sociedade em constante mutação, assim, precisa o direito também estar se adaptando aos fatos novos que venham a surgir dessas mudanças, mas considerando que nosso direito é baseado nas leis escritas em códigos, e que a maioria deles podem ser considerados desatualizados,

inclusive a Constituição Federal, que foi publicada no longínquo ano de 1988, e sabemos, que em 30 anos houveram várias mudanças na situação fática de nossa sociedade.

A situação descrita acima explica perfeitamente o grande problema do objeto principal desta pesquisa, que é a relação entre a jurisdição e a transferência de dados, também é um problema que passou a surgir nos últimos anos, devido a grande popularização da internet e as várias finalidades que passaram a ser utilizadas através dela, sendo que estas ocorrências não estão abrigadas pela legislação brasileira, diante da contemporaneidade destes fatos. Existe a ressalva quanto ao Marco Civil da Internet (Lei nº 12.965/2014), que tentou estabelecer algumas normas sobre fatos semelhantes.

2. PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Com o objetivo de estabelecer a relação com tudo que foi abordado no capítulo anterior e com o que será escrito na sequência, convém trazer o apontamento realizado por Danilo Doneda (2006, p. 139):

> Ao derivarmos a proteção de dados pessoais diretamente da privacidade, podemos sustentar que a tutela da privacidade abrange a proteção de dados pessoais. Tal operação, se basta para abarcar a disciplina sob a égide constitucional, arrisca simplificar os fundamentos da tutela de dados pessoais e eventualmente limitar o seu alcance.

Inicialmente, para ser possível a compreensão sobre as questões referentes à proteção de dados na internet, é importante ser analisada sob uma perspectiva sobre a proteção de dados de uma maneira geral, conforme consta na Constituição Federal de 1988, para após, contextualizar com a realidade atual que estamos vivendo, a realidade do mundo em que a internet é o maior meio de comunicação, de trabalho, entretenimento ou até de espionagem existente. Vinícius Borges Fortes comenta sobre essa questão:

> Em um contexto anterior à difusão da internet como meio para a disseminação da informação e da comunicação, a norma constitucional brasileira, ao contrário do que outras constituições realizaram, não reconhece expressamente a proteção da privacidade em relação aos bancos de dados informáticos. De acordo com Limberger (2007), o instituto mais próximo dessa proteção específica é o *habeas data*, previsto no artigo 5º, inciso LXXII, da Constituição brasileira, regulamentado pela Lei 9.507/97. (FORTES, 2016, p. 109/110).

No entanto, ao analisar a citação acima, e a aplicação do *habeas data*, se percebe que a amplitude de alcance do direito concedido por ele é muito restrita, considerando que sua aplicação é para a obtenção de informações existente em banco de dados públicos ou de órgãos governamentais, podendo haver a retificação em casa de algum problema verificado, todavia, não podendo ser utilizado em face de instituições privadas. (DONEDA, 2009).

Cabe, ainda, referir sobre o que se pode entender do que sejam as informações pessoais que venham a merecer qualquer tipo de proteção do ordenamento brasileiro, não somente as cobertas pelo habeas data, mas sim toda a informação relevante para a identidade de alguma pessoa, sobre isso, Danilo Doneda (2011, p. 93) diz:

> A informação pessoal, aqui tratada, deve observar certos requisitos para sua caracterização. Determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa

> que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras. É importante estabelecer esse vínculo objetivo, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre esta pessoa, por exemplo, a princípio não possuem esse vínculo objeto; também a produção intelectual de uma pessoa, em si considerada, não é per se informação pessoal (embora o fato de sua autoria o seja).

Sobre a relação existente entre o direito à privacidade e as informações pessoais, é possível afirmar que estão intrinsicamente ligadas "por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa." (DONEDA, 2011, p.94). Esta constatação não consegue delimitar perfeitamente tudo que engloba essa relação, entretanto, é um bom ponto de partida para entender como as informações pessoais passaram a ser tuteladas pelo ordenamento brasileiro, como uma derivação do direito à privacidade, que foi explicado no capítulo anterior, ficando clara a importância do que foi lá exposto.

Para evitar confusões, convém estabelecer a diferença entre os conceitos de informação e de dados, sendo que em vários casos, são utilizados no mesmo sentido e conotação, mas possuem pequenas diferenças, conforme Doneda (2011), o dado seria a informação em estado potencial, antes de ela ser transmitida, seria uma espécie de pré-informação, que ocorre antes do processo de interpretação e elaboração da informação.

Um dos grandes problemas envolvendo a obtenção de dados pessoais de maneira indevida, é colocada por Boff e Fortes (2014, p. 116), explicando que:

> Não bastassem os acontecimentos envolvendo a violação de privacidade e a publicação deliberada desses dados, a atual geração tecnológica tem como grande elemento catalizador das empresas de tecnologia da informação e comunicação a violação e a comercialização de dados pessoais.

Algumas medidas foram tomadas ao longo do tempo pelo direito brasileiro com o intuito de proteger os dados pessoais de seus cidadãos, foram a equiparação dos registros de dados de consumidores de qualquer gênero às entidades de caráter público, por meio da Lei nº 8.070/90, que institui o Código de Defesa do Consumidor, que além disso, tornou expressa a proteção do acesso do consumidor à informações e dados seus, existentes em cadastros, fichas registros pessoais e de consumo, sendo, ainda, garantida a obrigatoriedade da comunicação, por escrito, ao consumidor de qualquer abertura de novo cadastro ou armazenamento de dados pessoais sem sua solicitação. (FORTES, 2016).

Ainda, no direito processual penal, é possível dizer que a lei que trata a tutela das comunicações telefônicas (Lei nº 9.296/96) se a aproxima das da informática, mas não menciona sobre a transmissão de dados pessoais por meio da internet. (FORTES, 2016).

Outro ponto que vale ser destacado, é a Lei Complementar nº 105/2001, que estabeleceu:

> [...] no ordenamento jurídico brasileiro, dispositivos que conferem tratamento específico para o sigilo sobre operações de instituições financeiras. De acordo com a norma, informações bancárias como depósitos de valores, pagamentos, aplicação em fundos de investimento, operações em

> moeda estrangeira e operações com cartão de crédito estão no bojo das operações que devem estar sob sigilo, guardadas as exceções previstas na referida lei. (FORTES, 2016, p. 112).

Por fim, vale a menção ao Código Civil Brasileiro, que aborda sobre os direitos de personalidade, questão já debatida no capítulo anterior deste estudo. Cabe menção novamente, ao Marco Civil da Internet, que estabeleceu algumas regras sobre a privacidade de informações pessoais na rede, entretanto, antes de tratar especificamente sobre a lei que o instituiu, é relevante fazer mais alguns apontamentos sobre como chegamos ao estágio atual no debate da proteção de dados. Interessante trazer à tela a seguinte reflexão:

> Destaca-se que foi com o advento do computador pessoal que se possibilitou o armazenamento e avaliação de dados relativos à vida pessoal dos indivíduos sem a necessidade de existência de um complexo programa apropriado para tal propósito. Alguns setores sociais perceberam nisso quão útil poderia ser coletar e armazenar, para posterior uso ou divulgação, dados pessoais de terceiros. (RUARO; RODRIGUEZ, 2010, p. 183).

Com relação à questão supracitada, colocam que até certo momento da história da sociedade brasileira a proteção jurídica que existia para a privacidade era suficiente, entretanto, com a popularização da informática, a quantidade de dados armazenados na rede aumentou exponencialmente, sendo armazenados uma quantidade praticamente ilimitadas de dados das mais diversas naturezas, "os quais circulam entre Estados, particulares e empresas privadas, muitas vezes sem qualquer tipo de controle". (RUARO; RODRIGUEZ, 2010, p. 183)

Sobre esses novos fatos que passaram a surgir, devido a informatização de nossa sociedade, é relevante expor a ideia em sequência:

> Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais. Para uma completa apreciação do problema, estes interesses devem ser considerados pelo operador do direito pelo que representam, e não somente pelo seu traço visível – a violação da privacidade. (DONEDA, 2011, p. 95).

No contexto atual em que a nossa sociedade está inserida, onde a internet é uma das principais ferramentas que a norteiam, o ordenamento jurídico brasileiro recepcionou algumas normas, e entende que esse ambiente virtual era merecedor de reconhecimento normativo, diante da relevância que passou a ter.

As medidas que foram adotadas nesse sentido foram a instituição da Lei de Acesso à Informação (Lei nº 12.527/2011), a Lei de Crimes Informáticos (Lei nº. 12.737/2012) e como grande destaque, a instituição do Marco Civil da Internet (Lei nº. 12.965/2014), em consonância com Vinicius Borges Fortes (2016). Mais recentemente, se destaca a criação da Lei nº 13.709 de 2018, que trata especificamente sobre a proteção de dados pessoais, a qual foi sancionada pelo Presidente da República, Michel Temer, em 14 de agosto de 2018.

Com foco na aplicação da Lei do Acesso à Informação, sucintamente, é possível explicá-la da seguinte maneira:

> A Lei de Acesso à Informação determina que o tratamento das informações pessoais detidas por entidades e instituições nela abrangidas seja realizado de modo transparente, respeitando o direito fundamental à proteção da intimidade, da vida privada, da honra e da imagem das pessoas, o

> que, nos fundamentos defendidos nesta obra, corresponde à proteção do direito fundamental à privacidade. A lei impõe restrições substanciais de acesso a informações pessoais, como o acesso restrito às informações, pelo prazo máximo de cem anos, a agentes públicos autorizados, bem como a possibilidade de acesso ou divulgação a terceiros, mediante prévio consentimento do titular das informações, exceto nos casos previstos no regulamento. (FORTES, 2016, p. 118).

Com relação a Lei de Crimes Informáticos, que foi popularmente chamada de Lei Carolina Dieckman, pelo motivo de que no ano da promulgação da lei a atriz teve várias fotos íntimas divulgadas na internet, obtidas através de invasão de aparelhos eletrônicos pessoais da atriz, de acordo com notícia veiculada no site do Tribunal de Justiça de Mato Grosso, sendo essa uma das situações que evidenciou a necessidade de uma tipificação penal específica para esse tipo de crime, o que foi feito com a criação da Lei 12.737/2012, que inseriu no Código Penal o artigo 154-A, disciplinando esta matéria, sendo o seu teor:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 2012).

Já, o Marco Civil da Internet foi a tentativa de criar uma lei que abrangesse a maior quantidade possível de situações que pudessem ocorrer no âmbito da internet. E com a sua criação foi tentando positivar grande parte dos direitos que os cidadãos necessitam ter nessa sociedade informatizada em que já se encontra nosso país.

> O "Marco Civil da Internet" no Brasil, como se sabe, é a Lei que regula o uso da Internet no Brasil, por meio da previsão de princípios e estabelecimento de garantias aos usuários. O texto trata de temas como neutralidade da rede, privacidade e retenção de dados, imponto obrigações para os provedores de serviços de internet. (TEIXEIRA, 2016, s.p.).

Durante todo o transcorrer do texto pertencente a Lei nº 12.965, de 23 de abril de 2014, são estabelecidas normas para regular o uso da internet no Brasil, sendo que há menção, há proteção dos dados pessoais em inúmeros de seus artigos. No art. 3º da referida lei, expressamente define a proteção de dados como um dos seus princípios, no inciso III, bem como o direito à privacidade, no inciso II, que estão diretamente ligados, como já explicado no capítulo inicial deste estudo. (BRASIL, 2014).

Outros apontamentos sobre a proteção de dados pessoais existente nessa lei são citados por Fortes (2016), como por exemplo, limitando a finalidade dos usos dos dados pessoais para o motivo em que foram coletados, não podendo ser utilizados de forma diversa, sem o expresso consentimento do seu titular, devendo estar especificadas no contrato de prestação de serviços ou em termos de uso de aplicações de internet.

Ainda, no decorrer da obra do autor supracitado, ele aborda quanto à inviolabilidade dos dados pessoais, afirmando que, observando a garantia do direito fundamental à privacidade, que inclusive consta na nossa Constituição Federal, questão já tratada antecedentemente:

> [...] o Marco Civil determina que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas devem atender

> à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas." (FORTES, 2016, p. 128/129).

Por fim, no Marco Civil, se encontra certa ênfase na tutela da proteção de dados pessoais na internet, definindo que é necessário o consentimento expresso do seu titular para qualquer que seja o uso destinado a eles, devendo ser claras e completas todas as informações referentes a aplicação que serão destinados, bem como devem ser restritos a finalidade para que foram coletados, desde que não sejam vedadas pela legislação e que precisam estar especificadas no contrato de prestação de serviços ou em termos de uso de aplicações de internet. (BRASIL, 2014).

Por último, não há como não falar sobre a lei nº 13.709, de 14 de agosto de 2018, que versa sobre a proteção de dados pessoais. Para melhor compreensão da mesma, vale apresentar o texto do seu artigo 1º, que a define de forma geral a sua aplicação com o seguinte texto:

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

No texto desta nova lei, é abordada de forma muito mais complexa a proteção aos dados pessoais, estabelecendo algumas novas ideias, normas, conceitos e, abrangendo de uma forma muito mais ampla do que o Marco Civil da Internet, que tratava anteriormente sobre essa matéria.

Com a sanção do Presidente da República, a lei passa a tutelar praticamente qualquer operação de tratamento e utilização de dados em nosso país, garantindo uma segurança muito maior do que a existente no atual cenário do ordenamento brasileiro. Ela disciplina a forma como os dados são coletados e tratados, com maior enfoque nos meios digitais, como por exemplo, dados cadastrais ou até mesmo textos ou fotos publicadas em redes sociais.

Uma das inovações que se apresenta, é que estão protegidos tanto os dados pessoais que possibilitam uma pessoa a ser identificada ou que permita que ela seja identificável. No caso, a lei regula, também, os dados que, isolados, não demonstram quem seria o seu titular, como o endereço, mas em conjunto com outros dados poderia estabelecer a identificação da pessoa, indicando quem seria o titular destes dados, por exemplo, a combinação do endereço com a idade.

Outra novidade interessante são os chamados dados "sensíveis", que seriam os registros de raça, opiniões políticas, crenças, condição de saúde e características genéticas, que podem ser obtidos na rede, além de que foram estabelecidas regras específicas para informações e uso de dados, envolvendo crianças. (BRASIL, 2018).

Todas as normas estabelecidas por esta lei devem ser aplicadas nas operações de tratamento de dados realizadas no Brasil, bem como com relação a qualquer coleta de dados realizadas no país, ficando empresas estrangeiras que operam no país, também, sujeitas a esta legislação, mesmo que o tratamento dos dados seja feita em território estrangeiro, inclusive, devendo o país de destino dos dados, nível parecido de proteção com o desta lei ou que a empresa responsável pelos dados, garanta proteção compatível por meio de contratos ou de normas corporativas. (BRASIL, 2018).

Todavia, é importante mencionar que apesar da sanção, o Presidente da República, Michel Temer, vetou parcialmente a lei em análise, sendo o maior destaque o veto a criação de um órgão responsável sobre essa matéria, no caso, vetou a criação da Autoridade Nacional de

Proteção de Dados (ANPD), bem como apresentou o veto para a instituição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que seria um dos órgãos integrantes da ANPD, sendo informada oficialmente a seguinte justificativa para este ato: "Os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição." (BRASIL, 2018).

O primeiro ponto a se prestar atenção, é que a Autoridade Nacional de Proteção de Dados, seria uma autarquia da administração pública indireta, ou seja, atuaria como uma agência reguladora da proteção de dados no nosso país. Assim, de forma resumida, ao alegar esses dois artigos, o Presidente da República afirmou que em consonância com a Constituição Federal em vigência no Brasil, cabe somente ao Presidente da República a criação de órgãos da administração pública, seja os diretos ou indiretos, de acordo com o inciso II do parágrafo 1º do artigo 61. Com relação ao inciso XIX do artigo 37 da Carta Magna, o mesmo dispõe que as autarquias devem ser criadas por meio de lei específica destinada apenas para esta finalidade, não devendo ser instituída por uma lei que disciplina outras matérias. (BRASIL, 1988).

Apesar do veto, fica claro que o poder legislativo já percebeu a importância da criação de uma agência reguladora para a proteção de dados na internet, todavia, conforme afirmado pelo próprio chefe do poder executivo de nossa nação, cabe a ele dar a iniciativa com o devido trâmite constitucional para que venha a se tornar realidade essa medida.

Essa questão de transferências de dados, na esfera internacional, será abordada no último capítulo desta pesquisa, através de uma abordagem mais específica, que será realizada sobre a jurisdição dos dados pessoais que incumbe tanto ao nosso país quanto aos estrangeiros, e quais os limites de atuação nesse âmbito, bem como sobre a jurisdição responsável, em caso de conflitos.

Para compreender o que foi exposto no parágrafo acima, diante da utilização de termos técnicos, convém apresentar o conceito que é encontrado no próprio projeto de lei sobre o que seria o tratamento de dados, com o objetivo de evitar que fiquem pontos obscuros e facilitar o entendimento da explicação realizada anteriormente:

> Art. 5º Para os fins desta Lei, considera-se:
>
> X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

O tratamento para fins pessoais, artísticos e jornalísticos ficaram de fora da abrangência estipulada pelo projeto de lei, em consonância com seu art. 4º, inclusive, sendo a mesma situação em questões de atividades de segurança nacional, segurança pública e repressão à infrações, existindo indicação no texto de que, tais circunstâncias, devem ser tuteladas por meio de lei própria, havendo ainda, a possibilidade de que o poder público possa tratar dados sem o consentimento do titular em determinadas ocasiões, devendo informar, em seu site, sobre essa atuação. (BRASIL, 2018).

Como última reflexão sobre esse projeto de lei analisado, fica o questionamento se serão mesmo colocadas em práticas todas as normas estabelecidas nesta lei e como será realizada a fiscalização com relação ao seu cumprimento. Neste trabalho, foi retratada, de uma maneira rasa e superficial o Projeto de Lei nº 53, do Senado Federal, uma vez que não é o principal objeto de estudo, entretanto, tem grande relevância em todas as temáticas aqui desenvolvidas.

Vários pontos importantes propostos por esse projeto, não foram discutidos no decorrer do texto, diante da enorme quantidade de conteúdo e normas constantes nele, Foram tratadas sobre as questões relevantes para o estudo em tela, sendo que no futuro, em caso de sanção, esta lei merecerá uma atenção especial do mundo acadêmico do direito brasileiro, considerando que ela surgiu para resolver algumas das maiores indagações, dificuldades e problemáticas existentes na relação entre o judiciário, o direito e a internet, que foi objeto de estudo de inúmeros pesquisadores da área jurídica, com o surgimento da sociedade informatizada.

3. JURISDIÇÃO DE DADOS PESSOAIS NA INTERNET

O presente estudo visa abordar algumas questões com relação a jurisdição de dados pessoais na internet tanto na esfera nacional, quanto na internacional, dessa forma, é imprescindível termos em mente um conceito mais geral do que é jurisdição, como o apresentado no parágrafo anterior, para depois realizar uma análise mais precisa na esfera digital.

Giuseppe Chiovenda (2000, p.03), define a jurisdição como sendo:

> [...] função do Estado que tem por escopo a atuação da vontade concreta da lei por meio da substituição, pela atividade de órgãos públicos, da atividade de particulares ou de outros órgãos públicos, já no afirmar a existência da vontade da lei, já no torná-la, praticamente, efetiva.

A dificuldade em se estabelecer qual é a jurisdição responsável por um caso no mundo digital surge no momento em que alguns dos princípios já estabelecidos para o conceito de jurisdição pela doutrina e legislação brasileira acabam não sendo suficientes para abranger as novas demandas que advém do mundo digital.

Talvez, o princípio que mais pode ser contestado ao analisar a capacidade para a jurisdição de demandas relacionadas a temas digitais seria o princípio da aderência ao território ou também conhecido como princípio da territorialidade, que se utiliza das fronteiras físicas para definir o órgão responsável pelos conflitos.

> O princípio da aderência ao território diz respeito a uma forma de limitação do exercício legítimo da jurisdição. O juiz devidamente investido de jurisdição só pode exercê-la dentro do território nacional, como consequência da limitação da soberania do Estado brasileiro ao seu próprio território. Significa dizer que todo juiz terá jurisdição em todo o território nacional. Ocorre, entretanto, que, por uma questão de funcionalidade, considerando-se o elevado número de juízes e a colossal extensão do território nacional, normas jurídicas limitam o exercício legítimo da jurisdição a um determinado território. (NEVES, 2016, n.p.).

A partir desse problema que surge com o princípio da territorialidade, Lucas Borges de Carvalho (2018, p. 218-219), apresenta as ideias de David Johnson e David Post (1996, p. 1369-1374), no artigo *Law and borders – the rise of law in cyberspace* da seguinte maneira:

> Essa arquitetura tradicional da soberania é posta em xeque pela natureza transfronteiriça da internet. As fronteiras se diluem e os limites territoriais não mais coincidem com o âmbito de aplicação da lei. Ou, ainda, não mais se apresentam como um critério funcional para delimitar a extensão das competências jurisdicionais. De outro lado, há uma desconexão entre os efeitos das ações humanas e a localização territorial. Basta pensar que,

> em princípio, um blog ou um simples comentário em uma rede social podem ser vistos por qualquer pessoa conectada à internet, independentemente de onde esteja situada. Diante de tais transformações, seria infrutífera qualquer tentativa de regular o ciberespaço com base nos preceitos tradicionais da soberania e da jurisdição nacional. Além da diluição das fronteiras, a ineficácia decorreria do expressivo volume das comunicações eletrônicas, das tecnologias que permitem desrespeitar as ordens estatais e, por fim, do potencial conflito entre as diversas leis e jurisdições nacionais.

Em consonância com Carvalho (2018, p. 219), a melhor solução para a definição da jurisdição dos conflitos virtuais, seria reconhecer o ciberespaço como um local distinto do mundo físico que norteia o "direito comum", devendo ser dividido por "fronteiras virtuais", constituídas por telas e senhas. No caso, o acesso à internet passaria a ter efeitos jurídicos iguais a ação de cruzar a fronteira de um país, passando assim a iniciar a vigência da lei do ciberespaço. Com essa análise, o autor anteriormente mencionado, nos apresenta outra conclusão:

> Portanto, de acordo com a concepção liberal, a lei do ciberespaço seria mais legítima (visto que fundada no consentimento dos usuários e na liberdade individual) e mais eficaz (já que as suas normas seriam mais apropriadas para a resolução de conflitos virtuais) do que a jurisdição estatal. Por essa razão, os Estados deveriam adotar um princípio de autolimitação em qualquer processo de exercício da soberania ou de aplicação de leis locais no ambiente digital. (CARVALHO, 2018, p. 219).

Todavia, sabemos que não é dessa forma que se encontra o cenário atual da internet, seja no Brasil ou em qualquer outra nação. A definição da jurisdição de demandas virtuais é um problema realmente presente no cotidiano da sociedade que vivemos, estando longe de um consenso mundial.

Numa abordagem mais específica sobre a proteção de dados pessoais na internet, verificamos a existência de duas legislações no cenário brasileiro que tratam desse tema, que seriam o Marco Civil da Internet, que já se encontra há um bom tempo em vigência no ordenamento brasileiro, e mais recentemente houve a aprovação da lei 13.709, que trata especificamente da proteção de dados pessoais. Antes, porém, vale a menção do seguinte comentário de Vinícius Borges Fortes (2016, p. 129):

> Há outro ponto que representa evolução normativa para a tutela de direitos na internet e que responde, parcialmente, os frequentes questionamentos sobre a eficácia normativa de uma lei nacional, quanto estão em xeque a soberania dos Estados e as características transnacional da rede. Ele diz respeito à determinação de que, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, devem ser obrigatoriamente respeitado a legislação brasileiras e os direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e dos registros, considerando que pelo menos um dos terminais esteja localizado no Brasil, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior.

Os dois pontos que se tentará esclarecer, é a questão quanto à transferência de dados internacionais, assunto que já foi debatido de uma forma superficial no decorrer desta

pesquisa, e também, quanto a responsabilidade da jurisdição de conflitos em que o objeto é a proteção de dados, tanto no âmbito internacional, entre diversas nações, quanto no âmbito nacional, com relação aos Estados brasileiros.

No primeiro instante, será tratado sobre a jurisdição internacional de dados. Conforme já dito, o Marco Civil da Internet, é um dos dispositivos infraconstitucionais vigentes, que busca regular a proteção de dados virtuais em nosso ordenamento, inclusive, estabelecendo normas específicas quanto a transferência internacional dos mesmos, no texto do seu art. 11, que já teve seu conteúdo resumido no capítulo 2, deste trabalho, quando tratado especificamente sobre Lei nº 12.965/14.

A lei supramencionada estabelece a imperatividade das leis brasileiras sobre qualquer dado que em qualquer fase inicial de seu tratamento ou de sua operação tenha sido realizada no Brasil, havendo algumas exceções já demonstradas. Visando sempre a proteção da privacidade, dos dados pessoais e o sigilo das comunicações privadas, em concordância com as garantias dadas pela Constituição do nosso país, estabelecendo assim, a relação entre o conteúdo do primeiro capítulo e o presente.

A grande inspiração para a criação do Marco Civil da Internet no Brasil, foi o Regulamento nº 2016/679, de 27 de abril de 2016, da União Europeia, que entrou em vigor no mês de maio do ano de 2018. Estabeleceu inúmeras regras para a transferência de dados dos países membros do bloco econômico para terceiros, e também estabeleceu diretrizes para o monitoramento desses dados, além de várias outras normas.

A lei nº 13.709, em seu artigo 33, deixou ainda mais claro quais são as possibilidades em que é possível a transferência internacional de dados de forma licita, sendo interessante apresentar seu inteiro teor:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
>
> a) cláusulas contratuais específicas para determinada transferência;
>
> b) cláusulas-padrão contratuais;
>
> c) normas corporativas globais;
>
> d) selos, certificados e códigos de conduta regularmente emitidos;
>
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
>
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> V - quando a autoridade nacional autorizar a transferência;

> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
>
> VII - 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 desta Lei;
>
> VIII - 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; ou
>
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. (BRASIL, 2018).

No entanto, o maior problema que surge dessa relação entre transferência internacional de dados e o direito, não está apreciada de forma clara e precisa nem em nosso ordenamento já positivado, também, não havendo, em nenhuma outra nação especificações precisas, nem um consenso internacional para a definição da jurisdição responsável sobre conflitos e demandas relativas ao assunto aqui debatido, ou seja a proteção dos dados pessoais na internet.

A fim de elucidar o objeto em estudo, é possível apresentar uma situação hipotética: imaginando que um americano, por meio de um computador ligado à internet no território do Canadá, tenha acesso a informações pessoais e sigilosas de um argentino que apenas utiliza a internet no Brasil, qual seria o Estado responsável para julgar eventuais demandas penais e cíveis surgidas desta relação?

Apesar de confusa e peculiar, podem vir a ocorrer situações parecidas com o do exemplo acima, e esta pesquisa pretende esclarecer alguns pontos obscuros na definição da jurisdição deste tipo de relação, bem como apresentar propostas para facilitar a resolução destes conflitos.

Esse é um tema pouco analisado tanto pelos legisladores, quanto pelos doutrinadores e, inclusive, pelos pesquisadores da área jurídica, perante a situação ser um fato relativamente novo e havendo, ainda, um atraso do direito brasileiro sobre outros pontos referentes à internet que, em tese, são muito mais simples.

Dessa forma, coube a uma organização realizar estudos e análises sobre essa temática, que seria o Instituto de Referência em Internet e Sociedade, que realizou um profundo estudo sobre a proteção dos dados pessoais no Brasil, além de analisar expressamente o problema da jurisdição internacional de transferência de dados, sendo esse estudo realizado por esse Instituto, uma das principias referências para a produção desta pesquisa.

É evidente que os princípios aplicáveis comumente para definir a jurisdição das demandas em nosso país, não são suficientes para definir se é ele ou a outra parte da relação que é o responsável pela resolução do conflito, os princípios da soberania, territorialidade, nacionalidade e vários outros aplicáveis aos casos mais comuns, não são suficientes para redimir a dúvida quanto à jurisdição.

Assim, com o objetivo de apresentar propostas para a solução dessa dificuldade, o estudo do Instituto de Referência em Internet e Sociedade traz algumas suposições baseadas em ideias já existente dentro do direito internacional, para tentar manter o mínimo de segurança sobre a jurisdição internacional de dados. São elas: o pejorativamente denominado Fórum Shopping, e a criação de um direito internacional para a internet.

Sobre a primeira sugestão, ela pode ser assim entendida:

> Forum Shopping é a prática de direta ou indiretamente escolher o tribunal ou jurisdição que lhe parece mais favorável para dirimir um eventual litígio. Essa escolha é geralmente feita após análise de uma série de fatores que, sopesados, indicam ao demandante uma maior probabilidade de sucesso em sua reivindicação. Esses fatores podem variar de menores custos de litígio a normas processuais, substantivas ou jurisprudenciais mais favoráveis ao pedido. A expressão forum shopping é, frequentemente, utilizada de forma pejorativa, mas ela inegavelmente expressa uma estratégia de ação no contenciosos internacional privado. (INSTITUTO, 2018).

Quanto a proposta da criação de um direito internacional para a internet, já sabemos que apesar de ser a proposta ideal na teoria, é quase impossível de ser colocada em prática. Praticamente não existem chances de chegar há um consenso que agrade todos os países, inclusive porque em determinadas regiões do nosso planeta, a internet não é tão popularizada (nos países considerados pobres), da mesma forma que é nos países de primeiro mundo e nos em desenvolvimento, e para que funcionasse essa sugestão, muitos governantes teriam que abrir mão da autonomia que possuem ou de interesses que tenham sobre a regulação da internet, em prol do bem comum de todas as nações.

Já não é uma tarefa fácil estabelecer uma legislação em apenas um Estado, vide o exemplo do Brasil, que até os dias atuais, ainda não possui uma legislação abrangente e indubitável sobre a internet, numa esfera global, criar normas para a internet parece algo ainda mais surreal, tanto para definir normas gerais, quando sobre regras de jurisdição de transferência de dados bem como de demandas relacionadas à internet.

> É sabido que estabelecer uma forma de controle na internet é algo muito difícil. Alguns acreditam que a internet é insuscetível de controle; outros entendem que a autodisciplina permitiria manter a liberdade da rede e, ao mesmo tempo, disciplinar toda forma de comportamento na internet por operadores e usuários; e há aqueles que entendem que, em todo o sistema jurídico, a segurança é um elemento essencial para que as relações intersubjetivas, inclusive aquelas com direcionamento meta-individual, permaneçam em níveis mínimos e aceitáveis de organização pelo meio social, porque a vida coletiva exige comportamentos pautados por normas comuns, que sirvam de critérios orientadores das atividades individuais, que direcionem cada indivíduo consoante previsão do que os outros poderão fazer, e, em caso de necessidade, lhe permitam exigir desses outros certos comportamentos. Perfilhando esta última corrente, Fabio Podestá se posiciona – corretamente, a meu ver - no que concerne a regulamentação da internet. (GUERRA, 2006, p. 06).

Na visão do autor deste trabalho, uma alternativa viável seria tentar começar estabelecer as normas gerais de internet bem como de jurisdição por meio de tratados internacionais com a maioria de países que se dispunham a participar, inicialmente, sendo dada preferência para o estabelecimento de regras entre os países que existe um maior fluxo de dados e importância nesse novo modelo de sociedade que o Brasil está vivendo, fazendo algo parecido com o que foi realizado pela União Europeia, todavia, por já se tratar de um bloco econômico estabelecido com várias características em comum, era uma tarefa muito mais fácil do que iniciar uma relação do nada.

Possivelmente, seria necessária uma iniciativa dos Estados Unidos da América como precursor dessa ideia, tendo em mente, que possui grande parte das empresas que se utilizam

dos dados como mercadorias, e da grande parte dos provedores existentes na internet serem provenientes de lá, porém, diante do conhecido posicionamento deste país, em situações deste gênero, as chances de tentar fazer um tratado que favoreça seus interesses, passando a controlar quase que exclusivamente o fluxo de dados da rede, é enorme.

Existe a ressalva que já foram tentadas alternativas parecidas da acima exposta, como por exemplo, a tentativa de um acordo de cooperação internacional entre o Brasil e os Estados Unidos, que não possui a mesma força de um tratado e sua efetividade não possui garantias.

Outro ponto relevante colocado pela pesquisa do Instituto de Referência em Internet e Sociedade, é sobre os chamados "paraísos jurisdicionais", países onde a legislação sobre crimes cibernéticos e negócios na internet, tende a ser mais branda e flexível, passam a ser utilizados para as operações da maioria das empresas, que em outros territórios seriam ilegais, constituindo crimes.

De forma resumida, é possível colocar que a jurisdição sobre um crime de transferência de dados internacionais, depende do crime praticado, bem como dos países envolvidos, dependendo da legislação de cada um e se há existência de acordos de cooperação entre eles, entre outros meios.

Após essa análise em uma esfera internacional, não pode ser deixado de lado o que está ao nosso redor, ou seja, analisar aspectos da jurisdição dos Estados da República Federativa do Brasil, sobre o objeto desta pesquisa.

Essa discussão em nosso ordenamento ainda é um tanto quanto obscura, ficando, muitas vezes, sujeita a interpretação dos órgãos do Poder Judiciário, considerando que não é um ponto abrigado com clareza pela legislação existente, além de serem situações relativamente novas, onde muitos dos magistrados de nosso país, não estão preparados para lidar com isso.

O estudo do Instituto de Referência em Internet e Sociedade fala sobre alguns conflitos de competências existentes em nosso ordenamento, que podem ser utilizados como base para termos alguma ideia de como são procedidas as definições de competência e jurisdição das demandas desta espécie:

> No Brasil, o Superior Tribunal de Justiça (STJ) também reúne algumas decisões que merecem destaque. No Conflito de Competência no. 66981, ao analisar aspectos da jurisdição para processar parte acusada de veicular imagens pornográficas de crianças e adolescentes na internet, o Tribunal decidiu que é competente o foro do local onde ocorreu o lançamento, na internet, das fotografias de conteúdo pornográfico. Indicou-se também que é irrelevante, para fins de fixação da competência pelo tribunal, o local da sede da empresa provedora de acesso à internet. (INSTITUTO, 2018).

É apresentado também o Conflito de Competência nº. 107938, em que o Superior Tribunal de Justiça definiu:

> [...] que a competência para processar e julgar os crimes praticados pela internet, dentre os quais se incluem aqueles provenientes de publicação de textos de cunho racista em sites de relacionamento, é do local de onde são enviadas as mensagens discriminatórias. (INSTITUTO, 2018).

O Superior Tribunal de Justiça também definiu que quando a matéria da demanda for sobre reportagens jornalísticas, notícias e afins, será aplicada a mesma regra que é aplicada para a divulgação de material impresso, ou seja, a jurisdição será no local onde a vítima vive e que os efeitos causados pelo conteúdo divulgado, causarão mais prejuízos para a sua imagem.

Foram expostas algumas peculiaridades sobre o objeto principal desta pesquisa, não sendo possível aprofundar cada ponto do tema tratado, doravante sua complexidade, abrangência, mutação, e divergências existentes, ainda mais que não há legislação específica no Brasil, além de existirem várias interpretações no STJ e demais tribunais do nosso Poder Judiciário.

Nos crimes cibernéticos mais comuns, sem tantas características que o diferenciem, a tendência é que seja observado o disposto no Código de Processo Penal Brasileiro para os crimes em geral, enquadrando o fato conforme necessário para seu correto processamento. Para ilustrar isso, um crime de furto de dados bancários de um computador, em concordância com o Código Processo Penal Brasileiro, deve ser processado no local em que o agente ativo do crime o praticou, em tese, no entanto, podendo haver exceções, sempre observado o disposto nos códigos em situações análogas, uma vez que nem todos os crimes existentes no mundo virtual estão tipificados, e obviamente, as questões cíveis devem, inicialmente obedecer ao estabelecido no Código de Processo Civil.

Por fim, transcreve-se abaixo o art. 69 do Código de Processo Penal e o art. 53 do Código de Processo Civil, com o intuito de deixar um caminho para a interpretação do presente estudo, sendo que estes artigos são os que devem ser observados no primeiro instante, para definir a competência em nosso território, não sendo totalmente perfectibilizado seu uso no caso concreto, diante das características peculiares de cada demanda, dessa maneira, é sabido que não é fácil aplicação destas normas, como já foi colocado no decorrer da pesquisa. Assim, o teor do artigo referente à competência jurisdicional na esfera criminal. em nosso ordenamento é:

> Art. 69. Determinará a competência jurisdicional:
>
> I - o lugar da infração;
>
> II - o domicílio ou residência do réu;
>
> III - a natureza da infração;
>
> IV - a distribuição;
>
> V - a conexão ou continência;
>
> VI - a prevenção;
>
> VII - a prerrogativa de função. (BRASIL, 2018).

Na esfera cível, não se encontra colocada a competência jurisdicional de uma forma tão simplificada, diante da variedade de ações e direitos que podem ser pleiteados, mas nos incisos III e IV do art. 53 do CPC, é possível tentar estabelecer de qual tribunal será a competência de eventual direito postulado, em consonância com a presente pesquisa:

> Art. 53. É competente o foro:
>
> [...]III - do lugar:
>
> a) onde está a sede, para a ação em que for ré pessoa jurídica;
>
> b) onde se acha agência ou sucursal, quanto às obrigações que a pessoa jurídica contraiu;

> c) onde exerce suas atividades, para a ação em que for ré sociedade ou associação sem personalidade jurídica;
>
> d) onde a obrigação deve ser satisfeita, para a ação em que se lhe exigir o cumprimento;
>
> e) de residência do idoso, para a causa que verse sobre direito previsto no respectivo estatuto;
>
> f) da sede da serventia notarial ou de registro, para a ação de reparação de dano por ato praticado em razão do ofício;
>
> IV - do lugar do ato ou fato para a ação:
>
> a) de reparação de dano;
>
> b) em que for réu administrador ou gestor de negócios alheios; (BRASIL, 2018).

Fica ressalvado que existem, ainda inúmeras outras leis esparsas no nosso ordenamento, situações atípicas e interpretações diversas, que podem levar a que se distancie a competência dos tribunais, como está estabelecida nos artigos aqui citados.

Como uma reflexão sobre tudo que foi disposto neste capítulo, é perceptível que toda essa discussão buscou evidenciar a relação existente entre o direito humano fundamental à privacidade, com o acesso aos dados pessoais do cidadão brasileiro, e, em alguns momentos até, de qualquer outra pessoa deste mundo globalizado, e a dificuldade existente para definir a jurisdição responsável para resolver as demandas que surgem desta ligação.

A privacidade atingiu um patamar e uma mutabilidade que o direito brasileiro não estava preparado para lidar, passando a ter que resolver demandas que a legislação não estava preparada para redimir, no entanto, como está escrito na Constituição Federal de 1998, que embasa todas as demais normas de nosso ordenamento, ela deve ser sempre preservada, mesmo nesse novo prisma dos dados pessoais e da sociedade informatizada, bem como na resolução desses entendimentos inacabados como a jurisdição responsável por afrontas a esses dados, e nos demais que existem e que venham a surgir.

CONSIDERAÇÕES FINAIS

O ritmo de evolução da internet é muito mais elevado do que o do direito, todavia, o segundo precisa se adaptar às exigências que o primeiro lhe coloca. O Poder Judiciário não pode deixar de se pronunciar diante de uma demanda que lhe é apresentada, mas uma das indagações que podem vir a surgir diante de como nosso sistema é estabelecido, é: qual o tribunal responsável por cada um desses conflitos? Seja em relações internas, tanto como entre as realizadas entre pessoas de nações diversas.

Esta pesquisa tentou apresentar algumas dúvidas sobre essa dúvida e demonstrar o posicionamento adotado pelo nosso ordenamento. Para essa finalidade, foi necessário apresentar vários conceitos e entendimentos iniciais para possibilitar chegar a proposta final do estudo.

Não há como falar de como funciona a jurisdição de dados pessoais na internet sem explicar todo o contexto em que estão inseridos e sem estabelecer a sua relação com o direito

à privacidade, além de que, assegurar a melhor aplicação de um, diretamente influi na efetividade do outro.

Foram demonstrados os desafios, as dificuldades envolvendo o objeto desse estudo, e numa outra linha, também foi tentado apresentar algumas propostas e visões do autor da pesquisa, diante da falta de observação desse tema pelos doutrinadores e pesquisadores da área jurídica em nosso país.

A partir de todos os pontos levantados e analisados, entendemos que por mais utópica que seja essa proposta, a melhor forma de resolver os problemas em face da jurisdição internacional de dados pessoais, se daria com a criação de um direito internacional de proteção de dados, partindo-se da premissa de que a internet já trata-se de um bem global e que decisões de um país podem influir diretamente no outro, ou seus ordenamentos podem ser incompatíveis.

Considerando que o problema enunciado na Introdução foi respondido e os objetivos específicos foram atendidos e trabalhados da melhor forma possível durante o transcorrer do texto, sendo dessa forma alcançado o objetivo geral proposto no início do trabalho.

REFERÊNCIAS

ARAUJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. *Curso de Direito Constitucional*. 9. ed. São Paulo: Saraiva, 2005.

BASTOS, Celso Ribeiro. Tribunal Regional Federal da 1ª Região. *A Constituição na Visão dos Tribunais – Interpretação e Julgados- Artigo por Artigo*. vol. I. Brasília: Saraiva, 1997.

BOFF, Salete Oro; FORTES, Vinícius Borges. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. *Seqüência* (Florianópolis), n. 68, p. 109-127, jun. 2014. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/30375 Acesso em: 25 jul. 2018.

BRASIL. *Constituição Federal de 1988*. Brasília, DF, out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm. Acesso em: 21 jul. 2019.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. *Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras Providências*. Brasília, DF, nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 25 jul. 2018.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF, ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 ago. 2019.

BRASIL. *STJ - CC: 107938 RS 2009/0183264-2*, Relator: Ministro Jorge Mussi, Data de Julgamento: 27/10/2010. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=200901832642&dt_publicacao=08/11/2010. Acesso em: 17 ago. 2019.

CARVALHO, Lucas Borges de. Soberania digital: legitimidade e eficácia da aplicação da lei na internet. *Revista Brasileira de Direito*, Passo Fundo, vol. 14, n. 2, p. 213-235, Maio-Agosto, 2018. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/2183/1839. Acesso em: 17 ago. 2019.

CHIOVENDA, Giuseppe. *Instituições de Direito Processual Civil* – Vol. II. Campinas: Bookseller, 2000.

DINIZ, Maria Helena. Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido. *Revista Brasileira de Direito*, Passo Fundo, vol. 13, n. 2, p. 7-25, Mai.-Ago. 2017. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/1670/1185. Acesso em: 12 jul. 2018.

DONEDA, Danilo. A proteção de dados pessoais no ordenamento brasileiro e a ação de Habeas Data. *Revista Democracia Digital e Governo Eletrônico*, v.1, n.1. 2009. Disponível em:http://buscalegis.ufsc.br/revistas/index.php/observatoriodoegov/article/view/12297/30655. Acesso em: 24 jul. 2018

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Joaçaba*, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315. Acesso em: 23 jul. 2018.

DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

FORTES, Vinícius Borges. *Convergências conceituais para os direitos de privacidade na internet e a proteção dos dados pessoais.* In: PIRES, C.; PAFFARINI, J.; CELLA, J.R.. (Org.). Direito, democracia e sustentabilidade: Programa de Pós-Graduação Stricto Sensu em Direito da Faculdade Meridional. 1ed. Erechim: Deviant, 2017, v. 1, p. 269-288.

FORTES, Vinícius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet*. Editora Lumen Juris, Rio de Janeiro, 2016.

GUERRA, Sidney. A internet e os desafios para o direito internacional. *Revista eletrônica da Faculdade de Direito de Campos*, Campos dos Goytacazes, RJ, v. 1, n. 1, nov. 2006. Disponível em: http://bdjur.stj.jus.br//dspace/handle/2011/18803. Acesso em 23 jul. 2018.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. *Jurisdição e internet Competência Internacional dos Tribunais Domésticos e Litígios de Internet.* Disponível em: http://irisbh.com.br/wp-content/uploads/2018/02/Jurisdicao-e-internet-Compet%C3%AAncia-Internacional-de-Tribunais-Estatais-e-Lit%C3%ADgios-de-Internet.pdf

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. *Policy Paper Transferência Internacional de Dados no PL 5276/16.* Disponível em: http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Portugues.pdf Acesso em: 25 jul. 2018.

LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2011.

NEVES, Daniel Amorim Assumpção. *Manual de direito processual civil* – Volume único – 8. ed. – Salvador: Ed. JusPodivm, 2016.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. *Direito, Estado e Sociedade*, n.36, p. 178 a 199, jan/jun, 2010. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/o_direito_a_protecao_de_dados_pessoais_na.pdf Acesso em: 22 jul. 2018.

TEIXEIRA, Tarcisio. *Marco Civil da Internet.* São Paulo: Leya. 2016. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=JwADDAAAQBAJ&oi=fnd&pg=PT3&dq=marco+civil+da+internet&ots=_xY0ZiKLa-&sig=yf1qus8zuPSXloLX-2A2LHi3wSQ#v=onepage&q&f=false Acesso em: 22 jul. 2018.

WENCZENOVICZ, Thaís Janaina; BAEZ, Narciso Leandro Xavier. Direitos fundamentais, educação indígena e identidade emancipatória: reflexões acerca de ações afirmativas no Brasil. *Revista Brasileira de Direito*, 12(2): 95-107, jul.-dez., 2016. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/1271 Acesso em: 25 jul. 2018.

BIBLIOGRAFIA

BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. *Código de Processo Penal*. Brasília, DF, out. 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm. Acesso em: 25 jul. 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Brasília, DF, abril 2014.Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 jul. 2018.

BRASIL. Lei nº 13.105, de 16 de março de 2015. *Código de Processo Civil*. Brasília, DF, mar. 2015.

Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 25 jul. 2018.

SENADO FEDERAL. *Projeto de lei nº 53*. Iniciativa: Deputado Federal Milton Monti (PR/SP). Disponível em: https://legis.senado.leg.br/sdleggetter/documento?dm=7738646&disposition=inline Acesso em: 20 jul. 2018.

TRIBUNAL DE JUSTIÇA DO MATO GROSSO. *Lei de crimes virtuais já está em vigor.* Publicada em 05.04.2013. Disponível em: http://www.tjmt.jus.br/noticias/29323#.W1CSv9JKjIU Acesso em: 25 jul. 2018.

ABSTRACT

With a popularization of the internet, several new devices were introduced in the protection of the law, however, some of the new occurrences were not treated with the attention they deserve. The jurisdiction requires that the protection of data on the Internet is one of the aspects that improve the analysis, both in its national and international form. The purpose of this data set is a specific law institution on the jurisdiction of data transfer for the protection of the right to privacy. And the main conclusion that was reached was to transcend text that could improve the creation of an international data protection file. The method used in this research is monographic and a research technique is bibliographical.

KEYWORDS

Internet; international right; dices protection.