UNIVERSIDADE DO SUL DE SANTA CATARINA

FERNANDA CARRARO FIDELLIS STASCZAK

E-COMMERCE E PROTEÇÃO DE DADOS PESSOAIS
Análise jurídico-legal sobre os Fundamentos da Responsabilidade

Florianópolis

2023

FERNANDA CARRARO FIDELLIS STASCZAK

E-COMMERCE E PROTEÇÃO DE DADOS PESSOAIS
Análise jurídico-legal sobre os Fundamentos da Responsabilidade

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Profª Fátima Kamel Abed Deif Allah Mustafa, Espec.

Florianópolis

2023

FERNANDA CARRARO FIDELLIS STASCZAK

E-COMMERCE E PROTEÇÃO DE DADOS PESSOAIS
Análise jurídico-legal sobre os Fundamentos da Responsabilidade

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Direito e aprovado em sua forma final pelo Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina.

Florianópolis, dezembro de 2023.

_____
Professora e orientadora Fátima Kamel Abed Deif Allah Mustafa, Espec.
Universidade do Sul de Santa Catarina

_____
Professor Vilson Leonel, Msc
Universidade do Sul de Santa Catarina

Às minhas irmãs Jakeline e Rafaelly por estarem ao meu lado nesses anos todos, pela parceria e cumplicidade.

AGRADECIMENTOS

Aos meus amigos Luciano, Ricardo e Rodrigo por serem minha segunda família em Florianópolis e por todos os anos que passamos juntos.

“Trocava toda a minha tecnologia por uma tarde com Sócrates.” (Steve Jobs)

RESUMO

Este trabalho científico, visado através de uma metodologia de revisão narrativa, busca apresentar uma análise jurídico-doutrinária quanto à questão da responsabilidade civil frente às práticas de e-commerce que são realizadas no Brasil, com devido respaldo territorial ou aplicabilidade na lei brasileira. Neste sentido, buscou-se convalidar direitos da personalidade, como a privacidade e intimidade e também a dignidade da pessoa humana e estabelecer as diretrizes e o arcabouço jurídico que convalida a aplicação de responsabilidade civil. Enquanto metodologia, optou-se pelo uso de jurisprudências e acórdãos relacionados com a área a fim de resultar em maior fundamento jurisprudencial da área realizando uma discussão e análise com doutrina, buscando, com tal entendimento, entender quais são as características da responsabilidade, e os limites em que o Estado pode (e deve atuar). Durante o projeto, assim, foi constituída a caracterização dos e-commerces, o seu desenvolvimento ao longo do tempo – dentro do espaço brasileiro – e as denotações de dados, proteção de dados e tecnologias de informação e compartilhamento, que trazem respaldo técnico para atuação dos e-commerces no Brasil. Além disto, também se destrinchou a Lei Geral de Proteção de Dados e o Marco Civil da Internet, que são componentes jurídicos fundamentais para aplicação de responsabilidade frente ao Código de Defesa do Consumidor e também o Código Civil Brasileiro. Com base nestas pesquisas, possibilitou-se entender que, além da Responsabilidade Civil Contratual, tácita de aplicabilidade sob as relações de consumo no cenário eletrônico, a Responsabilidade Civil Extracontratual é também uma ferramenta tutela pelo direito brasileiro, especialmente sobre os direitos de personalidade como a intimidade, privacidade e dignidade da pessoa humana, estando as relações de consumo firmadas a partir do território brasileiro e/ou com qualquer componente técnico (celular, tablet, aparelho eletrônico) aqui usados, sempre que estabelecidos a autoria significativa, o nexo casual e o dano efetivo da prática realizada. Assim, pode-se entender e concluir que há arcabouço jurídico-doutrinário e legal na aplicabilidade de responsabilidade frente ao caso de compartilhamento, vazamento e alteração de informações e dado pessoas por instituições e-commerces (e de demais instituições) no Brasil, respeitados os limites estabelecidos pela figura deste instituto no direito brasileiro.

Palavras-chave: Direito Digital. Direito de Personalidade. LGDP.

ABSTRACT

This scientific work, aimed at using a narrative review methodology, seeks to present a legal and doctrinal analysis on the issue of civil liability in the face of e-commerce practices that are carried out in Brazil, with due territorial support or applicability in the Brazilian law. In this sense, an attempt was made to validate personality rights, such as privacy and intimacy, as well as the dignity of the human person, and to establish guidelines and the legal framework that validates the application of civil liability. As a method, we opted for the use of jurisprudence and judgments related to the area in order to result in a greater jurisprudential basis in the area, carrying out a discussion and analysis with doctrine, seeking, with such understanding, to understand what the characteristics of responsibility, and the limits within which the State can (and should act). Thus, during the project, the characterization of e-commerces, their development over time – within the Brazilian space – and the denotations of data, data protection and information and sharing technologies, which bring technical support for the performance of e-commerces in Brazil. In addition, the General Data Protection Law and the Marco Civil da Internet were also broken down, which are fundamental legal components for the application of responsibility against the Consumer Defense Code and also the Brazilian Civil Code. Based on these researches, it was possible to understand that, in addition to Contractual Civil Liability, tacitly applicable under consumer relations in the electronic scenario, Extra-contractual Civil Liability is also a tool under Brazilian law, especially regarding personality rights such as intimacy, privacy and dignity of the human person, with consumer relations established from the Brazilian territory and/or with any technical component (mobile phone, tablet, electronic device) used here, whenever the significant authorship, the casual link and the effective damage of the practice performed are established. Thus, it can be understood and concluded that there is a legal, doctrinal and legal framework in the applicability of liability in the case of sharing, leaking and changing information and personal data by e-commerce institutions (and other institutions) in Brazil, respecting the limits established by the figure of this institute in Brazilian law.

Keywords: Digital Law. Personality Right. LGDP.

SUMÁRIO

1 INTRODUÇÃO

A influência contextual de maior importância para muitos sistemas de informação (TIC) e, por consequência, para o comércio eletrônico e seus investimentos é a lei. Por exemplo, a lei fornece base que certamente se relaciona com design, implementação, uso de sistemas de informação e relações que baseiam as transações e negócios jurídicos que ocorrem nos principais meios eletrônicos (FINKELSTEIN, 2004).

Logo, em teoria, assim como um arquiteto que não projetaria um edifício para desabar, um projetista ou empreendedor, de sistemas e comercio eletrônico, não iria, intencionalmente, projetar negócios com possíveis falhas, levando danos e/ou lesões a pessoas e/ou organizações. Todavia, em prática, ainda se notam sistemas desenvolvimento (eletrônicos) resultando em danos/lesões que são levados, atualmente – às vistas dos marcos legais da internet –, ao conhecimento da lei – que busca amenizar os seus problemas de desenvolvimento e, inclusive, dentro do direito do consumidor (PAESANI, 2006).

Desta forma, o direito contratual é conhecido como uma influência importante nos assuntos relacionados aos sistemas de informação/e-commerce, remontando pelo menos aos anos 1950 (PAESANI, 2006), afinal, a negligência por parte de empreendedores tem sido um problema de anos com relevância em ações judiciais de responsabilidade, pela ausência de caracterização ou tipificação de condutas, ausência de clareza legal e, principalmente, discricionariedade impostada ao mundo virtual.

Com base nisto, este projeto científico busca, sobretudo, realizar uma parametrização legal-doutrinária e jurisprudencial acerca dos normativos que ceram o comércio eletrônico no país, focando em apresentar os fundamentos de responsabilidade civil frente ao direito fundamental da privacidade/intimidade e o rompimento de sigilo de dados retirados de um negócio jurídico eletrônico – seja por fraude ou por reconhecimento e trocas comerciais entre diferentes empresas.

Logo, sua estrutura é fundamentada em sete capítulos que incluem, respectivamente, a introdução, aqui mencionada, que apresenta as justificativas do estudo e seus objetivos geral e específicos; e-commerce, que traz uma convalidação de informações sobre os negócios jurídicos ocorridos neste âmbito, além de sua caracterização histórica e legal; relações de consumo, que apresenta a vertente estudada sobre a ótima do direito do consumidor; dados pessoais, que faz um levantamento sobre e LGPD (Lei 13.709/2018) e conceitos

constitucionais/legais sob o tema; responsabilidade, que discuti a aplicação desta para as condutas; análise comparativa, que realiza uma discussão e conclusão, que o projeto aqui impetrado.

2 E-COMMERCE

Enquanto conceito, o comércio eletrônico se trata de um negócio em que a Tecnologia da Informação e Comunicação (TIC) é usada para aumentar as vendas, eficiência empresarial e também para fornecer uma base para novos produtos e serviços, onde, por meio de suas atividades, cada empresa se comunica com muitas outras entidades, podendo ser estas clientes privados ou corporativos, parceiros de negócios, fornecedores e quaisquer indivíduos diretamente envolvidos com a produção, comercialização e/ou extinção de um ou mais produtos ou serviços que são oferecidos (ALBERTIN, 2004).

Assim sendo, pode-se entender, em conceituação básica, que o comércio eletrônico é o exercício da atividade comercial por meio de ferramentas eletrônicas, fundamentado no processamento eletrônico e na transmissão de informações (texto, vídeo, áudio); que, por consequência, envolve este em diversas atividades empresariais, desde comércio eletrônico de bens e serviços, entrega eletrônica de informações digitais, leilões eletrônicos, marketing direto aos consumidores e realização de serviços à distância (REEDY; SCHULLO, 2017).

Encontrado, este, amplo nos campos de comércio varejista eletrônico; transações financeiras nas prestações de serviços bancários, locação financeira, seguros e outros serviços, investimentos, operações especulativas em moeda e títulos dentro dos valores mobiliários e de capitais, câmbio de curto, médio e longo prazo; mercados de serviços – hotéis, turismo coletivo e individual, educação, consultoria, pagamento por utilitários, publicidade e outros; entre várias empresas, públicas, privadas e outras instituições mistas – como os bancos e instituições financeiras de tal caráter, pessoas físicas e jurídicas ou consórcios, famílias e indivíduos, dentre outros (REEDY; SCHULLO, 2017).

Os conceitos específicos, todavia, apresentam-se diferentes sobre o termo. Ao passo que Khan (2016) subscreve que o comércio eletrônico, ou e-commerce, é a compra e venda de bens e serviços na Internet, e que além de comprar e vender, muitas pessoas usam a Internet como fonte de informação para comparar preços ou veja os produtos mais recentes em oferta antes de fazer uma compra online ou em uma loja tradicional, Nakamura (2001) entende que o comércio eletrônico, comumente conhecido como e-commerce, é toda relação de negócio direta ou indireta de produtos e/ou serviços que usam redes de computadores, como a internet, baseada em tecnologias como o comércio móvel, transferência eletrônica de fundos, gerenciamento da cadeia de suprimentos, internet marketing, processamento de transações

online, intercâmbio eletrônico de dados (EDI), sistemas de gerenciamento de estoque e coleta automatizada de dados e sistemas (NAKARUMA, 2001).

Isto é, para o primeiro, o conceito de e-commerce propriamente dito se aprofunda dentro da atividade fim, ou seja, da realização própria de um negócio jurídico, da venda, da compra, do fechamento de contrato. Já para o segundo, a subjetividade entra no campo do conceito, pois o e-commerce se fundamenta desde as atividades acessórias, administrativas, de segurança e de organização, não somente na atividade fim que é a concretização do negócio, mas no pré-atendimento, na auditoria de processos eletrônico, no controle e segurança operativa, no gerenciamento e marketing e em quaisquer atividades que sejam suficientemente necessárias para que as transações fins ocorram.

O conceito do último é levado em consideração científica nesta análise, haja vista que a proteção de dados implica na subjetividade do e-commerce, isto é, nas atividades administrativo-gerenciais que respaldam os contratos jurídicos realizados durante um processo de venda eletrônica e não somente nas atividades fins – que dão origem aos negócios jurídico comerciais que são levantados na celebração de vendas.

Com base nesta conceitualização, a próxima subseção traz um aparto histórico-empírico do desenvolvimento de negócios e contratos à luz do comércio, avaliando as caracterizações da história do e-commerce internacional e, principalmente, no Brasil, convalidando seu desenvolvimento nos últimos anos no país.

2.1 EVOLUÇÃO HISTÓRICA: TICS, E-COMMERCE E SEGURANÇA DA INFORMAÇÃO

A história do comércio eletrônico pode ser rastreada até a década de 1960 com o desenvolvimento do Intercâmbio Eletrônico de Dados. Ele substituiu o correio e o fax, pois possibilitava a troca de dados por meio de transferências digitais, sem a necessidade de intervenção humana, popularizando-se rapidamente durante períodos de guerras menores e/ou em instituições que necessitavam ampla comunicação (TIAN; STEWART, 2016)

Os parceiros comerciais podiam transmitir pedidos, faturas e outras informações usando um formato que atendesse ao Comitê de Padrões Credenciado X12 do American National Standards Institute, o conjunto de padrões da América do Norte. As informações eram examinadas posteriormente por uma Rede de Valor Agregado (RVA) e, em seguida,

direcionadas ao sistema de processamento de pedidos do destinatário (TIAN; STEWART, 2016). Para muitos doutrinadores como Tian; Stewart (2016) e Nakaruma (2001) este foi o marco inicial do comércio eletrônico global, da transação de informações de negócios em eletrônica, pela sua caracterização de conduta à longa distância.

Todavia, outros, como Khan (2016), afirmam que a primeira ocorrência registrada de uma transação online foi em 1972, onde alunos de Stanford supostamente venderam cannabis para alunos do MIT por meio de uma conta da Arpanet ou Advanced Research Projects Agency Network, uma rede de comutação de pacotes que implementou o pacote de protocolos TCP/IP e é conhecido como o precursor da Internet. Aqui, então, cabe compreender que a definição de início depende do conceito de atrelado pelos autores: os que consideram o e-commerce a partir do seu objetivo fim desprender o início de suas atividades em 1972, os demais, a partir de 1960, com as primeiras utilizações entre nações.

Não muito depois disso, em 1979, um inventor inglês recebeu o crédito pelo desenvolvimento do conceito de compras online. Michael Aldrich tinha acabado de terminar suas compras no supermercado com sua esposa quando teve a ideia de ligar a televisão deles ao supermercado para entregar as compras. Aldrich, então, conectou uma TV a um computador de processamento de transações usando uma linha telefônica, dando origem ao que ele chamou de televenda, ou compras à distância. Este sistema de televendas foi comercializado um ano depois como um sistema B2B, embora nenhuma evidência mostrasse que ele tenha sido usado para o varejo (TIAN; STEWART, 2016). Neste período, a popularização das vendas ganhou destaque no mercado internacional – inclusive no Brasil.

Finalmente, em 1990, Tim Lee e Robert Cailliau construíram um projeto de hipertexto chamado WorldWideWeb. Lee usou o computador NeXT para criar o primeiro servidor web, bem como escrever o primeiro navegador web. Em 1991, a web estreou como um serviço disponível ao público na Internet. Ele então casou o hipertexto com a Internet e desenvolveu a URL, HTML e HTTP (TIAN; STEWART, 2016). Nessa época, o mundo viu as primeiras compras online seguras (TURBAN et al., 2009).

Em 1992, um dos primeiros sites de comércio eletrônico, Book Stacks Unlimited, foi inaugurado por Charles M. Stack. Tornou-se Books.com em 1994 e, eventualmente, tornou-se parte da Barnes & Noble. Em 1997, a Dell se tornou a primeira empresa a ter um recorde de vendas online de US$ 1 milhão (TURBAN et al., 2009). Foi também nessa época que o certificado de criptografia Secure Socket Layers (SSL) foi desenvolvido.

O protocolo de segurança feito pela Netscape proporcionou melhor segurança para transmissão de dados pela Internet. O navegador da web primeiro verifica se há um certificado SSL autêntico em um site para saber se deve confiar nele ou não. E isso veio na esteira das hesitações e preocupações dos clientes com as compras online. Hoje, o protocolo de criptografia SSL é um padrão para a maioria dos servidores da web, o que o torna uma parte vital da segurança da web (TURBAN et al., 2009).

Neste ponto, não havia como parar o e-commerce, especialmente com avanços significativos em tecnologia chegando, que aumentam as seguranças previstas na coleta e transformação de informações repassadas dos clientes para as, poucas até então, empresas que realizam vendas por atividade a distância. Neste sentido, em 1995, dois sites colocaram as compras online no mapa para sempre, estabilizando desejo dos consumidores: a Amazon.com e o Ebay.com (TURBAN et al., 2009; TIAN; STEWART, 2016)

A primeira, talvez o varejista online mais proeminente hoje, começou como uma livraria online e ofereceu mais títulos em comparação com seus concorrentes offline. Em 2001, lançaram seu primeiro site para celulares smartphones. Hoje, a empresa atrai mais de 65 milhões de clientes mensalmente, e o mundo viu a eficiência das páginas de categoria de comércio eletrônico surgiu com a Amazon, mas, mais importante, foram a avaliação do usuário e a escala de avaliação que definiram o sucesso da empresa. Esse recurso ajudou compradores indecisos a ter uma ideia de seu produto preferido de clientes existentes.

O eBay foi lançado no mesmo ano que a Amazon (1995). Embora também permitisse compras online, é principalmente famoso por apresentar leilões online. Esses dois sites abriram caminho para Zappos e Victoria's Secret entrarem nas compras online em 1999. Enquanto isso, 1995 viu-se o início dos mecanismos de busca começando com o Yahoo!, e depois o Google em 1998. Ambos agora têm subsidiárias de comércio eletrônico, respectivamente, Google Shopping e Yahoo! Leilão – que mostra o foco crescente no e-commerce como canal de receita (TURBAN et al., 2009).

Em 1998, o PayPal tornou o comércio eletrônico global possível como um banco adquirido que faz o processamento de pagamentos para vendedores online, sites de leilão e usuários comerciais. Os clientes podem enviar, receber e reter fundos em 24 moedas diferentes. Hoje, as transações do PayPal têm uma taxa de conversão de checkout 79% maior em comparação com as que não são do PayPal (KARR, 2016). Do período para frente, o setor de comércio eletrônico passou a movimentar milhares milhões por ano.

Como consequência, segurança adicional para transações online foi aplicada com a criação do Conselho de Padrões de Segurança da Indústria de Cartões de Pagamento em 2004 para todas as operadoras do globo. O conselho foi encarregado de garantir que as empresas cumpram os requisitos de segurança. Eles também estabeleceram, melhoraram, armazenaram, divulgaram e implementaram padrões de segurança para proteção de dados de contas, aumentando as vendas em nível internacional, inclusive no Brasil, onde, a partir de 2001, mais de 0.5 (meio) bilhão de reais eram faturados anualmente com o comércio eletrônico – mesmo com a baixa popularidade da internet (TOREZANI, 2008).

Conforme mencionado previamente, a melhoria contínua da tecnologia abriu caminho para um melhor e-commerce e, em 2003, mais de 20% dos americanos tinham Internet banda larga em suas casas ou acesso à Internet mais rápido e sempre ativo em comparação ao dial-up (TIAN; STEWART, 2016). Como consequência, com conexões de alta velocidade à disposição, houve aumento de acesso às lojas online: o comércio eletrônico começava a despontar como a macroeconomia global que se tornaria em 2015.

Os resultados vieram a partir de 2010, principalmente com a disseminação das TICs em todo o mundo. Assim, a última década viu o domínio do e-commerce, não apenas devido à melhor tecnologia, mas também ao aumento do interesse e da participação do consumidor. Em 2018, a China faturou cerca de US$ 900 bilhões em vendas, enquanto os EUA faturaram mais de US$ 423 bilhões. Já no Brasil, em 2019, o e-commerce faturou R$61,9 bilhões, 16,3% acima de 2018 (ECOMMERCE BR, 2020).

Todos estes resultados, sobretudo, foram pautados a partir da necessidade de maior segurança e políticas de privacidade definidas por comitês éticos internacionais, que respaldou os contratos eletrônicos realizados nas relações de consumo. Neste sentido, as próximas duas subseções findam as observações temáticas acerca do e-commerce analisando tanto tais políticas quanto as relações jurídicas dos e-contratos.

2.2 PRIVACIDADE E POLÍTICAS DE E-COMMERCE

Muitas disciplinas diferentes examinaram o tópico da privacidade e usaram várias definições de privacidade, tornando difícil relacionar um estudo a outro para suas múltiplas definições. No entanto, um tema central de um século de discussões sobre privacidade é o

direito de uma pessoa exercer controle sobre suas informações pessoais, isto é, de requerer tutela frente ao Estado de dados puramente individuais. (TEIXEIRA, 2001).

A definição mais antiga, frequentemente citada, é: “um direito de ser deixado em paz” (WARREN; BRANDEIS, 1890). Todavia, num aspecto próprio de direito, entende-se a privacidade como "a reivindicação de indivíduos, grupos ou instituições para determinar por si próprios quando, como e em que medida as informações sobre eles são comunicadas para outros” (FINKELSTEIN, 2011, p. 83). Assim sendo, esta não passa, em base, às luzes constitucionais de 1988, do fundamento pétreo da dignidade humana, ou seja, de manter as relações mínimas que produzem ao indivíduo uma vida sustentável, sem conflitos espirituais, tácitos, físicos e de nível coletivo com seus outros iguais.

Por consequência, sua aplicabilidade vai desde a doutrinária básica até especialidades como o Direito Eletrônico. Neste sentido, tendo em vista que este estudo enfoca na privacidade do contexto e-commerce, faz-se importante a contextualização nesta área temática. Assim, ao que tange ao e-commerce, a privacidade é ligada diretamente com a segurança da informação e transferência de comunicação falha, isto é, a invasão de privacidade, que é comumente vista como coleta, uso e transferência não autorizada de dados pessoais e informações como resultado direto destas transações (TEIXEIRA, 2001), ferindo-se princípios éticos-sociais.

Fundamentalmente, tem-se a seguinte definição ao Direito Digital: privacidade da internet é o direito dos indivíduos de controlar suas informações pessoais com relação à sua coleta, uso e transferência pela internet, indiferente de quais relações que este possua com quaisquer membros que nesta existam (TEIXEIRA, 2001). À luz doutrinária, Ferraz Júnior (1993) estabelece que para o ordenamento jurídico:

> O sujeito é o titular deste direito (...) é toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira, residente (ou transeunte) no País (art. 5º, caput). O conteúdo é a faculdade específica atribuída ao sujeito, que pode ser a faculdade de constranger os outros ou de resistir-lhes (caso dos direitos pessoais) ou de dispor, gozar, usufruir (caso dos direitos reais). A privacidade, como direito, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para

> si, ao abrigo de sua única e discricionária decisão. O objeto é o bem protegido, que pode ser uma res (uma coisa, não necessariamente física, no caso de direitos reais) ou um interesse (no caso dos direitos pessoais). No direito à privacidade, o objeto é, sinteticamente, a integridade moral do sujeito (FERRAZ JÚNIOR, 1993, p. 440)

Já a Constituição Federal de 1988, no seu artigo 5º, afirma que: "X - 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), respaldando o fundamento de que a privacidade é um controle da dignidade humana, no que tange ao processamento e divulgação de informação. Deste modo, é possível perceber que a privacidade, à luz doutrinário-legal do direito em comércio eletrônico, respalda-se pela segurança da informação e comunicação, ou seja, pela não violação da propriedade individual.

Este entendimento doutrinário-legal também apresenta base jurisprudencial, que reafirma as ligações da privacidade com a relação íntima e inviolável da pessoa. E ainda sobre o aspecto característico, amplia suas aplicações e responsabilidades para o meio externos, quando de condutas fora do território brasileiro. Este entendimento – sob ponto de vida do e-commerce – é visto no RE Nº 1.745.657 - SP (2018/0062504-5):

> RECURSO ESPECIAL. INTERNET. JURISDIÇÃO. SOBERANIA DIGITAL. PREQUESTIONAMENTO. AUSÊNCIA. MARCO CIVIL DA INTERNET. APLICAÇÃO DA LEGISLAÇÃO. Um dos maiores desafios postos hoje à regulação da internet reside na compatibilização entre sua natureza transfronteiriça e o exercício da soberania digital pelos Estados, com óbvias implicações para o exercício da jurisdição estatal. Não se trata de um debate apenas teórico, uma vez que abrangidos conflitos de ordem prática, cuja resolução e desdobramentos podem ter grande impacto no desenvolvimento da internet, em temas que variam de proteção de direitos e dados online à preservação de suas características fundamentais, tais como a abertura, a universalidade e descentralização. Como bem descrito por Lucas Borges de Carvalho, é um grande desafio garantir a legitimidade e a efetividade das decisões judiciais em um mundo altamente conectado. VIII. De forma, geral, regulação de condutas em ambiente digital pode ser efetuada de duas formas centrais: (i) com base no uso da tecnologia e conforme parâmetros fixados em normas internas dos provedores de serviço; ou (ii) pela regulação estatal. Desde o começo, este debate está dividido entre defensores desses dois modelos, que podemos denominar, respectivamente, de liberais e realistas. No entanto, ambas as correntes tratam de maneira simplista a

> questão da legitimidade da regulação sobre a internet e, a fortiori, das decisões judiciais que envolvam assuntos digitais, pois ignoram as complexidades existentes no tema. Tanto visão liberal quanto realista falham ao captar os detalhes da discussão, pois é impossível adotar um determinismo tecnológico cego tampouco transplantar à força ao mundo digital as regras existentes do direito nacional. Diante desse cenário, a doutrina argumenta que, em conflitos transfronteiriços de privacidade na internet, a autoridade responsável deve atuar de forma "prudente, cautelosa e autorrestritiva, reconhecendo que a territorialidade da jurisdição permanece sendo a regra, cuja exceção somente pode ser admitida quando atendidos, cumulativamente, os seguintes critérios: (i) fortes razões jurídicas de mérito, baseadas no direito local e internacional; (ii) proporcionalidade entre a medida e o fim almejado; e (iii) observância dos procedimentos previstos nas leis locais e internacionais. Também se firmou o seguinte critério para estabelecer a jurisdição brasileira em controvérsias envolvendo a internet: quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil, aplicando-se à hipótese o disposto no artigo 88, III, do CPC. Especificamente sobre o mundo digital, afirmou-se a necessidade de afastar qualquer ideia da internet como um "porto seguro" ou "zona franca" contra a aplicação do direito estatal, na hipótese, do direito brasileiro: Não sendo assim, poder-se-ia colher a sensação incômoda de que a internet é um refúgio por meio da qual tudo seria permitido sem que daqueles atos adviessem responsabilidades. Contudo, com desenvolvimento da tecnologia passamos a ter um novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, ou seja, o consentimento do interessado é o ponto de referência de todo o sistema de tutela da privacidade. (STJ, RE Nº 1.745.657 – SP 2018/0062504-5, Min. NANCY ANDRIGHI, Julgado 03/11/2020, Dje: 17/11/2020).

Neste sentido, a privacidade eletrônica é referida sobre duas atribuições à luz jurisprudencial: razoabilidade de aplicação – indiferente do território em que se fora auferida a conduta de ação e infringimento da proteção de dados e informações eletrônicas que, em base, estão em armazenamento em instituições presentes nos modelos de negócios digitais. Com isto, organizações grandes e pequenas usam sites de comércio eletrônico para alcançar clientes em potencial, buscando-se diferenciar por meio de relacionamentos aprimorados com estes, através das coletas de comportamento, navegação, preferências e gostos, o que enseja

diretamente na proteção de informações e dados eletrônicos pessoais – fruto da discussão aqui inferida, afinal, os limites jurídicos permitem quais tipificações de conduta.

A maneira mais fácil de coletar informações pessoais é durante um processo de registro ou pedido. Os clientes são solicitados a fornecer informações pessoais, como nome, endereço de e-mail e número do cartão de crédito (PAESANI, 2006). Outra abordagem é capturar endereços IP (Internet Protocol) dos clientes e usar esse IP endereço para rastrear as páginas da Web específicas que o cliente visualizou e a sequência da Web páginas que o cliente visitou (PAESANI, 2006). Já uma terceira abordagem é coletar informações pessoais dos clientes por meio do uso de um Cookie (PAESANI, 2006). Todas estas, irreversivelmente, implicam em notações jurídicas de privacidade e sigilo da informação (PAESANI, 2006; FINKELSTEIN, 2011; TEIXEIRA, 2001; KHAN, 2006).

Em geral, segundo Finkelstein (2011), o procedimento de acolhimento/armazenamento de dados eletrônicos é realizado a partir dos passos a seguir: preferências e informações comportamentais do cliente são rastreadas/armazenadas em sistemas de armazenamento eletrônico. Mais tarde, a empresa acessa o cookie para obter informações valiosas sobre estes e determina quais produtos ou serviços pode atribuir a este.

Logo, com o armazenamento massivo destas informações, uma parte dos indivíduos se tornou preocupado com o possíveis políticas internas das organizações ao passo que empresas podem “negociar ou compartilhar informações entre empresas terceirizadas sem conhecimento ou consentimento expresso do consumidor ou de outra forma a comprometer sua privacidade” (FINKELSTEIN, 2011, p. 37), como, por exemplo, por meio de segurança inadequada sobre a informação – falta de governança corporativa em Segurança de TI e eventual reprodução de procedimento fraudulento (FINKELSTEIN, 2011).

Três são as principais abordagens para lidar com as questões de privacidade na Internet, que são: regulamentação governamental, autorregulação do setor e tecnologias que aumentam a privacidade (Segurança em TI). Á primeira difundida em países como o Reino Unido, a Alemanha e, inclusive, o Brasil, que promulgaram legislação de privacidade que rege a coleta, uso e transferência de informações pessoais, bem como as transferências de tais informações para outros países que não adotaram legislação de proteção de privacidade semelhante (FILHO, 2015). Por outro lado, há alguns países, como os Estados Unidos, que adotaram regulação legal liberal do setor (FINKELSTEIN, 2011), com menor implicância aos fundamentos da privacidade e sigilo de informações.

Já diretamente sob a abordagem de autorregulação no e-commerce, cada empresa é responsável por decidir sobre o grau de informação que é coletada e usada e para desenvolver sua própria política de privacidade declaração alinhada com as diretrizes do setor. As agências governamentais só se envolvem em casos de flagrantes violações de privacidade (FINKELSTEIN, 2011). E quanto a terceira, esta depende de tecnologias como a Plataforma para Privacidade Preferências (P3P) e Anonymizer (www.anonymizer.com) para proteger a privacidade dos clientes, sendo a primeira um protocolo padronizado e legível por máquina, usado para implementar práticas de privacidade; e a segunda é um software de navegação em sites que permite aos indivíduos navegar na web páginas em total anonimato, de forma que suas informações pessoais não sejam disponibilizadas na web sites que eles estão navegando (FINKELSTEIN, 2011).

A relação entre princípio e direito à privacidade, assim, é horizontal dentro do ordenamento brasileiro, isto é, com o Marco Civil da Internet, fundamentou as mesmas práticas feitas no ambiente físico ao universo on-line. E estas relações, à luz do e-commerce, baseiam todas as realizações jurídicas dos contratos eletrônicos, que são analisados na próxima, e última, subseção desta temática, abaixo.

2.3 NEGÓCIOS E CONTRATOS ELETRÔNICOS

Uma vez que a Internet deixou de ser isolada apenas para comunicação ou computação e análise de dados, os contratos online estão agora na ordem do dia e não há diferenças jurídica, propriamente dita, no respaldo da relação comercial, entre os contratos online e offline. Portanto, os contratos online ainda são contratos e todas as regras dos contratos ainda serão aplicáveis (ALBERTIN, 2004).

Neste intento, cabe avaliar a celebração de negócios jurídicos que é prevista pelo Código Civil (2002) art. 107º, que estabelece: a validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir. Isto é, não existem naturezas específicas quanto à estrutura dos contratos realizados no âmbito brasileira, prevalecendo, sobretudo e legalmente, a formalização de três institutos básicos, previstos no art. 104º do mesmo diploma:

> Art. 104. A validade do negócio jurídico requer:
> I - Agente capaz;
> II - Objeto lícito, possível, determinado ou determinável;

> III - Forma prescrita ou não defesa em lei. (BRASIL, 2002).

Isto é, existindo um indivíduo, um objeto lícito e os ditames contratuais sendo os minimamente previstos em lei, há existência de um contrato jurídico, indiferente de seu meio de realização, que pode ser o eletrônico conforme a análise jurisprudencial do Apelação Cível nº 20120111804179 do Tribunal de Justiça do Distrito Federal e dos Territórios, que assimilou sob o conceito de contratos eletrônicos:

> DIREITO DO CONSUMIDOR. AÇÃO DE COBRANÇA. CONTRATO ELETRÔNICO. ALEGADA AUSÊNCIA DOS TERMOS DO CONTRATO DE ADESÃO. ÔNUS DA PROVA. INVERSÃO. POSSIBILIDADE TECNOLÓGICA DE COMPROVAÇÃO. CONFIGURADA. NÃO IMPLEMENTADA. TERMO GERAL DO CONTRATO DE MÚTUO. INEXISTÊNCIA. ELEMENTOS PROBANTES. AUSÊNCIA. DEVER DE REGISTRO DOS ATOS PRATICADOS. COMPROMISSO DE TRANSPARÊNCIA E DE INFORMAÇÃO. INCIDÊNCIA. CAPITALIZAÇÃO MENSAL DE JUROS. AUSÊNCIA DE PACTUAÇÃO EXPRESSA. VEDADA. SENTENÇA REFORMADA. MAJORAÇÃO DA SUCUMBÊNCIA. 2. O contrato eletrônico é de mesma espécie do contrato tradicional, não se tratando de uma nova modalidade de contratação, divergindo apenas em sua forma, pois possui os mesmos requisitos para a sua validade jurídica. 3. O documento digital deve atender aos requisitos de identificação, autenticação, impedimento de rejeição, verificação e integridade, privacidade e aos princípios da neutralidade e da perenidade das normas reguladoras do ambiente digital, conservação e aplicação das normas jurídicas existentes aos contratos eletrônicos, boa-fé objetiva e figura do iniciador [...] (BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Apelação Cível nº 20120111804179. Relator: Romeu Gonzaga Neiva. Brasília, 19 de julho de 2017, negrito da autora).

No mesmo sentido, Barreto (2009, p. 452) subscreve conceitualmente sobre os contratos eletrônicos que, em suma natureza, estes podem ser definidos em um primeiro momento como “uma expectativa normativa que as partes possuem, ou seja, em frente a situações conflituosas complexas e contingentes, ele se mantém, traduzindo vontades dos polos contratantes”. Assim, enquanto instituição, “para a elevação do grau de abstração, da elasticidade, da capacidade de adaptação e da possibilidade de diferenciação de expectativas comportamentais institucionalizadas” (BARRETO, 2009, p. 452) sem fugir dos fundamentos e princípios básicos da validade jurídica do ordenamento brasileiro de direito. Deste modo, contratos eletrônicos possuem respaldo jurídico legal, desde que visados através da

neutralidade, capacidade jurídica, perenidade, identificação e requisitos mínimos estabelecidos no Livro III do Código Civil de 2002.

Neste sentido, à luz da legalidade, contrato eletrônico é qualquer tipo de contrato formado no curso de comércio eletrônico pela interação de duas ou mais pessoas por meio eletrônico, como e-mail, a interação de um indivíduo com um agente eletrônico, como um programa de computador, ou a interação de pelo menos dois agentes eletrônicos programados para reconhecer a existência de um contrato. Assim sendo, obrigatoriamente, utiliza banco de dados de pessoas e informações sigilosas, haja vista que é modelado, especificado, executado e implantado por um sistema de software (FILHO, 2015).

Os dois principais componentes de um contrato eletrônico são: originador e destinatário. O originador, de acordo com a Lei 13.709/2018, é o envolvido que envia, gera, armazena e/ou transmite qualquer mensagem eletrônica a ser enviada, gerada, armazenada ou transmitida a qualquer outrem sem incluir um intermediário.

Já o destinatário, à vista do mesmo normativo, é uma pessoa que é destinada pelo originador a receber registro eletrônico, também não incluindo intermediário. Logo, a lei divide estes dois, frente ao artigo 5º, em: titular: pessoa natural a quem se referem dados pessoais que são objeto de tratamento; e controlador – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais ou operador – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018).

Uma vez que os contratos eletrônicos são atualmente levados tão a sério quanto os contratos off-line, os mesmos princípios que se aplicam a um contrato válido serão aplicados aqui. A lei já reconhece os contratos firmados com fac-símile, assim, um acordo entre partes é legalmente válido se cumprir os requisitos da lei quanto à sua formação, ou seja, que as partes pretendiam principalmente criar um contrato. Esta intenção é evidenciada pela sua conformidade com os 3 pilares clássicos, ou seja: oferta, aceitação e consideração, e deve intimamente considerar a proteção de dados desde as etapas de oferta até o ato final de negociação jurídica, onde mora a problemática de direito aqui assumida: a proteção de dados.

Entendidos os componentes do e-commerce no que tange à negociação de contratos, da natureza e legalidade jurídica e historicidade, a fim de realizar a avaliação sistemática sobre os pontos de vista da proteção de dados na esfera jurídica brasileira, fundamenta-se, sequencialmente, algumas observações de consumo que são prevalecidas dentro dos contratos

eletrônicos, que, por igual, também respaldam a Lei Geral de Proteção de Dados Pessoais (LGPD) e trazem um maior fascínio às discussões aqui levantadas. Assim sendo, a próxima seção traz uma avaliação doutrinário-teórica com enfoque dentro do Direito do Consumidor buscando tangebilizar maiores entendimentos sobre a lesão ao direito à privacidade.

3 DAS RELAÇÕES DE CONSUMO

O Código Brasileiro de Defesa do Consumidor, Lei n ° 8.078 datada de 11 de setembro de 1990, é a legislação federal que cria declaração abrangente de direitos para os consumidores e representa nascimento do conceito de relações de consumo em Brasil. Projetada para, especificamente, proteger interesses vulneráveis, na medida em que um relacionamento de consumo é encontrado, foi p primeiro ao integralmente legal e normativo a reconhecer a posição vulnerável dos consumidores (GAMA, 2002).

Dentre os direitos assegurados pelo CDC, no que se refere aos contratos eletrônicos, estão o disposto no artigo 31. Isso porque, certamente, uma das principais funções da internet é fornecer os meios de apresentar e oferecer produtos e serviços, prevalecendo as competências dos negócios e contratos jurídicos em suas relações. Neste sento, tal artigo apresenta que:

> A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores (BRASIL, 1990).

Logo, a oferta e apresentação de produtos via Internet deve assegurar informações que tragam informações gerais para os clientes, especialmente no que tange à segurança destes – e aqui se impetra a segurança da informação, do negócio e das transações realizadas, isto é, seu fundamental direito à privacidade. Além disto, o Código também complementa o Decreto 7.962 de 2013, que surgiu a fim de suprir lacunas de direito sob o e-commerce e os fundamentos das relações de consumo no Brasil. Neste sentido, a subseção abaixo traz uma avaliação lega das disposições desprendidas neste.

3.1 DECRETO N. 7962/13

O Código de Defesa do Consumidor estabelece, em seu art. 46º, que os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo, ou se os respectivos

instrumentos forem redigidos de modo a dificultar a compreensão de seu sentido e alcance (BRASIL,1990). Assim, Garcia (2009) entende que para que contratos tenham validade e obriguem consumidores, faz-se preciso que os fornecedores ofereçam oportunidade de tomar conhecimento efetivo de todos os direitos e deveres, principalmente no que se refere à privacidade.

Todavia, ocorre que, previamente à 2013, a maioria dos sites de venda não informam os direitos básicos do consumidor nem suas políticas de privacidade, as condições em que o consumidor possa estar prejudicado, e quais os seus direitos fundamentados, fato que fundamentou a construção de ato legislativo nº 7.962 – que buscou, sobretudo, desprender competência jurídica sobre as relações de consumo eletrônica. Enquanto demandas jurídicas, estabelece-se em seu segundo artigo 2º que:

> Os sítios eletrônicos ou demais meios eletrônicos utilizados para oferta ou conclusão de contrato de consumo devem disponibilizar, em local de destaque e de fácil visualização, as seguintes informações: I - nome empresarial e número de inscrição do fornecedor, quando houver, no Cadastro Nacional de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda; II - endereço físico e eletrônico, e demais informações necessárias para sua localização e contato; III - características essenciais do produto ou do serviço, incluídos os riscos à saúde e à segurança dos consumidores; IV - discriminação, no preço, de quaisquer despesas adicionais ou acessórias, tais como as de entrega ou seguros; V - condições integrais da oferta, incluídas modalidades de pagamento, disponibilidade, forma e prazo da execução do serviço ou da entrega ou disponibilização do produto; e VI - informações claras e ostensivas a respeito de quaisquer restrições à fruição da oferta. (BRASIL, 2013, negrito da autora).

Logo, a lei traz, à luz do e-commerce, competências que previamente eram atribuídas às empresas factíveis no meio físico, ampliando as aplicações legais e, principalmente, ensejando o dever a responsabilidade civil sobre os atos eletrônicos, frente ao aspecto de segurança e celeridade contratual. Além disto, em seu artigo 4º, apresentou os princípios da informação e transparência nas relações e-commerce, ao fomentar que:

> Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá: I - apresentar sumário do contrato antes da contratação, com as informações necessárias ao pleno exercício do direito de escolha do consumidor, enfatizadas as cláusulas que limitem direitos; II - fornecer ferramentas eficazes ao consumidor para

> identificação e correção imediata de erros ocorridos nas etapas anteriores à finalização da contratação ; III - confirmar imediatamente o recebimento da aceitação da oferta; IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução, imediatamente após a contratação; V - manter serviço adequado e eficaz de atendimento em meio eletrônico, que possibilite ao consumidor a resolução de demandas referentes a informação, dúvida, reclamação, suspensão ou cancelamento do contrato; VI - confirmar imediatamente o recebimento das demandas do consumidor referidas no inciso , pelo mesmo meio empregado pelo consumidor ; e VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor (BRASIL, 2013, negrito da autora).

A quebra da privacidade, às vistas de Filho (2015), principalmente quando do compartilhamento de dados entre instituições de diferentes naturezas jurídicas, é um rompimento com os preceitos estipulados ainda na base do artigo 2, que afirma ser dever do fornecedor de apresentar ao consumidor, haja vista o princípio da transparência e a qualificação da privacidade: “III - características essenciais do produto ou do serviço”, e se afunila nos entendimentos do artigo 4, que compreende que este ainda deve: “IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução” e “VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor” (BRASIL, 2013). Assim, ao importar no compartilhamento de informações sem devido respaldo contratual, incorre-se em responsabilidade compartilhada de ambos.

É importante discernir, neste sentido, que o Direito do Consumo vem para amplificar os entendimentos do e-commerce como um sujeito com personalidade jurídica no ordenamento brasileiro, isto é, trazer o sujeito eletrônico empresarial sobre responsabilidade, devidamente fundamentada, das ocorrências de seus atos. Esta denotação é observada em julgados onde se tem uma caracterização íntima de responsabilidade, como devidamente registrada na Apelação do TJ-RS disponibilizada abaixo:

> APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. ATAQUE DE HACKERS À PLATAFORMA DE LOJA DE E-COMMERCE. FURTO DE DADOS PESSOAIS DE CLIENTES. INFORMAÇÕES NÃO SENSÍVEIS. AUSÊNCIA DE PROVA DE VIOLAÇÃO DA IMAGEM, DA INTIMIDADE E DA PRIVACIDADE. DANOS MORAIS NÃO CONFIGURADOS. 1 Embora seja de todo pertinente

> e compreensível a preocupação do autor que teve seus dados pessoais hackeados por uma falha no serviço de segurança cibernética da ré, não se vislumbra, no caso concreto, qualquer circunstância que justifique excepcionalidade de indenização por dano moral. 2. Situação em que os dados furtados não se qualificam como informações sensíveis, assim consideradas as relativas à orientação ideológica ou sexual do indivíduo, ou aquelas que respeitem a sua origem étnica ou social, ao seu patrimônio genético ou as suas convicções política, partidária, filosófica ou religiosa. Inexistente, ademais, qualquer indicativo de que tenha havido difusão de dados bancários e financeiros ou a divulgação de outras informações cobertas por sigilo. 3. Caso dos autos que não revela, assim, qualquer ofensa à garantia constitucional de inviolabilidade da honra, da imagem, da privacidade e da intimidade do autor, de sorte que incabível a indenização postulada na petição inicial. Precedentes jurisprudenciais. APELAÇÃO DESPROVIDA. (TJ-RS - AC: 70082870973 RS, Relator: Carlos Eduardo Richinitti, Data de Julgamento: 20/11/2019, Nona Câmara Cível, Data de Publicação: 22/11/2019, negrito da autora).

Na relação exposta pela 9º Câmara do TJ-RS, fica evidente a caracterização de consumo que ensejou na relação de responsabilidade – tal quanto o objetivo de análise deste trabalho científico. Assim, sobretudo, nesta tipificação, é importante que entender que o ordenamento brasileiro – com auxílio da Decreto nº 7.962/2013 e do Código de Defesa do Consumidor (1990) estabilizam o e-commerce como uma figura jurídica que pode se subscrever tanto no polo passivo quanto ativo da ação. E em tal ímpeto de responsabilidade, o AC 10000204652572001 MG (TJ/MG) reafirma as posições do TJ-RS, embora com resultado contrafecho:

> EMENTA: APELAÇÃO CIVIL. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS. SITE DE VENDAS DIGITAL ("E-COMMERCE"). "MERCADO LIVRE". "MERCADO PAGO". FRAUDE. DANO MATERIAL. CULPA CONCORRENTE. CONFIGURAÇÃO. DANO MORAL. REQUISITOS. AUSÊNCIA. 1. Independentemente da modalidade de dano, o dever de indenizar somente se verifica se comprovado pelo autor da demanda, nos termos do que dispõe o art. 373, inc. I, do CPC, a efetiva ocorrência do dano, seja patrimonial ou extrapatrimonial. 2. Embora o vendedor realmente pudesse ter observado algumas regras de segurança antes de enviar o produto anunciado, certo é que a prestadora dos serviços de "e-commerce" possui parcela de culpa na ocorrência do evento danoso, motivo pelo qual resta configurada a culpa concorrente. 3. Diante da

> constatação de culpa concorrente, a fixação do valor dos danos deverá ser proporcional à conduta de cada um dos envolvidos. 4. Para configuração do dano moral é indispensável a demonstração da violação aos direitos da personalidade da vítima, como sua honra, imagem, privacidade ou bom nome. (TJ-MG - AC: 10000204652572001 MG, Relator: Cláudia Maia, Data de Julgamento: 19/11/2020, Câmaras Cíveis/14º CÂMARA CÍVEL, Data de Publicação: 19/11/2020).

É notável, desta forma, que à luz da relação de consumo – que pauta as atividades que são realizadas dentro do e-commerce, há configuração e personalidade jurídica deste a fim de assumir posição de direito no ordenamento brasileiro, não somente (e principalmente quanto se fala nesta análise científica) dentro do campo da privacidade, mas nas celebrações contratuais e nos negócios jurídicos que são celebrados nos meios eletrônicos, indiferente das plataformas e/ou provedores que são utilizados nesta relação.

Assim, é possível compreender uma seguinte premissa sobre a relação e-commerce, consumo e os direitos fundamentais: há previsão legal e, inclusive, constitucional, quando se fala violação da imagem, da intimidade e da privacidade por parte dos contratos jurídicos eletrônicos formulados no país. E com isto em determinado, portanto, inicia-se a avaliação legal a respeito desta temática, trazendo aspectos fundamentais dos dados pessoas no meio digital e da Lei Geral de Proteção de Dados estipulada em 2018.

4 DADOS PESSOAIS

De acordo com Finkelstein (2004), dados pessoais são toda e qualquer informação relativa a uma pessoa física identificada ou identificável; isto é, quando um conjunto de informações individuais é referida sob um sujeito identificado, dá-se nome, para este conjunto, de dados pessoais, sendo o sujeito aquele que pode ser identificado, diretamente ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou para um e/ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa in natura (CASTELLS, 1999; FINKELSTEIN, 2004).

Neste sentido, dados anônimos são o oposto de dados pessoais e se referem a informações que não se relacionam com uma pessoa identificada ou identificável, ou são dados tornados anônimos de tal forma que seu titular não é ou não mais será identificável, geralmente atribuído a competência coletiva. Logo, o processamento de dados anônimos não aciona o aplicativo da lei de proteção de dados. Já os dados pseudônimos, ou seja, dados pessoais após pseudonimização, ainda são informações pertencentes a uma pessoa e assunto identificáveis à lei de proteção de dados, pelo caráter individualista (TURBAN et al., 2009).

Com base nestes conceitos, é perceptível que a definição resultante de dados pessoais é ampla, flexível e adaptável a contexto tecnológico, isto é, os dados podem ir desde informações de competência normativa (registros gerais, cadastros e documentos próprios) até o rompimento do sigilo e da intimidade humana, entrando no campo do registro religioso, sexual e, até mesmo, espiritual (TURBAN et al., 2009). No maior sentido, portanto, entende-se dados pessoais como uma referência à pessoa natural identificável por informações relativas a esta – que, automaticamente, levanta à interpretação sobre o que constitui uma possibilidade relevante de identificação e um relacionamento relevante entre informação e um indivíduo. Isto é, qual a tipificação (ou as mais de uma) que caracteriza as possibilidades de identificação de alguém.

Barreto Júnior; Gallinaro; Sampaio (2018) adotam um teste de probabilidade razoável de identificação por controlador ou por outra pessoa, levando em consideração não a subjetivo capacidade de identificar, mas o Estado da Arte da tecnologia no momento do processamento; ou seja, para verificar se um indivíduo é identificável, deve-se levar em consideração todos os meios razoavelmente prováveis de serem usados, como a seleção, pelo controlador ou por

outra pessoa para identificar alguém direta ou indiretamente, o tempo e as possibilidades da informação já ter sido vazada e, obviamente, a competência de informações. Logo, não somente dados pessoais devem ser resguardados, mas seu vazamento deve ter fundamento legal.

4.1 CONCEITO JURÍDICO LEGAL

Enquanto conceito legal, dados pessoais são assumidos pela Lei nº 13.709/2018, frente ao seu artigo 5º, para fins legais como informações legais tão quando observadas por Finkelstein (2004) e Barreto Júnior; Gallinaro; Sampaio (2018). Assim sendo, este diploma legal estabelece em generalidade e especificidade, que:

> Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; 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 (BRASIL, 2018).

Neste sentido, Danilo Cesar Maganhoto Doneda estabelece, frente a caracterização geral de dados pessoais, que:

> O vínculo da informação pessoal com o seu titular deve ser de tal natureza a revelar diretamente algo concreto sobre esta pessoa. Assim, a informação pessoal refere-se às suas características ou ações, atribuíveis à pessoa em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então informações diretamente provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como opiniões que manifesta, e tantas outras (DONEDA, 2019, p. 19)

O sentido resultado do autor é amplo tão como as observações de Cots (2019), também defensor do conceito geral do termo. Já a lei, além desta definição, também estabelece o dado sensível que, embora tenha a mesma natureza e competência jurídica, é atribuída a áreas que fundamentam a dignidade humana e os princípios da inviolabilidade da

intimidade, liberdade e dignidade à vida. Além disto, também traz composições já apresentadas, como os dados anônimos e os bancos de dados – informações retidas no e-commerce.

Ainda sob os dados, a 13.709/2018 estabelece ainda uma visão sobre os agentes de conduta, ainda no art. 5º, ao conceituar que o titular dos dados pessoais é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); e os agentes de tratamento são, respectivamente, o controlador e o operado (BRASIL, 2018).

4.2 Natureza jurídica

Em suma, entende-se que que o direito à proteção de dados pessoais tem natureza jurídica de direito fundamental autônomo, haja visto que é inserido dentro dos direitos fundamentais do art. 5º da CF/88, expressamente no LXXIX, que aprende ser "assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (DE LUCCA, 2009). Assim, com fundamento e caráter pétreo (BRASIL, 1988).

Tal entendimento encontra escopo em Borges (2007), que assimila:

> Os direitos da personalidade, portanto, são próprios do ser humano. Não se trata de direito à personalidade, mas de direitos que decorrem da condição humana. Com os direitos da personalidade, protege-se o que é próprio da pessoa, como o direito à vida, o direito à integridade física e psíquica, o direito à integridade intelectual, o direito ao próprio corpo, o direito à intimidade, o direito à privacidade, o direito à liberdade, o direito à honra, o direito à imagem, o direito ao nome, dentre outros. Todos esses direitos são expressões da pessoa humana considerada em si mesma. Os bens jurídicos mais fundamentais, primeiros, estão contidos no direito da personalidade. A Constituição Federal bem andou ao inseri-los, todos os acima tirados, em um único Título (segundo), a que atribuiu denominação consentânea com seu conteúdo: “Dos direitos e garantias fundamentais” (art. 5º a 17), entre os quais repousam, como anotados foram, outros de natureza personalíssima, que, a partir daí, com eles se identificariam (BORGES, 2007, p. 141)

Logo, os dados pessoais, ou o direito à privacidade e intimidade, tem sentido de intransmissibilidade e irrenúncia, extrapatrimonialidade, imprescrição, vitalidade e ilimitação; limitando inclusive a própria ação do seu titular, não podendo ser exercido por outro exceto o titular de causa dentro do normativo jurídico brasileiro. Deste modo, somente o indivíduo que foi de maneira direita ou indireta influenciado pela ausência de proteção de dados que pode reconhecer o direito de tutela em juízo ao passo que, pela própria natureza do conceito de dados pessoais, é obrigatoriamente necessário que se reconheça a existência de vazamento de dados e, em principal, o indivíduo para o qual os dados foram vazados (BORGES, 2007), sob ilegitimidade de ação na tutela de direito.

4.3 Lei da Proteção de dados gerais

O Brasil é o maior país da América do Sul e o quinto maior do mundo em área e população, estimada em mais de 205 milhões em julho de 2012. Barbosa (2011), aponta que o uso de tecnologias de informação e comunicação vem aumentando significativamente em todo o país nos últimos anos, segundo indicadores nacionais. Para citar apenas alguns, a proporção de domicílios com computador nas áreas urbanas passou de 17% em 2005 para 39% em 2010; no mesmo ano, a grande maioria das empresas pesquisadas afirmou usar computador (97%) e ter acesso à Internet (95%).

A preocupação com a proteção dos dados das pessoas cresceu ao longo dos anos, mas somente após a aprovação da Lei brasileira que recebeu o nome de Marco Civil da Internet, instituída pela Lei nº 12.965, de 2014, ganhando apelo popular. E recentemente, uma nova lei foi recentemente sancionada e está gerando discussão em várias áreas. Chamada de Lei Geral de Proteção de Dados Pessoais, de nº 13.709/ 2018, esta fomenta os direitos à população brasileira e garantias sobre como as organizações terão de se adaptar à recolha e aos tratamentos de dados pessoais, seja por meios físicos ou digitais.

No Brasil, a legislação é baseada no modelo positivista de direito, adotado por escolas lusitanas, alemãs e italianas que privilegiam a lei escrita, isso se reflete no atraso da implementação do processo legislativo, que se inicia com a ideia, passa pela criação do

projeto de lei, depois pela aprovação bicameral e depois pela sanção presidencial, para finalmente entrar em vigor com força coercitiva (DINIZ, 2012).

A primeira iniciativa brasileira sobre proteção de dados pessoais foi no artigo 5º da Constituição Federal de 1988, que estipulou que "todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo aos brasileiros e estrangeiros residentes no País a inviolabilidade do direito à vida, liberdade, igualdade, segurança e propriedade, nos seguintes termos:

> X - A intimidade, a privacidade, a honra e a imagem das pessoas são invioláveis, garantindo-se o direito à indenização pelos danos materiais ou imateriais decorrentes de sua violação XII - O sigilo da correspondência e das comunicações telegráficas, dos dados e das comunicações telefônicas é inviolável, salvo neste último caso por ordem judicial, nos casos e na forma que a lei estabelecer para a investigação criminal ou processo penal (BRASIL, 1988).

Em 11 de setembro de 1990 foi promulgada a Lei nº 8.078, conhecida como Código do Consumidor (CDC), trazendo em seu artigo 43º a garantia de acesso aos dados do titular, exigindo clareza e objetividade das informações e possibilidade do consumidor a exigir a correção de seus dados cadastrais. Todavia, mesmo trazendo alguns avanços na proteção de dados pessoais, o CDC ainda era limitado em sua abrangência sobre o assunto, o que significa que a proteção existiria na relação entre fornecedor e consumidor no âmbito apenas de conceitos legais estabelecidos em lei, praticamente em um rol taxativo. Entretanto, com a modernização do país a partir de 2005 e com o avanço da comunidade eletrônica, especialmente após 2010, não demorou muito para que novas leis fossem criadas.

Em 23 de abril de 2014, foi aprovada a Lei nº 12.965, hoje conhecida como Marco Civil da Internet (BRASIL, 2014), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, e tem a garantia de privacidade e proteção de dados pessoais, e só tornará esses dados disponíveis por meio de uma ordem judicial. Também inclui aspectos da responsabilidade pela proteção de dados pessoais pelos provedores de acesso e nas operações realizadas através da Internet, potencializando a existência da Lei nº 13.709, denominada Lei Geral de Proteção de Dados Pessoais, que dispõe sobre o tratamento de dados pessoais, sejam eles digitais ou não, para proteção dos direitos fundamentais de liberdade e privacidade e a

desenvolvimento da personalidade pessoal do indivíduo na sociedade, da qual se fomenta um estudo nas alíneas comentadas abaixo.

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi sancionada em 18 de setembro de 2020, mas as sanções administrativas ocorreram em fins de 2022. Fornecendo orientações sobre como os dados pessoais serão coletados e processados para garantir a segurança e integridade do titular destes, foi aprovada através do Projeto de Lei 53/2018 pelo plenário do Senado Federal e sancionada em 14 de agosto de 2018 pelo 37º Presidente do Brasil.

Seu primeiro artigo da afirma que está preparada para proteger o processamento de dados pessoais e direitos de liberdade, privacidade e desenvolvimento da personalidade do indivíduo. Além disso, aplica-se a qualquer pessoa física ou jurídica que realize operações de processamento, como coleta, produção, recepção, classificação, processamento, entre outras atividades por meio físico ou digital, no território nacional, ou no exterior, utilizando dados pessoais de pessoas físicas morando no Brasil, especialmente nos campos de consumo e comerciais, de onde se notaram as maiores problemáticas na área (BRASIL, 2018). Além disto, descreve, em seu artigo 2º, que:

> A disciplina da proteção de dados pessoais tem como fundamentos: I o respeito à privacidade; II a autodeterminação informativa; III a liberdade de expressão, de informação, de comunicação e de opinião; IV a inviolabilidade da intimidade, da honra e da imagem; V o desenvolvimento econômico e tecnológico e a inovação; VI a livre iniciativa, a livre concorrência e defesa do consumidor; e VII direitos humanos, livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018, negrito da autora).

Assim, é uma disciplina jurídica que busca não somente a regulamentação das práticas eletrônica, mas fundamentalmente a busca pela tutela dos direitos de privacidade, dignidade humana, intimidade e liberdade, além deum resguarde dos sistemas financeiros e de possíveis crimes supraindividuais, causados pela disseminação de informação incoerente, incompetente, não autorizada ou anacrônica no mercado brasileiro.

Um dos pontos mais importantes que possibilita o tratamento dos dados é a obtenção do consentimento do titular dos dados, nos termos de seu artigo 7º, sendo que no artigo 8º é reforçado que a autorização deve ser por escrito ou por outro meio de manifestação da

vontade do titular, constando do §2º que, caso a autorização seja por escrito, deverá constar das cláusulas contratuais (BRASIL, 2018).

A LGPD também explícita que quaisquer atividades que requeiram processamento de dados devem ter o consentimento do titular dos dados, no artigo 6, parágrafo 1, e que o processamento de dados irá ser lícito mediante consentimento do titular dos dados para fins específicos previamente informados a este (BRASIL, 2018). Isto posto, é importante desprender que sem uma lei de referência para a utilização de dados pessoais, aumenta a possibilidade de abusos na recolha e utilização de dados pessoais, bem como o incentivo de vários outros organismos não especializados a emitirem suas opiniões sobre a utilização de dados, o que faz com que grande confusão, e por isto a essencialidade da lei aqui apresentada, sob a qual os princípios são apresentados na subseção abaixo.

4.3.1 Princípios da LGPD

Para um melhor entendimento da LGPD, é necessário conhecer os princípios que devem ser observados para qualquer tipo de atividade de processamento de dados. Esta é composta por dez princípios, listados nas projeções abaixo conforme determinado via a sanção ocorrida em agosto de 2018 pelo presidente Michel Temer.

O primeiro princípio é sob o objetivo. Na LGPD, a finalidade para a qual os dados serão feitos deve ser muito específica, explícita e informada ao titular dos dados pessoais que serão processados (BRASIL, 2018). Neste caso, frente ao princípio de limitação de propósito, os dados devem ser coletados para fins específicos, legítimos e explícitos e não podem ser processados para outros fins não especificados, sob pena de nulidade contractual e, inclusive, responsabilidade dos agentes envolvidos.

O segundo princípio enseja sobre a adequação das informações. A referida lei afirma que há necessidade de formalidade com o titular dos dados pessoais para o tratamento de dados pessoais, isto é, segundo o princípio de limitação de armazenamento, dados podem ser armazenados em um banco de dados até o final do processamento dos dados e devem ser informados ao proprietário destes, além de serem excluídos ao final do processo (MARQUES, 2014).

Há também o princípio de minimização de dados, onde se afirma que a quantidade de dados para processamento de dados é apenas relevante, proporcional e não excessiva

(MARQUS, 2014) ao passo que o livre acesso, quarto princípio afirmado pelo seu artigo 17º descreve que o detentor de dados tem livre acesso à sua totalidade de informações. A mesma premissa segue para o quinto princípio, que respalda na qualidade dos dados, que devem ser claros, precisos e apresentar relevância e atualização (BRASIL, 2018).

Em frente, a LGPD também garante que o proprietário dos dados terá acesso a todas as informações necessárias de forma precisa, além de fácil acesso ao processamento dos dados. Logo, o princípio de transparência é dividido em três palavras: legalidade, justiça e transparência. No que se refere à legalidade ou licitação, controladores de dados devem cumprir o regulamento. Já sobre equidade ou lealdade, afirma-se que o processamento deve ocorrer de forma justa com consentimento do proprietário dos dados e, na transparência, o controlador de dados permitirá que ele tenha acesso a todas as informações de todos os processamentos de dados que venham a ocorrer (BRASIL, 2018).

Findando a caracterização de princípios, tem-se ainda o de segurança, que afirma a obrigatoriedade do fornecer de cumprir com os respaldos técnicos mínimos para garantir a segurança da informação bem como também o princípio da prevenção que assimila que o mesmo (fornecedor) deve evitar processos que possam onerar o processamento da informação. Por fim, mais dois são assumidos, não discriminação de dados e emissão de relatórios de responsabilidade e competência a fim de garantir a segurança para o hipossuficiente da relação.

4.3.2 Aplicações da Lei

Deve-se observar que tanto a legislação brasileira quanto a europeia fornecem guia para o processamento de dados e quais os procedimentos as empresas devem adotar. E caso estes guias não sejam seguidos, empresas que tem práticas ilícitas incorrem em sério risco jurídico.

No Brasil, já diversos casos de perda de dados já ocorreram, como no caso do site da Netshoes, que produziu o vazamento de dados de mais de 1.999.704 usuários e consumidores,

colocando em risco sua saúde, bem-estar psicológico e direitos à privacidade e intimidade, caso estes os dados vazados caíssem em mãos erradas.

O impacto que o vazamento de dados vai muito além das perdas financeiras, a exposição das informações de cada cidadão pode ser um dano irreversível que se torna impossível mensurar o tamanho da perda. Sem uma política de segurança da informação, pode causar sérios problemas como invasão de sistemas vitais para roubo de declarações de impostos, dados, realização de transferências financeiras ilegais, interrupção de operações estratégicas de uma empresa ou governo. Por isso a importância de se aprender com o passado.

Outro caso de vazamento de dados foi escrito por Liliane Nakagawa e publicado no site Olhar Digital, que exibe notícias sobre a instituição bancária, especificamente o Fundo de Previdência do Banco do Brasil. Segundo Nakagawa (2020), o vazamento chegou a 153 mil clientes, número oficial de cadastrados na plataforma do BB Providência, segundo o Banco do Brasil. A fonte, que identificou lacuna de segurança, afirmou que por meio da previdência privada, destinada a empresas e órgãos públicos, é possível ter acesso a qualquer dado pessoal dos participantes e, desde a quebra, edição e cadastramento dos beneficiários, todos no nome da própria pessoa registrada.

Para que esses vazamentos não ocorram, as empresas devem ter *data protection officer* (DPO), que na lei brasileira é conhecido como encarregado dos dados, onde a função primária é garantir que os processos da organização os dados pessoais de seus funcionários, seus clientes, seus fornecedores ou quaisquer outros indivíduos de forma segura e confiável, de acordo com as normas legais de proteção de dados (UE, 2016).

No Brasil, a LGPD atua desde que entrou em vigor. O primeiro caso relatado foi a sentença proferida pela juíza Tonia Yuka Koroku, da 13ª Vara Cível de São Paulo, de que a Cyrela, que repassou os dados de um cliente após a compra de um imóvel, violando assim o respeito à privacidade, inviolabilidade da intimidade, proteção do consumidor e direitos humanos. A sentença determinou que a empresa não repasse ou ceda dados pessoais, financeiros e/ou sigilosos do cliente a terceiros, sob pena de multa de R$300 por contato indevido e pagamento de indenização de R$10.000 por danos morais (TJ-SP, 2021).

Com estes casos, é perceptível que há uma atuação prévia da lei, todavia, faz-se importante uma análise minuciosa sobre os requisitos de responsabilidade que devem ser

aplicados, fator que é analisado a partir da próxima seção, que define as características deste institutos e a sua aplicabilidade geral, frente a qual, em frente, faz-se uma discussão.

5. RESPONSABILIDADE CIVIL

5.1 Conceito e características da Responsabilidade Civil no Direito Brasileiro

De modo geral, às vistas de Lobo (2009):

> Responsabilidade civil é um dever jurídico sucessivo que surge para restaurar um dano causado pela violação do dever jurídico originário, em outras palavras, é a obrigação pecuniária de reparar um dano causado a outrem, seja ele por ação ou omissão, através da indenização – indiferente do tempo em que este está sendo julgado; obviamente não prescrito no ordenamento jurídico brasileiro (LOBO, 2009, p. 244).

Esta se baseia, assim, nas determinações do art. 186 e 937 do CC (2002), onde apresenta, *in verbis*, que 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. 186) e que aquele que, por ato ilícito (artigos 186 e 187), causar dano a outrem, fica obrigado a repará-lo (Art. 927) (BRASIL, 2002). Portanto, entende-se que a responsabilidade civil se trata de uma garantia do constituinte de que o lesado sofrerá uma indenização, que não se formula através de um modelo de vingança, por quaisquer que sejam os danos sofridos nem uma área de direito; seja esta de maneira sancionatória ou via outros resultados jurídicos possíveis, assumidos frente a interpretação (NICOLAU, 2006).

Considerando que todas as ações realizadas pelo homem e as coisas que estão ligadas a ele podem dar lugar à responsabilidade, o termo advém do latim *responre ou responsum*, que significa forçar-se a algo, comprometer-se a. Aparece quando uma obrigação não foi cumprida ou quando um dano é causado a outra pessoa, e pode ser definido como uma obrigação, agora então legal, de reparar ou satisfazer, por si ou por outrem, qualquer perda, dano ou prejuízo que possa ter sido causado por um ato realizado com discernimento, intenção e liberdade, segundo as definições de Diniz (2012).

De forma que a responsabilidade civil pela sua imputação seja “a qualidade ou condição da pessoa que, por ser livre e ciente do que faz, é obrigada a responder por sua conduta: o bem ou o mal que fez; ordem ou desordem em suas ações” (MIGUEL, 2003, p. 109), é claro que a, tem um duplo sentido, o primeiro como atitude compensatória de quem fez mal a outrem e o segundo como alteração para que a pessoa aja com a devida diligência; sendo estes fundamentados no Estado de direito brasileiro.

E frente a tal visão, dentro de sua responsabilidade, há os seguintes e elencados pressupostos ou requisitos devem ser dados: (a) uma violação, ou seja, uma real violação (voluntária ou não) do dever, que pode decorrer de uma ação ou omissão. Esta violação pode resultar de um ato ilegal, da violação de um contrato ou da violação de uma obrigação imposta diretamente por lei *ex lege* (MIGUEL, 2003); (b) dano ou dano suscetível de valorização pecuniária à pessoa, propriedade ou direitos (DINIZ, 2012); (c) uma relação causal entre a ação ou omissão e o dano causado (DINIZ, 2012); e/ou (d) um autor que pode responder pessoalmente pelo evento lesivo no caso de ser o autor direto ou por meio de um terceiro a quem é atribuído o dever de reparação das ações do autor material responsabilidade indireta (MIGUEL, 2003).

Neste sentido, os pressupostos para a existência de responsabilidade civil são: o incumprimento decorrente de um contrato ou obrigação legal, o dano quantificável, a relação causal entre a ação e o dano causado e a atribuição do dano causado à pessoa que executa a ação lesiva, sendo obrigatório a formulação de todos estes para que coexista o direito do Estado de punir o indivíduo e tutelar um direito de outrem (NICOLAU, 2006).

Já no que tange à sua imputação, admite duas versões: dolo, se praticada com a intenção e com conhecimento de prejudicar, e culpa que consiste na omissão das medidas que a natureza da obrigação exige e que correspondem às circunstâncias da pessoa, tempo e lugar. Da mesma forma, a culpa pode ser apresentada como: inadequação, que é a falta de conhecimento técnico em determinada arte ou profissão; imprudência, que é enfrentar os riscos sem tomar as devidas precauções para evitá-los ou não adotar as devidas salvaguardas, e negligência, que é não fazer o que é devido ou não agir com diligência (DINIZ, 2012).

Como já foi indicado, para que haja responsabilidade civil deve haver um sujeito autor da conduta lesiva a quem se possa atribuir a responsabilidade civil, esta atribuição deve ser por conduta negligente ou fraudulenta (dolo), ou seja, por uma conduta voluntária e/ou involuntária ou quando não se deseja a ação de dolo, mas é produzida por negligência, imprudência ou inexperiência do ator (DINIZ, 2012), o que deve recair sobre as práticas mencionadas.

Para a caracterização da responsabilidade civil, no que tange às relações especialmente comerciais, é imprescindível a prova da culpa, exceto quando houver disposição legal permitindo a responsabilização objetiva, conforme entendido por Venosa (2003), que afirma que a teoria da responsabilidade objetiva não pode, portanto, ser admitida como regra geral,

mas somente nos casos em que se tem aplicabilidade. Este respaldo vem do próprio artigo 12º e também do art. 14º do Código de Defesa do Consumidor, que assimilam:

> Art. 12: O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.
> Art. 14. O fornecedor de serviços responde, independentemente da existência da culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e risco (BRASIL, 1990).

Neste horizonte, percebe-se que ao mesmo passo que o art. 12 impõe a responsabilidade objetiva aos fornecedores dos produtos pelos danos causados, e o art. 14, igualitariamente, impõe a responsabilidade aos fornecedores de serviços, impondo que exista nexo casual entre o dano e/o defeito em um determinado negócio jurídico, este que pode ser complementado através de diversas formas, e todas estas podem se aplicar, impreterivelmente, dentro do direito digital e do direito do consumidor – inclusive no que se entende sobre o resguardo de suas informações e também seu direito à privacidade e intimidade, fato que é correlacionado a partir da próxima subseção, onde se faz uma análise da relação da Responsabilidade Civil com o Direito do Consumidor dentro da esfera jurídica brasileira.

5.2 Responsabilidade civil e Direito do Consumidor

Para resolver a questão da relação entre estas matérias de direito, ou seja, para entender o regime de responsabilidade aplicável ao fornecedor, vendedor e/ou figura que representa um polo ativo na relação comercial, é necessário voltar às obrigações, uma vez que a responsabilidade desta só surge em consequência do descumprimento daquelas entendido com falta de satisfação plena e oportuna da obrigação do que ela prescreve. Portanto, é imprescindível saber qual é a origem das obrigações quanto ao fato do consumo, tendo em vista as clássicas: contrato, crime, quase-contrato, quase-delito e direito, reconhecidas no

direito infraconstitucional brasileiro, que são subconjuntos de direito que determinam a relação entre responsabilidade, autoria, dano e infração de tutela.

Nesta visão, no CDC, observa-se que a autonomia privada que se conhece como formação do vínculo contratual é irrelevante do ponto de vista do que une as partes e das normas que regulam o fato do consumo (BRASIL, 1990). Assim, tanto situações como a entrada de alguém em um shopping center e a compra de um bem ou serviço tanto quanto relações, mesmo que não financeiras na internet, que constituem um mínimo vínculo de consumo, merecem proteção; logo, a lei contra fato jurídico adverso de consumo se vincula à formação de uma consequência jurídica da proteção, pois se os direitos do consumidor forem violados pelo fornecedor, ele será o responsável em virtude da lei, como determinado no art. 5º da Constituição de 1988 e também a própria lei 8.078/1990.

A imputação de responsabilidade consiste no elemento que a lei prevê para atribuir legalmente a obrigação de indenizar um dano, que no caso da responsabilidade civil desta pesquisa incorre por fraude e/ou culpa frente ao rompimento do direito à privacidade e intimidade do indivíduo na internet. Neste sentido, o objetivo do CDC é proteger os interesses do consumidor, de forma que o consumidor permaneça em pé de igualdade com o fornecedor em decorrência do alto nível de assimetria informacional que existe em um mercado de vendas massivas, especialmente na internet (onde não existem fronteiras), trazendo efetividade jurídica ao ator com hipossuficiência (SILVA, 2003).

Por isso, o interesse da Lei recai sobre o lesado e não sob o autor do dano, recusando-se, assim, a estabelecer um orçamento subjetivo, que, se presente, dificultaria a ação do lesado por ter um ônus maior em corte. Dentro deste caso, a Lei é quem prescreve o padrão mínimo que o fornecedor deve respeitar no mercado, acrescentando que a única violação das obrigações legais responsabilizará perante o consumidor, devendo proceder à sua reparação ou indenização, consoante tenha havido dano e, inclusive e imprescindível, este tenha ocorrido no bem ou serviço adquirido ou na integridade física ou mental do consumidor, encaixando-se o último em propriedade nos direitos fundamentais (privacidade) do art. 5º da Constituição Federal de 1988 (CAVALIERI FILHO, 2000).

Seguindo Cavalieri Filho (2000), a responsabilidade civil deve sempre tender a assegurar às vítimas uma compensação pelos danos que sofreram. Por sua vez, a respeito da adequada reparação dos danos sofridos pelo consumidor, indica-se que toda a limitação jurídica se deve dar pelas regras de causalidade objetivamente consideradas e não somente

pelo grau de culpa do fornecedor, isto é, o que importa, em suma referência, é o resultado do ato que fora ocorrido e não necessariamente – e obrigatoriamente – o grau de culpa ou o possível dolo ou culpa feito por um fornecedor, empresa, instituição e afins (CAVALIERI FILHO, 2000).

Assim sendo, em um negócio jurídico onde houve uma quebra de informações pessoais e privado, por exemplo, tem-se não apenas que considerar problemas que retornaram ao indivíduo (psicológicos, sociais e financeiros), mas também o impacto econômico-financeiro para a ordem social, a fim de estabelecer tutela para todos os envolvidos, especialmente porque, ao mínimo vazamento de informações, um grupo de pessoas tendem a ser desfavorecido e, inclusive, tutela supraindividuais podem ser mencionadas, haja vista que o vazamento de informações pode ascender processos de fraude no Sistema Financeiro Nacional.

Já na extensão dos danos, na responsabilidade, o CDC prescreve como reparável e amplo e que também incluirá tanto a pessoa do consumidor quanto o bem e/ou serviço adquirido, que em casos de informações pessoais vai desde campos econômicos até a moral, dignidade humana e saúde do indivíduo. Assim, à luz da responsabilidade e direito do consumidor, o réu deve responder em duas faces em favor do consumidor: “reparação” e “indenização”, por todos os danos materiais e morais em caso de não cumprimento de qualquer das obrigações contraídas pelo fornecedor e/ou pelos ferimentos ético-morais que tenha cometido em algum contrato, uso de informações e quaisquer condutas que se equiparem a uma relação de consumo, mesmo que não tácita para o consumidor (BONATTO; MORAES, 1998).

No que tange diretamente sobre os danos aos bens e serviços, relativamente à aquisição de um bem ou serviço pelo consumidor (aqui, por exemplo, podem ser incluídos kits de maquiagem, saúde, pastas comerciais de investimentos eletrônicos, cartões de créditos vazados e/ou roubados, dentre outros), o CDC estabelece garantia legal que consiste no exercício de uma série de direitos alternativos como a reparação, substituição, redução de preço e resolução e/ou a indenização pelos danos causados, tanto ao produto quanto ao indivíduo, imputando obrigatoriedade de indenização (BONATTO; MORAES, 1998; SILVA, 2003).

À vista disto, nota-se que o CDC busca estabelecer um vínculo de dever do fornecedor, indiferente de dolo, nas condutas de negócios jurídicos ou extrajurídicos, e aqui é

importante desprender o entendimento de Oliveira (2002) que afirma não existir limitação nas formas de realização do contrato e/ou no seu ambiente, quando dentro dos requisitos legais, isto é, indefere se a conduta inapropriada foi realizada no mundo real ou virtual. No mesmo entendimento, cabe trazer a visão jurisprudencial do caso relatado pelo Tribunal de Justiça de São Paulo que, inclusive, atribuiu responsabilidade subsidiária às plataformas eletrônicas que realizam intermediação de vendas, mesmo que não a concretizem:

> EMENTA: Prestação de serviços. Ação de indenização por danos material e moral. Site de intermediação de negócios por meio eletrônico. Consumidor vítima. Aquisição de celular junto à ofertante que promovia a venda ostentando falsa qualificação. Falso cadastro hospedado no domínio da empresa apelante. Aplicação do Código de Defesa do Consumidor (artigo 14). Responsabilidade objetiva do prestador de serviço. Relação jurídica de intermediação que não exonera o intermediador de responder pelos defeitos verificados na segurança das informações disponibilizadas que levaram ao usuário ao prejuízo experimentado. Dano material comprovado. Restituição do valor pago na falsa aquisição. Dano moral comprovado e fixado com moderação, observados os fatos, as condições das partes envolvidas e a repercussão do dano. Desnecessidade de qualquer redução. Correção monetária não se aplica do evento, mas da decisão que o arbitrou. Apelo provido em parte (Tribunal de Justiça de São Paulo, Apelação Cível 1.224.674-0/5, Relator Aleksander Coronado Braido da Silva, Julgado em 28 ago. 2015, Dje: 01 setembro de 2015).

Seguindo, no contexto do consumo antes, durante ou após a aquisição de um bem ou a prestação de um serviço, o consumidor pode estar exposto a lesões físicas ou mentais devidas a vários fatores. Esse dano que o CDC busca reparar acaba sendo extenso, pois não só os danos materiais, mas também os morais devem ser indenizados, especialmente quando se fala no direito à privacidade e intimidade (onde o número, grau e quantidade de informações vazadas e/ou repassadas muitas das vezes não é matematicamente quantitativo e, inclusive, incorre em grandes escalas de indivíduos), visando deixar o consumidor, hipossuficiente, ileso, no mesmo estado em que se encontrava antes de ser vítima do ato lesivo que a lei prescreve, como o rompimento do princípio da privacidade.

Todavia, aqui há ampla discussão sobre a validade do negócio jurídico realizado, que também pode importar menores prejuízos ao réu (CAVALIERI FILHO, 2000), isto é, se houve autorização para utilização e para o compartilhamento de informações previamente salientada para o cliente, com seu devido consentimento, pode-se gerar dúvidas quanto as

responsabilidades que devem ser assumidas frente ao caso, haja vista que muitos termos de adesão já incluem estas políticas comerciais.

Por fim, no campo da causalidade, embora seja pela ação do fornecedor que o descumprimento de uma norma legal cause danos ao consumidor, não há fator psicológico que atue em relação ao dano previsto; isto é, não existe a necessidade de um vínculo devidamente psicológico – que afete o lesador neste campo – para que se determine o grau de intimidade entre os campos da responsabilidade civil e a necessidade de reparar os danos causados (CAVALIERI FILHO, 2000; BONATTO; MORAES, 1998).

Será, então, um vínculo normativo, pois é a lei infringida que deve agregar todo o elemento nocivo e configurar a responsabilidade do vendedor, fornecedor ou fabricante e, consequentemente, gerar ampla reparação e indenização em favor do consumidor (CAVALIERI FILHO, 2000), a partir de vazamento de informações privativas e também, e até mesmo, da quantidade de verba retirada do lesado na realização de negócios jurídicos, muitas das vezes não autorizados (aqui não se discute a validade destes). O nexo de causalidade é fato importante, portanto, para estas relações, pois determina se há obrigatoriedade em indenizar ou reparar um possível dano, e se este possui um mínimo impacto no consumidor.

Isto posto, findadas as compreensões teóricas sobre o CDC, realiza-se uma análise frente ao campo da Responsabilidade Civil e o Direito Digital, afirmando suas relações – nacionais e internacionais – e as principais problemáticas encontradas dentro do direito brasileiro no que tange à reparação e indenização de danos. Tal análise é feita na próxima subseção, disponibilizada logo abaixo.

5.3 Responsabilidade civil e Direito Digital

Mais da metade da população do Brasil utiliza o celular como principal meio de comunicação e acesso à internet. Isso permite, hoje, que as pessoas estejam conectadas a maior parte da vida, utilizando esse meio de conexão para diversos assuntos como trabalho, comércio, recreação, cultura, entretenimento, socialização e informação (OLIVEIRA, 2002). Este fenômeno causou um aumento de atos ilícitos e criminosos, que ultrapassam as fronteiras políticas que se conhece e complicam a forma como a responsabilidade civil é exigida, especialmente por, muitas das vezes, não serem comportados dentro do Estado brasileiro, mas

também em outros países onde há pouca legislação na área ou um comportamento constitucional demasiado disperso do encontrado no Direito brasileiro.

Atualmente, a responsabilidade civil na Internet é um dos grandes desafios da sociedade da informação. Para o direito civil clássico, a responsabilidade pode ser contratual ou extracontratual (OLIVEIRA, 2002). A primeira decorre da violação de uma obrigação por uma das partes de um contrato jurídico, como, por exemplo, exigir uma taxa de juros diferente da devidamente prevista dentro do contrato ao decorrer do pagamento de um empréstimo.

A segunda é o resultado de danos causados por pessoas, naturais ou jurídicas, que mantêm uma relação extracontratual (OLIVEIRA, 2002), como o quase do rompimento da privacidade e intimidade e, por consequência, da dignidade humana de indivíduos a partir do compartilhamento das suas informações pessoas à demais empresas, instituições ou pessoas. Em ambos casos, a lei brasileira impõe a obrigação de reparar os danos causados e/ou sofridos, mas em nível global não existe um padrão que possibilite a cooperação jurídica internacional sobre este assunto, o que acaba por desgastar, muitas das vezes, a legislação do Brasil.

A classificação dos danos nas relações privadas na Internet é uma faculdade dos regulamentos internos de cada Estado, que provoca variações consideráveis de um país para outro. Somado a isso, a ausência de um tratado multilateral ou de uma lei modelo que permita uma aproximação de cima para baixo da legislação, impossibilita o estabelecimento de padrões mínimos para as atividades dos provedores de conexão e aplicativos no ambiente virtual bem com para os e-commerces, para uma abordagem legislativa de baixo para cima. Isto, por exemplo, acaba por afetar as relações internacionais de direito (especialmente à privacidade pelo rompimento de informações na esfera brasileira).

Nesse sentido, o direito brasileiro é bastante flexível e aberto no que incorre em responsabilidade civil, pois reconhece em seu Código Civil um amplo universo de competências para as autoridades brasileiras, no que se vê ao contencioso transnacional e internacional. Os artigos 21 e 22 da referida norma permitem que o tribunal seja competente quando o réu, independentemente de sua nacionalidade, seja domiciliado no Brasil, quando a obrigação deva ser cumprida no Brasil ou quando o ato tenha ocorrido ou seja praticado no Brasil (BRASIL, 2002). É este entendimento que transcende a visão de que a Responsabilidade Civil pode ser aplicada na relação de consumo (e em qualquer outra) que ocorre pela internet e que tenha um mínimo de ligação com o território brasileiro – como, por

exemplo, prejuízo a um cidadão ou estrangeiro que esteja no país, mesmo que temporariamente.

No que diz respeito à responsabilidade civil na legislação brasileira, o ato causador do dano pode ser lícito, ilícito ou de risco. De acordo com o artigo 186 do Código Civil de 2002, comete ato ilícito quem, por ação ou omissão voluntária, negligência ou imprudência, violar direitos e causar danos a outrem, ainda que exclusivamente morais, como pode ser o caso de se romper a privacidade no meio eletrônico. Além disso, o artigo 187, também aplicável ao espaço virtual, dispõe que "o titular de um direito comete ato ilícito que, ao exercê-lo, ultrapassa manifestamente os limites impostos por sua finalidade econômica ou social de boa-fé ou de bons costumes" (BRASIL, 2002).

Neste caso, impreterivelmente no espaço eletrônico, Responsabilidade Civil também objetiva "estabelecer situações endossadas por atos ilícitos de terceiros, como elemento essencial para a vida em sociedade" (VENOSA, 2012, p. 411), impondo na causa do dano, a obrigação de repará-lo independentemente de culpa, ou quando da atividade normalmente efetuada pelo autor do dano implica, pela sua natureza, risco para os direitos de outrem, nos termos do artigo 927º do Código.

É inegável dizer, na relação de Responsabilidade e Direito Digital, que um dos grandes avanços da legislação brasileira foi a aprovação da Lei nº 12.965, de 23 de abril de 2014, que estabelece regras sobre responsabilidade civil por danos causados na internet. Conhecida como Lei do Marco Civil da Internet, estabelece princípios, garantias de direitos de uso da Internet no Brasil, bem como elementos de conexão para a solução de controvérsias decorrentes de atividades online, denotando a proteção legislativa dos prestadores e dos consumidores, em busca da liberdade de expressão e contrária à censura prévia, além de outros requisitos mínimos como a dignidade humana, privacidade e criminalização de condutas.

Nesta lógica, as regras gerais de competência são aplicáveis às relações jurídicas transnacionais na Internet, envolvendo os diferentes atores, tais como conexão, aplicação ou provedores de conteúdo e usuários bem como lojas de e-commerce, plataformas de relacionamento e pesquisa, redes sociais e até mesmo sites informações que resguardam informações de seus consumidores em controles de TI.

Como regra geral, à luz da jurisprudência, observa-se que as empresas estrangeiras domiciliadas no Brasil buscam minimizar a competência dos foros brasileiros para examinar

litígios envolvendo direitos de personalidade. No caso do Recurso Especial N ° 370.46 do Tribunal de Justiça de São Paulo, a Google Brasil Internet LTDA alegou a impossibilidade de cumprir a ordem judicial brasileira que ordenou o envio dos dados do responsável pela inserção de determinado vídeo na Internet, pois tais informações estariam sob jurisdição internacional dos Estados Unidos, e não do Brasil.

Todavia, o Superior Tribunal de Justiça determinou que o fato de a PI e outras informações serem de origem estrangeira não limita a competência judicial brasileira e não impede que as informações sejam fornecidas pelo provedor de conteúdo. Além disso, o tribunal baseou sua decisão no Decreto nº 3.810/2001, que regulamenta a cooperação internacional em matéria penal, o que não impede a jurisdição brasileira sobre a matéria (BRASIL, 2001). Neste caso, ao passo que as empresas internacionais buscam reduzir os danos ao direito à privacidade, intimidade e dignidade humana, a jurisprudência brasileira, cada vez mais, se unifica em comportamento ao discernir que não importa a caracterização sede, mas sim o fato ocorrido, ou seja, o nexo casual que traz Responsabilidade Civil a um determinado caso.

Embora a Lei de Dados Pessoais, Lei nº 13.709 de 14 de agosto de 2018, deixe clara a importância do respeito à privacidade, liberdade de expressão e autodeterminação informacional, entre outros princípios, esta não confere liberdade de manipulação de dados ao natural ou pessoas coletivas de direito público ou privado que trabalham com dados pessoais. A esse respeito, o artigo 3º deixa claro que, independentemente do país ou da sede onde se localizem os dados, e desde que a operação ou tratamento seja realizado em território brasileiro, compete a este conhecer e julgar as questões. relacionado ao assunto (BRASIL, 2018). Assim, prevê-se a competência legal para que se haja sobre o direito à privacidade, especialmente nas relações de consumo – que já são afirmadas pelo próprio Código de Defesa do Consumidor, como devidamente registrado na subseção acima.

Muitos são os elementos de conexão que levam à aplicabilidade da Responsabilidade Civil no Direito Digital, considerando tanto o nível nacional quanto internacional. O primeiro é referente aos atos jurídicos, e leva em consideração o lugar onde os provedores de conexão e aplicativos desenvolvem suas atividades (*locus regit actum*).

Neste sentido, o Capítulo II da Lei de Marco Civil na Internet, dispõe no artigo 11 que em qualquer operação, coleta, armazenamento, guarda e processamento de dados pessoais ou registros de comunicações por provedores de conexão e aplicativos à Internet (como os e-

commerces e redes sociais), em que, pelo menos, um (1) desses atos ocorra no território nacional, devem ser respeitados a legislação brasileira e os direitos à privacidade, proteção de dados pessoais e sigilo das comunicações privadas e de seus registros. Assim sendo, a legislação brasileira abre espaço para punibilidade tanto de fornecedores (e quaisquer outros agentes ativos de consumo) nacionais quanto internacionais ao polo passivo de uma ação de responsabilidade, indenização e de reparação, seja esta contractual e/ou extracontractual, como é o caso dos danos à imagem.

Isto é, se uma das atividades previstas na regulamentação ocorrer em território brasileiro, a lei aplicável será a brasileira. Considerando a imaterialidade da internet e que o usuário também é produtor de dados, a conexão com a legislação brasileira sempre será possível quando se tratar de atos de coleta, armazenamento ou processamento de dados pessoais. Em caso de dano, aplica-se a legislação brasileira em razão da *lex loci damni* (lei do lugar onde o ato ilícito foi cometido ou inicialmente gerado) (DE LUCA et al., 2015).

Em relação ao segundo elemento de conexão, é levado em consideração o local onde se encontra o bem móvel (terminal de comunicação) (*lex rei sitae*), sendo aplicável a legislação brasileira quando pelo menos um dos terminais (laptop, celular, tablet, entre outros) está localizada no Brasil para a coleta de dados em território nacional e também para o conteúdo das comunicações, nos termos do §1º do art. 11º, do Marco Civil da Internet. Em outras palavras, quando, por exemplo, uma compra (mesmo que no exterior) é realizada por um consumidor no Brasil e há infração contractual ou extracontractual, insurge competência jurídica para julgamento no direito brasileiro, em busca de reparar o ano

O terceiro elemento de ligação diz respeito às pessoas coletivas, estabelecendo que o disposto no referido artigo 11º também se aplica independentemente das atividades serem exercidas por pessoas coletivas domiciliadas no estrangeiro. Sempre que oferecerem serviços ao público brasileiro, aplica-se a legislação local, visto que toda empresa estrangeira deve ter pelo menos uma filial ou representação em território brasileiro *lex societatis* (MIGUEL, 2003). Aqui cabe desprender que estas realizações são aplicadas, obvia e tacitamente, aos fornecedores que são naturalmente brasileiros.

Ao mesmo tempo que afirma a competência dos tribunais brasileiros (já estabelecido o direito de punir), a Lei do Marco Civil da Internet impõe aos provedores de conexão e aplicativos de internet a obrigação de oferecer informações que permitam verificar p

cumprimento da legislação brasileira sobre armazenamento ou processamento de dados, no que se refere ao respeito à privacidade e ao sigilo das comunicações.

No entanto, essa obrigação exige mais regulamentação para estabelecer procedimentos que agilizem a apuração de infrações, o que ainda não ocorre no Brasil (DE LUCA et al., 2015). Todavia, é necessário entender que há uma busca estrutural e jurídica para tal realização.

Aliás, nesse sentido, a responsabilidade civil por danos decorrentes de conteúdo gerado por terceiros está definida na Lei de Marco Civil da Internet, que em seu artigo 18 estabelece que o provedor de conexão à Internet não é civilmente responsável por danos decorrentes de conteúdo gerado por terceiros, mas que estes respondem por suas atividades e subsidiariamente todos os envolvidos em uma determinada cadeia de produção de serviços, produtos e de quaisquer relações de consumo previamente estabelecidas (BRASIL, 2014).

No caso de provedores de aplicativos, o artigo 19 prevê que, a fim de garantir a liberdade de expressão e prevenir a censura, o provedor de aplicativos de internet só pode ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, ele não toma as medidas necessárias para que, no âmbito dos limites técnicos do seu serviço e no prazo estabelecido, os conteúdos indicados como infratores fiquem indisponíveis, reservando-se as disposições legais em contrário (BRASIL, 2015). Neste ditame, mais importante se faz o entendimento de que a Responsabilidade Civil é uma questão já pacificada dentro do Direito Digital, que não imputa discussões gerais, haja vista as duas legislações acessórios de 2014 e 2018.

Entretanto, é importante destacar que a finalidade destas leis é, por um lado, garantir a liberdade de expressão, comunicação e expressão de pensamento e prevenir censura. Por outro lado, buscam também proteger os direitos de personalidade, privacidade e dados pessoais, garantindo a neutralidade da rede e o respeito aos direitos humanos, considerando o potencial de danos transfronteiriços e soberania dos Estados para legislar sobre a matéria (MIGUEL, 2003).

Logo, à luz da inexistência de acordos internacionais percorridos no tema, a legislação brasileira supre a necessidade – mesmo que por somente agora – de pacificar o entendimento de que Responsabilidade Civil decorre das relações, seja elas consumidoras ou não, que ocorrem no ambiente virtual e eletrônico, indiferente da natureza contractual ou extracontractual e do nível de dano causado – quando este é perceptível.

É necessário entender ainda, à luz da relação da Responsabilidade Civil e do Direito Digital, que a aplicação *lex fori*, princípio predominante na jurisdição brasileira, muitas vezes é insuficiente para resolver os problemas que ocorrem no espaço virtual, pois tanto a imaterialidade quanto o caráter transnacional das violações dificultam a efetiva execução de um marco civil, que visa regular relações na internet e que acaba encontrando mais diversificadas barreiras jurídicas na execução de decisões judiciais que só chegam a uma solução através da cooperação jurídica internacional (DE LUCA et al., 2015).

Neste caso, embora a legislação brasileira não seja perfeita nos termos de proteção da Responsabilidade Civil em questões de atos ilícitos na internet, pelo menos há uma preocupação do governo em proteger essas questões delicadas e complexas. Assim, a exclusividade de que a jurisdição brasileira tem de ser competente em matéria de conflitos de leis abrange plenamente o ambiente da Internet. Desta forma, mesmo com a insuficiência total do *lex fori*, o ordenamento jurídico brasileiro, nos últimos anos, tem efetivado inúmeras jurisprudências que corroboram, cada vez mais, com Responsabilidade Civil em todos os ambientes de sua aplicabilidade, nacionais e internacionais.

O grande problema está em como responsabilizar os processos em relação ao anonimato e ao controle das informações, quando estas circulam por outros meios eletrônicos fora do controle de provedores de internet ou empresas. As trocas de terminal para terminal, como bluetooth, continuam a ser o terreno adequado para a ocorrência de atos criminosos ou danos civis. E assim sendo, o uso do princípio da analogia entre mundo físico e o virtual, embora seja alternativa mais utilizada até o momento, não é uma solução definitiva quando se enfrenta questões de responsabilidade civil, especialmente porque a responsabilidade exige os componentes assumidos nas subseções acima, como nexo de causalidade, dano e, principalmente, comprovação de autoria – que podem ficar inaptas quando não se reconhece de onde se vem um erro ou principalmente quem é o seu autor de competência.

Esta é uma problemática que pode ser discutida em outro momento, numa análise estrutural, haja vista que o foco deste trabalho científico é discutir a aplicabilidade da Responsabilidade Civil dentro do e-commerce quando do rompimento, divulgação ou compartilhamento – por culpa ou dolo – de informações que prejudicam o direito à privacidade, intimidade e a dignidade humana dos consumidores em um negócio.

Isto posto, cabe entender, então, que a legislação nacional brasileira trabalha para tornar mais claras as regras sobre os problemas derivados de danos causados no ciberespaço.

E que já se mostra pacífico que a relação entre Responsabilidade Civil, Direito Digital e Direito do Consumidor, matérias que são objetivamente aplicáveis às relações de consumo estabelecidas nos e-commerces e na disseminação de dados pessoas e informações gerais de indivíduos na internet, fato que é discutido na última seção de análise desta pesquisa, que busca evidenciar, tanto em nível doutrinário quanto jurisprudencial, o arcabouço jurídico nacional (e internacional) que afirma a existência e as possibilidades de aplicação na matéria aqui discutida. Abaixo, apresentam-se suas considerações.

6. E-COMMERCE, COMPARTILHAMENTO DE DADOS E RESPONSABILIDADE

Nesta seção, busca-se, especialmente, trazer a perspectiva jurídica sobre a responsabilidade no compartilhamento de informações e dados pessoais, sem devido consentimento, dentro das relações de consumos previamente estabelecidas dentro do cenário virtual. Logo, ao passo que se fundamenta as análises nos princípios da privacidade, intimidade, dignidade humana e demais outros, foca-se na discussão sobre a Responsabilidade Civil Extracontractual, que se faz pela subjetividade dos negócios jurídicos realizados no mundo eletrônico. Isto posto, abaixo se analisam as competências ligadas com tal instituto de responsabilidade.

6.1 Responsabilidade civil extracontratual

A Responsabilidade Civil é obrigação decorrente do dever legal de indenizar dano gerado, e neste caso, a questão da Responsabilidade civil contratual na internet apresenta um problema adicional, pois, ao contrário do que acontece na vida física, a relação jurídica no mundo virtual tem duas arestas contratuais: a que se refere às informações que são prestadas pela rede (ou seja, bytes, que são transmitidos quando salvamos uma imagem, design, vídeo, música ou serviço no computador); e outra referida quando a rede era apenas o veículo para a formalização de um contrato, servindo como qualquer outro suporte (LEONARDI, 2005).

O século XX foi marcado pelo papel do consumidor internacional, que se tornou agente ativo das relações econômicas transfronteiriças. Antes, o consumo era visado por deslocamento físico e com a expansão da internet, já no espaço virtual, os e-commerces

ganharam um notável reconhecimento dos consumidores, pela praticidade de contrato atribuídos, principalmente, por compras realizadas em cartões de crédito. Com isto, a Responsabilidade Civil Extracontractual ganhou uma nova discussão sobre a privacidade no meio eletrônico.

O Código Civil Brasileiro de 2002 estabelece que a liberdade de contratar será exercida em decorrência dos limites da função social do contrato, bem como a obrigação de cumprir o princípio da boa-fé até a assinatura do contrato (BRASIL, 2002). Observa-se aqui que, embora a legislação não seja expressa sobre contratos eletrônicos, por analogia, pode-se deduzir que nada na legislação local proíbe a aplicação desta norma ao contexto virtual para a realização de negócios jurídicos neste meio.

Normalmente, as soluções jurídicas em matéria de conflito e/ou violação contratual são dadas pelo estabelecimento do local onde ocorreu o dano, ou pela aplicação da legislação acordada no contrato. Porém, na Internet, a informação circula em várias jurisdições ao mesmo tempo, é necessário estabelecer ou definir qual seria a legislação aplicável. Assim, a solução oferecida pela legislação brasileira no sentido de submeter à jurisdição local é uma saída razoável para a reparação de danos causados a pessoas físicas ou jurídicas em território brasileiro, isto é, responde-se aqui pelo que é feito e realizado diretamente em território brasileiro, indiferente da nacionalidade do indivíduo (DE LUCA et al., 2015).

Ante a entrada do Marco Civil da Internet, o STJ já havia decidido pela obrigatoriedade dos provedores de aplicativos ou conteúdo e também e-commerces e demais fornecedores presentes na internet de obedecerem ao Código de Defesa do Consumidor (CDC). Assim afirmou o STJ: “o fato de o serviço ser prestado pelo provedor de internet gratuitamente não prejudica a relação de consumo” (BRASIL, 2011, p. 4). O que se determinou, *in verbis*, foi:

> Os provedores de serviços de Internet são aqueles que fornecem serviços ligados ao funcionamento dessa rede mundial de computadores, ou por meio dela. Trata-se de gênero do qual são espécies as demais categorias, como: (i) provedores de backbone (espinha dorsal), que detêm estrutura de rede capaz de processar grandes volumes de informação. São os responsáveis pela conectividade da Internet, oferecendo sua infraestrutura a terceiros, que repassam aos usuários finais acesso à rede; (ii) provedores de acesso, que adquirem a infraestrutura dos provedores backbone e revendem aos usuários finais, possibilitando a estes conexão com a Internet; (iii) provedores de hospedagem, que armazenam dados de

> terceiros, conferindo-lhes acesso remoto; (iv) provedores de informação, que produzem as informações divulgadas na Internet; e (v) provedores de conteúdo, que disponibilizam na rede os dados criados ou desenvolvidos pelos provedores de informação ou pelos próprios usuários da web. É frequente que provedores ofereçam mais de uma modalidade de serviço de Internet; daí a confusão entre essas diversas modalidades. Entretanto, a diferença conceitual subsiste e é indispensável à correta imputação da responsabilidade inerente a cada serviço prestado (Supremo Tribunal Federal, Relatora Ministra Nancy Andrighi, Terceira Turma, julgado: 26/06/2012, DJe 29/06/2012).

Aqui, por analogia, assume-se não somente os provedores, mas também os fornecedores em geral nas relações de consumo ocorridas na competência eletrônica. E neste caso do Recurso Especial 1.316.921 do RJ, o juízo determinou a responsabilidade do Google de excluir determinadas imagens dos resultados de busca de seu site, independentemente da indicação dos urls das páginas de providência das imagens. Responsabilidade subsidiária.

A busca era por garantir o direito à dignidade humana dos ofendidos e por resguardar imagens que ofendessem classes sociais e grupos de indivíduos menos favorecidos. E com este entendimento, é jurisprudencial a visão de aplicabilidade da Responsabilidade Civil, e aqui se entra no campo Extracontractual, de todo e qualquer fornecedor (mesmo que gratuito de relação de consumo) da internet.

Na perspectiva dos direitos fundamentais, a Constituição Federal assegura a liberdade de expressão, o direito do consumidor, a inviolabilidade da privacidade, a vida privada, a honra e a imagem das pessoas, garantindo o direito à indenização pelos danos materiais ou morais decorrentes de sua violação e garantindo o direito de propriedade, que deve atender à sua função social (BRASIL, 1988).

Além disto, acrescenta-se ao dispositivo constitucional que a manifestação do pensamento, criação, expressão e informação, sob qualquer forma, processo ou veículo não sofrerá qualquer restrição. Por sua vez, o Código Civil Brasileiro prevê que a liberdade de contratar será exercida pela razão e dentro dos limites da função social do contrato, o que determina que não há impedimento para equiparar contrato físico ao virtual, fator levantado no Recurso Especial 1.316.921 do RJ na aplicabilidade analógica do caso.

Com isto em entendimento, é possível discernir que, no caso de relações jurídicas internacionais que ocorram na Internet, envolvendo provedores de conexão ou aplicativos com seus usuários, o tribunal brasileiro é competente para decidir sobre a matéria nos termos

do artigo 21 do Código de Processo Civil, quando o réu, seja qual for a sua nacionalidade, está domiciliado no Brasil; quando a obrigação deve ser cumprida no Brasil; e quando o fato ou ato ocorreu ou foi praticado no Brasil. No mesmo sentido, o artigo 22 da referida norma também estabelece como jurisdição competente aquelas referentes às relações de consumo transfronteiriças, ou seja é possível, legalmente, punir e responsabilidade as condutas que conferem práticas ilícitas aos direito à privacidade, intimidade e a dignidade e honra do indivíduo, inclusive no compartilhamento de informações pessoas sem devida, e prévia, autorização.

Portanto, fica tácito que a autoridade judiciária brasileira é competente para dirimir as controvérsias decorrentes de danos por descumprimento de obrigações contratuais, relativos a danos causados pela própria pessoa ou por terceiros em razão do conteúdo publicado no espaço virtual (*damni fórum/forum delicti commissi*). O conteúdo pode implicar em infrações a vários direitos, como personalidade, privacidade, dados pessoais ou propriedade intelectual, todos que podem ser submetidos a indenizações individuais e coletivas (DE LUCA et al., 2015; MARICHAL, 2017; MULHOLLAND, 2015).

As relações internacionais privadas entre usuários e e-commerce têm sido objeto de processos judiciais perante os tribunais brasileiros. Em um dos primeiros processos perante o Supremo Tribunal de Justiça, Sentença 784-DF, o Google Brasil alegou a suposta impossibilidade de cumprir ordem de quebra de sigilo das comunicações, proferidas pelo investigado por meio do Gmail, e que o os dados em questão foram armazenados em território norte-americano. Alegou, ainda, que a controladora da Google Inc., domiciliada nos Estados Unidos, era quem de fato armazenava os dados do e-mail e do sms, que estariam física e legalmente inacessíveis para a filial no Brasil. A Câmara Especial do Juízo, decidida por maioria sobre a questão apresentada pelo juiz encarregado da causa, que a empresa sediada no Brasil se submete obrigatoriamente às leis brasileiras, seja com o vencimento do despacho de sigilo telemático expedido, então penalidade de multa diária. (STJ, 2013)

No caso do Recurso Especial 370.461-SP, interposto no Superior Tribunal de Justiça, Google Brasil Internet Ltda. Alegou não ser responsável pelo descumprimento de ordem judicial que determinou o fornecimento de dados pelo responsável pela inserção do vídeo indicado pelo Banco Opportunity SA, na jurisdição internacional, dos Estados Unidos, no que se refere à soberania, limites de jurisdição e efeitos da ordem judicial brasileira. O tribunal afirmou que a justificativa não obteve êxito e que o fato de a PI e outras informações serem de

origem estrangeira não retira a jurisdição brasileira e não impede que as informações sejam fornecidas. Além disso, o Decreto 3.820/2001 trata da cooperação jurídica em matéria penal, não sendo obstáculo ao tipo de informação solicitada (STJ, 2013). Mais uma vez, o comportamento das jurisprudências se alinhou na aplicabilidade de Responsabilidades frente aos e-commerces e/ou plataformas de consumo, como a Google.

No caso do Recurso Especial 733.830-SP, o STJ indeferiu o pedido apresentado pela Terra Networks Brasil S.A. contra decisão do juízo que determinou indenização da autora Eliana Cristina D.K. Bruno. Apesar de não ter produzido a reportagem, as imagens utilizadas foram da autora e foram divulgadas comercialmente no site, sem sua autorização, o que comportou em uma relação de consumo não autorizada e, por isto, passível de indenização, como fora salientado pelo Supremo Tribunal de Justiça (2013).

Aliás, no julgamento, o STJ destacou que a empresa que pretende trazer ao Brasil um serviço estruturado em novas tecnologias, e com abrangência que a internet tem, deve se preocupar em garantir a segurança desse sistema, não podendo atribuir ao consumidor ônus de buscar no exterior, e na legislação estrangeira, as garantias de proteção de seus direitos, cabendo à empresa responsável pelo serviço, no Brasil, assumir plena responsabilidade, sem prejuízo de que a empresa possa exigir o direito de retorno e compensação de acordo com as regras dos seus contratos internacionais (STJ, 2013).

Assim sendo, o entendimento da Justiça brasileira é que os fornecedores têm o dever de remover mensagens, imagens ou propaganda considerado ilegal ou ofensivo, promover a máxima legalidade contratual de seus negócios jurídicos e respeitas os limites jurídicos de transmissão de informações, à luz de penalidades de responsabilidade, como as correlatadas acima pelo Supremo Tribunal de Justiça.

Considerando que as empresas, tanto nacionais quanto estrangeiras, estão sujeitas à legislação e aos tribunais brasileiros no respaldo da responsabilidade, a decisão é aplicável em todo território nacional, portanto, quando os danos forem devidamente perceptíveis, com o seu devido acompanhamento de indenização e reparação. Neste caso, cabe entrar diretamente dentro da perspectiva de privacidade e intimidade, marco fundamental deste projeto, apresentado na subseção abaixo.

6.2 E-commerce e a proteção de dados

Para a análise das questões que acabam por exigir responsabilidade civil extracontratual na internet, é importante colocar especial ênfase em duas linhas fundamentais: a proteção dos dados pessoais e proteção dos direitos da personalidade, pela amplitude do direito civil que são suscetíveis a violações na rede. Afinal, o fenômeno da globalização tem fomentado o desenvolvimento de novas tecnologias, trazendo grandes vantagens para a sociedade e enormes desafios, que se baseiam, cada vez mais, na dificuldade de proteger direitos fundamentais como os salientados acima.

Com o desenvolvimento da tecnologia da informação, tem-se buscado dar maior segurança à proteção dos direitos à privacidade e à inviolabilidade dos dados pessoais decorrentes da atividade cotidiana do indivíduo na Internet. E o controle e a fiscalização exercidos, tanto pelos Estados quanto por grandes empresas de internet e sua automação, geraram o que a doutrina internacional reconhece como Big Data, ou seja, a grande massa de dados pessoais jurídicos e físicos (DE SOUZA, 2014).

As primeiras definições de dados pessoais na Internet vêm da jurisprudência europeia no caso Lindquist, onde o tribunal europeu decidiu que os nomes das pessoas, seu número de telefone, informações sobre seu trabalho, hobbies, gostos e preferências constituem dados pessoais, que não podem ser compartilhados entre instituições e nem devem ser utilizados para as atividades pelas quais não se obteve previsão em contrato lícito (DE SOUZA, 2014).

No desenvolvimento deste estudo se encontrou duas categorias: dados sensíveis e dados anônimos. Os primeiros se referem a dados cujo armazenamento, processamento e circulação podem levar a situações discriminatórias, pois se referem a questões de raça, saúde, vida sexual e condições criminais. Estes, pela visa extracontractual, sugerem danos não somente aos princípios fundamentais aqui salientados (privacidade, intimidade e dignidade humana), mas também em condutas criminosas, que são observadas a partir do Código Penal Brasileiro.

Já no caso dos anônimos, autores como Schertel (2014) referem que estes vêm de pessoas indeterminadas e podem ser usados para fins estatísticos, uma vez que sua finalidade acaba protegendo estas pelo anonimato. A ausência de legislação nacional a esse respeito indica que tal definição é inspirada na jurisprudência europeia e legislação existente a este respeito. Assim, à luz do contrato, o anonimato garante a inexistência de responsabilidade (SCHERTEL, 2014), ao passo que não se reconhece o dano envolvido e, muito menos, os indivíduos que sofreram consequências sobre a ação.

O desenvolvimento da web em nível internacional ocasionou um aumento na circulação de informações em escala global. Esse novo cenário foi propício ao desenvolvimento de novos bens e serviços por meio da internet, aumentando a quantidade de dados e seu armazenamento e comercialização, surgindo assim conceitos como o Big Data.

Milhões de consumidores deixam rastros digitais na web, que são convertidos em dados que passam a fazer parte da grande massa de dados que os gigantes da internet possuem hoje. Embora o termo venha da astronomia, acabou migrando para informática e o direito e adotando a definição daquela grande massa de dados que hoje é gerada por todo usuário que navega na rede. Thomas Davenport entende:

> Big Data é um termo genérico para dados que não podem estar contidos nos repositórios usuais; refere-se a dados que são muito grandes para serem armazenados em um único servidor; mal estruturado para ser adequado para um banco de dados em linhas e colunas, é muito fluido para armazenamento estático. Embora o conceito se refira ao seu tamanho, na verdade o mais complicado é a falta de estrutura (DAVENPORT, 2014, p. 81)

Se os dados eletrônicos estão disponíveis em qualquer lugar, pode-se falar em territorialidade como um elemento de conexão com as violações dos direitos sobre os dados pessoais? Certamente que não, pois a ausência de tratados internacionais de proteção de dados pessoais deixa o internauta desprotegido e à mercê das políticas e/ou contratos de adesão estabelecidos por gigantes da internet como Google, Facebook, Mercado Livre e OLX, que não oferecem aos seus usuários básicos informações sobre sua política de privacidade e de censura. Este ditame, todavia, tem respaldo na lei brasileira, como se pode ver abaixo.

No caso do Brasil, a Constituição de 1988 consolida o princípio da dignidade humana em seu artigo 1º, III, no qual é possível vislumbrar o tratamento da proteção à personalidade. Nos incisos X, XII e LXXII do artigo 5º, a disponibilização do habeas data é destacada como um recurso constitucional que visa garantir o acesso individual à retificação dos seus dados pessoais que se encontram nos bancos de dados públicos.

Outra norma que trata brevemente do assunto é a Lei de Acesso à Informação no Brasil (2011), que dispõe sobre os procedimentos a serem seguidos pelos estados e municípios brasileiros para garantir o acesso à informação, conforme dispõe o artigo 5º inciso XXXIII, artigos 37.2 e 216 da Constituição Federal de 1988.

Essa norma enfatiza que o tratamento dos dados pessoais deve estar em equilíbrio com o acesso à informação, de forma a garantir esse direito fundamental, art. 3º. Por sua vez, o art. 31, dispõe que o tratamento de dados pessoais deve ser feito de forma transparente, com respeito à privacidade, à vida privada, à honra e à imagem das pessoas, e de acordo com as liberdades e garantias individuais. Um aspecto interessante do próprio artigo é que não pode ser invocada a restrição de acesso às informações relacionadas à vida privada, quando o objetivo é prejudicar o processo de irregularidades nas informações.

No que diz respeito ao tratamento de informações pessoais, a Lei 12.414/2011 prevê em seu artigo 3º parágrafo III a proibição de anotações relacionadas às informações sensíveis como origem social, etnia, saúde, arquivo genético, orientação sexual e convicções políticas, religiosas e filosóficas. *In verbis*, afirma-se:

> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
> § 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado.
> § 3º Ficam proibidas as anotações de:
> I – Informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
> II – Informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (BRASIL, 2011).

Além disso, o CDC estabelece no artigo 43, parágrafo 2º, as questões relativas à abertura do cadastro de dados pessoais e do consumidor devem ser comunicadas por escrito ao consumidor, quando não por ele solicitadas. Assim afirma que todo "consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes" (BRASIL, 1990). Neste quesito, é importante destacar o caso Phorm Brasil, ordenado pela Secretaria de Proteção e Defesa do Consumidor, vinculada ao Ministério da Justiça, que determinou a aplicação de multa de 3,5 milhões de reais para fiscalização da navegação de consumidores na Internet, a fim de posteriormente comercializar seus dados, tornando-se uma prática comum no ambiente virtual. Este fato culminou na responsabilidade da empresa por utilizar dados pessoais para comportamentos de e-

commerces e foi determinado através dos princípios salientados na Constituição de 1988 e também nas discussões e aplicações do Marco Civil da Internet, entrado em vigência meses antes do caso. É importante, assim, entrar em alguns casos notórios de jurisprudência a fim de estabelecer a responsabilidade pela proteção e compartilhamento de dados propriamente ditos pelos e-commerces. O primeiro caso é da Apelação Cível 1.0471.16.012594 do TJMG, que afirma:

> EMENTA: APELAÇÃO CÍVEL - AÇÃO ANULATÓRIA DE CONTRATO E INDENIZAÇÃO POR DANOS MORAIS - CONTRATAÇÃO DE EMPRÉSTIMOS - CAIXA ELETRÔNICO - CULPA EXCLUSIVA DA VÍTIMA - NÃO CONFIGURADA - DEFEITO NA PRESTAÇÃO DO SERVIÇO BANCÁRIO - VAZAMENTO DE DADOS PESSOAIS - DANOS MORAIS CARACTERIZADOS - QUANTUM INDENIZATÓRIO - ADEQUAÇÃO DEVIDA - SENTENÇA REFORMADA EM PARTE. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, nos termos do art. 14 do Código de Defesa do Consumidor. Para que seja configurada a excludente de responsabilidade do fornecedor prevista art. 14, §3º, II do CDC deve ser comprovada a culpa exclusiva do consumidor. Reveste-se de ilicitude a hipótese em que a instituição financeira permite ou não cuida para impedir o vazamento dos dados pessoais de seus clientes oportunizando, assim, a atuação ilícita de terceiros fraudadores. A fixação da indenização por danos morais pauta-se pela aplicação dos princípios da razoabilidade e da proporcionalidade. (TJMG - Apelação Cível 1.0471.16.012594-7/001, Relator(a): Des.(a) Juliana Campos Horta , 12ª CÂMARA CÍVEL, julgamento em 31/7/19, publicação da súmula em 8/8/19)

A decisão do Tribunal de Justiça de Minas Gerais, neste caso, imputa que a Responsabilidade Civil pelo resguardo de informações é diretamente impetrada pela Instituição Financeira, que aqui é representada pelo e-commerce (atividades em internet e no aplicativo). Logo, mesmo que as informações tenham vazadas por meio de fraude, é aplicável a Responsabilidade Civil Extracontractual devido à ofensa a proteção de dados e os riscos assumidos por possíveis fraudes em informações do cliente. Entendimento idêntico é visto também no Tribunal de Justiça do Estado do Tribunal de Justiça do Amapá, que afirma:

> CONSUMIDOR CONTRATO DE FINANCIAMENTO DE VEÍCULO. FRAUDE. COMPROVADA. DANOS MORAIS. COMPROVAÇÃO. VALOR DO DANO. ADEQUAÇÃO. RECURSO CONHECIDO E PROVIDO EM PARTE. somente não responderá pela reparação dos danos causados se provar que, tendo prestado o serviço, o defeito inexiste

> ou o fato é exclusivo do consumidor ou de terceiros. a) No caso dos autos, Ficou evidente que os dados do autor, independentemente de sensíveis ou pessoais (art. 5°, I e II, Lei Gera de Proteção de Dados Pessoais - LGPD) foram tratados em violação aos fundamentos de sua proteção (art. á°, LGPD) e à finalidade específica, explícita e informada ao seu titular (art. 6°, I, LGPD). 3) Não houve contrato firmado entre as partes. Entretanto, conforme prova documental, houve a utilização de seus dados para finalidade diversa e sem que o autor tivesse informação adequada (art. 6°, II, LGPD), o que afronta diretamente o disposto no artigo 6°, III e IV, do Código de Defesa do Consumidor, quanto as dever de informação. Assim, não existe suporte para a exclusão de responsabilidade, pois ficou caracterizado o ilícito relativo à violação de direitos da personalidade, por utilização indevida de dados pessoais. 4) Quanto aos danos morais, no caso em particular, deve ser reduzido, em consonância com os julgados desta Turma Recursal, para o valor de R$ 4.000,00 (quatro mil reais). 5) Recurso conhecido e provido em parte. Sentença parcialmente reformada para reduzir o valor dos danos morais para R$ 4ar00,00 (quatro mil reais), permanecendo inalterados os demais termos do julgado. Sem honorários (Tribunal de Justiça do Amapá, RI 0034398-48.2019.8.03.0001 AP, Relator Mário Mazurek, Julgado em 01/04/2021, Dje: 04/04/2021).

Neste requisito, além da utilização do Código Civil (2002) e também do Código de Defesa do Consumidor (1990) para o respaldo jurídico destas jurisprudências, é importante salientar o artigo 6 da Lei Geral de Proteção de Dados Pessoais (LGPD), que assume as seguintes composições jurídicas:

> As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações

> acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

Assim, ao passo que estas também não são cumpridas, incorre-se em mesmo direito de repara dano e compadecer com indenização para os casos de transmissibilidade de informações. E isto posto, então, é conclusivo que a Responsabilidade Civil Extracontratual importa, diretamente, em obrigatoriedade indenizatório e reparatório de danos causados por e-commerces, e para maior tratativa do fato, a próxima (e última) subseção, realiza uma avaliação quanto à aplicabilidade aos direitos da personalidade e pessoais, que respaldam em intimidade, privacidade, dignidade humana, liberdade e demais outros que podem recorrer do compartilhamento, fraude ou utilização inadequada de dados por e-commerces no Brasil.

6.3 E-commerce e os direitos da personalidade

A Internet traz um grande desafio às normas de direito privado relativas aos direitos da personalidade e à liberdade, pois geram divergências e conflitos entre esses direitos fundamentais. Hoje, a troca de informações no mundo virtual é intensa e instantânea. Por meio das redes sociais e de quaisquer componentes eletrônicos, uma pessoa ou empresa/instituição é capaz de interagir direta e indiretamente com muitas outras pessoas, influenciando seus hábitos, costumes, gostos e interesses. Essa troca em altos níveis é conhecida como efeito viral, onde imagens, vídeos, escritos, etc. são compartilhados ou divulgados (SCHERTEL, 2014).

Um conteúdo, uma imagem ou um vídeo publicado na internet, dependendo do seu conteúdo, pode ser viralizado sem o controle do primeiro usuário que o colocou na web. Este efeito viral pode causar violações dos direitos da personalidade, incluindo a imagem como o elemento mais vulnerável, expedindo casos de fraudes processuais, difamação, transferências de oportunidades e perdas incontáveis ao psicológico e desenvolvimento saudável de um indivíduo ou um grupo destes (SCHERTEL, 2014)

A Lei Geral de Proteção de Dados Pessoais estabelece em seu artigo 11º que o tratamento, compartilhamento e utilização de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

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

Assim, a LGDP assume as situações taxativas em que são previstas o compartilhamento e utilização de dados, respaldando aplicação de Responsabilidade Civil Extracontractual para os casos que assim não obedecerem. E ainda destaca que “dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido” (BRASIL, 2018). Logo, para a mesma aplicabilidade de responsabilidade, há o que se entender a necessidade de estabelecer um nexo causal e, principalmente, um dano ao indivíduo que pleiteou a ação, como no caso dos vídeos e informações divulgados, que, em intimidade, caracterizem tacitamente um indivíduo.

Lei do Marco Civil da Internet destaca, em seu artigo 21, a responsabilidade subsidiária para os e-commerces, qualquer que seja a situação que resulte da divulgação não autorizada de imagens, vídeos ou outros dados pessoais, financeiros, familiares e quaisquer materiais por seus participantes. Consequentemente, os fatos e atos praticados por pessoas no espaço virtual podem ter efeitos globais, e assim, a simples transmissibilidade de informações

que implique em ato ilícito no território brasileiro não apresentam respaldo jurídico se este não for cometido, em obrigatoriedade, dentro dos limites do Estado.

Isto dito, o fenômeno da viralização possibilita a qualquer pessoa ter seu momento de fama a nível nacional e global, levando em consideração a popularidade da pessoa, o fato e as circunstâncias de cada caso. Os efeitos negativos das informações (conteúdos errôneos, não autorizados pelo autor, entre outros) podem causar danos aos direitos da personalidade e à sua privacidade. No caso de e-commerces, a divulgação de informações para outras empresas pode ser punida quando foge aos interesses do contrato, ou são subjetivas no negócio jurídico, como bem aponta da LGPD no art. 9º, que afirma: "§1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo e/ou não tenham sido apresentadas, previamente, com transparência, de forma clara e inequívoca" (BRASIL, 2018) e também que "§2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações" (BRASIL, 2018). Deste modo, é de responsabilidade do fornecedor de cumprir com as obrigações do negócio jurídico e, fundamentalmente, informar os consumidores de eventuais mudanças nas políticas de privacidade, sob pena de aplicação de responsabilidade. Tal visão é observada na jurisprudência do Supremo Tribunal Federal:

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. A existência de fundamento não impugnado – quando suficiente para a manutenção das conclusões do acórdão recorrido – impede a apreciação do recurso especial (súm. 283/STF). 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011 – dentre as quais se destaca o dever de informação, que tem

> como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sob o armazenamento e o objetivo do tratamento dos dados pessoais 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentadas pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido (Supremo Tribunal Federal, REsp 1.758.799 MG 2017/0006521-9, Min. Nancy Andrighi, julgado 12/11/2019, Dje 17/11/2019, negrito da autora).

Com isto, o alinhamento da jurisprudência superior no país é de que não somente se faz obrigatório resguardar possíveis informações pessoais auferidas num negócio jurídico (quando devidamente declaradas) como também é necessária o informe ao consumidos, em todo e qualquer caso de e-commerce, sobre as alterações em suas informações e também a utilização destas para outras atividades empresas, seja da própria empresa ou de terceiros. Neste caso, mais uma vez, assume-se a tutela do direito à privacidade e intimidade, resguardando o direito do consumidor de ser indenizado em fatos equivalentes, tanto em nível nacional quanto, e também, no nível internacional de atividades.

É muito comum que os gigantes e-commerces e instituições da Internet fujam às suas responsabilidades sob diversificadas justificativas técnicas. Certamente, na jurisprudência brasileira existe consenso comum quanto à responsabilidade desses gigantes da internet no que diz respeito às violações cometidas por terceiros, como casos de fraude e processos de invasão e de hackers. Todavia, como bem entendido por Marques (2014), é de responsabilidade das instituições a Governança Corporativa em T. I., resguardando a segurança da informação e dos seus potenciais clientes de mercado. É o que se prevê no art. 46 da LGDP, que estabelece:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

As soluções que os grandes e-commerces (Mercado Livre, OLX, AliExpress e Alibaba) da internet oferecem hoje no ciberespaço se concentram apenas no caso a caso, e não na busca de um consenso único e geral para atos ilícitos que geram responsabilidade civil. As violações dos direitos da personalidade carregam a pior parte, pois uma vez praticadas no ambiente virtual, os obstáculos técnicos muitas vezes tornam os danos causados irreparáveis. E assim, além do pedido de indenização moral para a vítima, deve-se buscar uma solução técnica definitiva que consiga minimizar a permanência na rede de eventos que violam direitos da personalidade por tempo indeterminado, como maior segurança da informação, contratos eletrônicos devidamente delimitados e lógicos, dentre outros.

A jurisprudência brasileira apoia uma posição que acaba beneficiando os gigantes da internet em detrimento dos usuários que sofrem violações virtuais. No REsp 690.123-MG, o juízo de primeira instância resolveu a ação de obrigatoriedade ajuizada pela Diretoria de Transportes e Logística S.A. contra o Facebook Serviços Online de Brasil Ltda., para estabelecer a exclusão de perfis nas redes sociais.

Nesse caso, o magistrado decidiu que os provedores de serviços de internet só são responsáveis por danos causados a terceiros em decorrência de atos ilícitos praticados por seus usuários, se forem notificados sobre o conteúdo divulgado e permanecerem inertes, não retirando as informações prejudiciais. O mesmo pode ser aplicado também para empresas de e-commerces, como Mercado Livre e OLX, retirando a responsabilidade, por exemplo, de

transmissão de informação para perfis de fraudadores. Isto não somente afronta o princípio da privacidade e dignidade humana como também das relações éticas previstas pelo Código de Defesa do Consumidor e sua responsabilidade subsidiária.

Sobretudo a tal entendimento, ainda assim a justiça brasileira é competente para conhecer das questões que geram responsabilidade civil na internet. O fechamento da legislação local em relação aos elementos de conexão tem um ponto positivo se comparado com as realidades estrangeiras que estabelecem questões de compra de fórum, jurisdição pessoal ou fórum inadequado. Na LGPD, em suma, estabelece-se que "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, é obrigado a repará-lo" (BRASIL, 2018), explicitando a relação da Responsabilidade Civil Extracontractual com o Direito do Consumidor e Digital. Este entendimento fica mais evidente na caracterização da jurisprudência, que entende:

> APELAÇÃO CÍVEL. DIREITO PÚBLICO. PROCON. MULTA. COMPARTILHAMENTO DE DADOS PESSOAIS DE CONSUMIDORES. OI S.A. 1. Viola o direito do consumidor e o disposto na Resolução n° 003/ 24210 da SMSPC, a atitude da empresa de telefonia que compartilha seus dados pessoais com terceiros, ou, no mínimo, é negligente no cuidado com essas informações, possibilitando que outra empresa os obtenha. 2. 0 art. 57 do CDC diz que a multa será fixada de acordo com a gravidade da infração, a vantagem auferida e a condição econômica do fornecedor, o que se constata tenha prevalecido como parâmetro para fixar o valor da penalidade (TJ-RS, AC 021613280.2019.8.21.7000 RS, Rel. Carlos Roberto Lofego Canibal, Julg 13/11/2019, 22/11/2019).

Sobretudo a tal entendimento, ainda assim a justiça brasileira é competente para conhecer das questões que geram responsabilidade civil na internet. O fechamento da legislação local em relação aos elementos de conexão tem um ponto positivo se comparado com as realidades estrangeiras que estabelecem questões de compra de fórum, jurisdição pessoal ou fórum inadequado. Na LGPD, em suma, estabelece-se que "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, é obrigado a repará-lo" (BRASIL, 2018), explicitando a relação da Responsabilidade Civil Extracontractual com o Direito do Consumidor e Digital. Este entendimento fica mais evidente na caracterização da jurisprudência do TJ-DF, que entende:

> DIREITO CIVIL. DIREITO DO CONSUMIDOR. FRAUDE DE TERCEIRO. FALHA NA PRESTAÇÃO DE SERVIÇOS. SEGURANÇA. VAZAMENTO DE DADOS. RENEGOCIAÇÃO DE DÍVIDA. EMISSÃO DE BOLETO. - Na forma do art. 46 da Lei 9.099/1995, a ementa serve de acórdão. Recurso próprio, regular e tempestivo. Pretensão declaratória de inexistência de renegociação de dívida bem como indenizatória por danos materiais e morais em razão de ação de terceiro fraudador no âmbito de renegociação de dívida junto ao Serasa. Recurso do réu visando à reforma da sentença de procedência parcial dos pedidos. - Falha na prestação de serviços. Na forma do art. 14, § 1°, inciso II do CDC, é objetiva a responsabilidade civil do fornecedor quando há falha na segurança da prestação de serviços que o consumidor pode razoavelmente esperar. No caso presente, houve falha no sistema de segurança da ré, que permitiu a interceptação de comunicação de danos no próprio site da ré, permitindo a fraude praticada por terceiro. O vazamento de dados pelo SERASA é objeto, inclusive, de investigação perante a Secretaria Nacional do Consumidor - SENACON, de forma que a responsabilidade pela falha na prestação de serviços resta caracterizada (https://valorinveste.globo.com/nolicia/gogi/m/g6/senacon-notifica-serasa-sobre-sobre-vazamento-de-dados-de-gg3-milhes-de-pessoas.ghtml). 3 - Responsabilidade Civil. Ausência de culpa exclusiva do consumidor. No caso, diante do vazamento de informações dos consumidores pela própria empresa ré, não restou caracterizada nenhuma das hipóteses de exclusão da sua responsabilidade. 4 Fraude. Renegociação de Dívida. Demonstra o autor que ao fornecer seu CPF através do aplicativo whatsapp para o fraudador, que na oportunidade utilizava o nome ?Serasa Limpa Nome?, este confirmou outros dados pessoais como nome, endereço e o valor da dívida (ID. x1.3x14xx), de forma que diante da aparência de regularidade realizou a renegociação da dívida através da empresa Ideal Acordo, suposta representante da ré. A informação correta pelo fraudador de todos os dados vazados pela instituição ré subsidia a atitude de confiança do autor ao realizar o acordo sem desconfiar de possível fraude. Ainda que o autor não tenha sido totalmente diligente e evitado o prejuízo suportado, a disponibilização de seus dados de forma indevida não exime o fornecedor de sua responsabilidade. 5 - Danos Materiais. Demonstrada a responsabilidade do fornecedor de serviços, devida a reparação material no valor de R$L9o8,44, equivalente ao prejuízo que teve ao realizar o pagamento de boleto fraudado, conforme determinado na sentença. Sentença que se mantém pelos próprios fundamentos. (TJ-DF, 0702829-80.2020.8.07.0020 DF, Rel. AISTON HENRIQUE DE SOUSA, jul 09/04/2021, Dje: 29/04/2021.

A contrapartida também é válida ao passo que é devidamente necessário o nexo causal para que se estabeleça a efetividade e materialidade da Responsabilidade Civil

Extracontractual, como pode ser visto no julgamento do Tribunal de Justiça do Rio Grande do Sul, que no AC 0259006-80.2019.8.21.7000 RS estabeleceu que:

> APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. ATAQUE DE HACKERS À PLATAFORMA DE LOJA DE E-COMMERCE. FURTO DE DADOS PESSOAIS DE CLIENTES. INFORMAÇÕES NÃO SENSÍVEIS. AUSÊNCIA DE PROVA DE VIOLAÇÃO DA IMAGEM, DA INTIMIDADE E DA PRIVACIDADE. DANOS MORAIS NÃO CONFIGURADOS. 1. Embora seja de todo pertinente e compreensível a preocupação do autor qui teve seus dados pessoais hackeados por uma falha no serviço de segurança cibernética da ré, não se vislumbra, no caso concreto, qualquer circunstância que justifique a excepcionalidade de uma indenização por dano moral. 2. Situação em que os dados furtados não se qualificam como informações sensíveis, assim consideradas as relativas à orientação ideológica ou sexual indivíduo, ou aquelas que respeitem a sua origem étnica ou social, ao seu patrimônio genético ou as suas convicções política, partidária, filosófica ou religiosa. Inexistente, ademais, qualquer indicativo de que tenha havido difusão de dados bancários e financeiros ou a divulgação de outras informações cobertas por sigilo. 3. Caso dos autos que não revela, assim, qualquer ofensa à garantia constitucional de inviolabilidade da honra, da imagem, da privacidade e da intimidade do autor, de sorte que incabível a indenização postulada na petição inicial. Precedentes jurisprudenciais. Desprovida. (TJ-RS, AC 0259006-80.2019.8.21.7000 Relator Carlos Eduardo Richinitti, Julg: 20/11/2019, Dje: 22/11/219).

Este é o mesmo entendimento do RI 1003754-95.2020.8.26.0562 do Tribunal de Justiça de São Paulo que determinou “Dano material configurado. Devolução do valor da bem. Danos morais afastados. Indenização por dano moral que deve ser reservada para os casos de dar profunda e intensa, em que morre violação aos direitos da personalidade. Recurso parcialmente provido” (TJ-SP, 2021). Com isto posto, fica clara existência de Responsabilidade Civil quando cumpridos os requisitos mínimos de sua existência já explicado bem como quando de relações consumidoras abusivas e que fogem ao padrão da LGDP. Frente a isto, abaixo apresenta-se as considerações finais da pesquisa.

7 CONCLUSÃO

A responsabilidade civil por danos é um dos grandes desafios da sociedade globalizada, dada a ausência de tratados internacionais que unifiquem normas de direito internacional privado em matéria de conflitos de jurisdição e as legislações aplicáveis na matéria e também da natureza dos contratos realizados por atividades e-commerces, que muitas das vezes fogem das premissas básicas dos negócios jurídicos.

Na legislação brasileira, a responsabilidade civil é o mecanismo geral que visa responsabilizar a pessoa física ou jurídica que causa dano a outrem e estabelece a obrigação de reparar o dano sofrido, independentemente da origem do dano. Tanto a Lei de Introdução às Normas Brasileiras, o Código Civil, o Código de Processo Civil e a Lei do Marco Civil da Internet, coincidem na exclusividade da aplicação das normas brasileiras às empresas, tanto nacionais quanto internacionais, em suas atividades *latus sensus,* determinando como regra de jurisdição a aplicação de responsabilidade, comprovado o nexo de causalidade, autoria e fato, que, no caso de empresas e-commerces do exterior, infere necessidade do ato (dano) ter sido praticado em território brasileiro ou com obrigação aqui cumprida.

A Lei do Marco Civil da Internet bem como a LGPD, por sua vez, como norma específica em vigor para regulamentar questões de internet, protege o direito à personalidade e a proteção de dados e afasta a ideia de censura aos conteúdos inseridos na internet, estabelecendo, ao nível de transição de dados, um comportamento seguro da empresas no compartilhamento e resguardado de dados pessoais (e pessoais sensíveis).

Esta regra cria um novo tipo de responsabilidade civil para as empresas da internet, não sendo objetiva nem subsidiária, em relação aos danos causados por terceiros, ou seja, responsabilidade civil pelos danos derivados de conteúdos gerados por terceiros por violação de ordem judicial, que requer a remoção do conteúdo declarado ofensivo ou reparação de dado em caso de vazamento por imperícia ou incompetência da instituição encontrada na web. Assim, sobretudo, e a partir dos entendimentos expelidos nos demais capítulos, cabe entender que há aplicabilidade de responsabilidade civil nos mais diversos casos de violação de privacidade, intimidade e dignidade humana para os dados tratados na web, seja por culpa ou dolo do fornecedor, que deve responder pelas condutas (inclusive implícitas) às luzes do Código de Defesa do Consumidor, do Código Civil que, quiçá, do Código Penal Brasil.

Com base nestas conclusões iniciais, entendendo que o objetivo central deste projeto era de realizar uma parametrização legal-doutrinária e jurisprudencial acerca dos normativos que ceram o comércio eletrônico no país focando em apresentar os fundamentos de responsabilidade civil frente ao direito fundamental da privacidade/intimidade e o rompimento de sigilo de dados retirados de um negócio jurídico eletrônico – seja por fraude ou por reconhecimento e trocas comerciais entre diferentes empresas, cabe desprender que a pesquisa saciou o conhecimento buscado, passando pelas origens jurisprudências, doutrinárias e técnicas do tema, inclusive sob a letra da lei, reafirmando a legitimidade da Responsabilidade Civil, neste caso, especialmente Extracontractual, observadas as premissas necessárias da aplicabilidade desta, como o nexo de causalidade, o efetivo dano e autoria e também o repasse ou compartilhamento de informações pessoais e/ou sensíveis, e não anônimas.

Com isto, cabe concluir também que o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais servem como marcos primitivos de direitos para assumir as responsabilidade das relações que ocorrem no ambiente eletrônico, não tão somente ao nível de consumo, mas também nas tipificações, como os crimes de injúrias, compartilhamento inadequado de informações e publicidade enganosa. Estas leis, assim, são respaldos objetivos jurídicos que buscam a efetividade da Responsabilidade Civil (para e-commerces internacionais e nacionais) para os casos de ofensas e danos, sem necessitar de analogia ou subjetividade jurídica de entendimento, bastando a comprovação dos fatos para que se conclua a reparação e possível indenização do dano sofrido.

Assim sendo, marcam uma nova geração de conhecimento em direito digital e constitucional, ao ligarem o mundo real (prático e ostensivo) com a globalização da comunidade virtual, que carece de arcabouço jurídico para regulamentar suas operações em todo o mundo, em suas mais diversificadas áreas de direito. O que se espera, daqui pra frente, considerando as inserções notadas durante este projeto, é que se aprofunde as caracterizações de infração e, fundamentalmente, a subsidiariedade da Responsabilidade Civil Extracontractual, haja vista que, no nível contractual, este componente já encontra respaldo no Direito do Consumidor.

Além disto, falta estruturação física e maior publicidade do direito atribuído ao consumidor nas relações com o e-commerce que, por estarem em pouca pauta, passam despercebidos à tutela individual e coletiva dos indivíduos, que pouco conhecem dos seus

direitos. Hoje, a internet é ainda um universo sem regramentos, mas que pode ser usada para a transmissão de informação útil e competente aos cidadãos, como as tutelas indenizatórias e de reparação, que são atribuídas pelas leis aqui mencionadas, mas pouco conhecidas por seus benefícios.

Por fim, como sugestão de próximos estudos, fica a realização de uma análise comparativa dentro do direito internacional a fim de reconhecer os limites territórios de aplicação dos institutos aqui tratados e como os demais países tratam a perspectiva de privacidade, compartilhamento de dados e sistemas de consumo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTIN, A. L. Comércio eletrônico: modelo, aspectos e contribuição da sua aplicação. 2ª ed. São Paulo: Atlas, 2004.

BARRETO JUNIOR, I. F.; GALLINARO, F.; SAMPAIO, V. G. R. Marco civil da internet e direito à privacidade na sociedade da informação. Revista Direito, Estado e Sociedade, n. 52, 2018.

BARRETO, R. M. Contrato Eletrônico Como Cibercomunicação Jurídica. Revista Direito Gv, São Paulo (SP), v. 5, n. 2, p. 443-458, Jul-dez/2009. Disponível em: <https://www.scielo.br/pdf/rdgv/v5n2/10.pdf>. Acesso em 10 mar. 2021.

BOIAGO, J. W. J. Contratação Eletrônica: Aspectos Jurídicos – 1º ed.- Curitiba: Juruá, 2005. pg. 78.

BONATTO, C.; MORAES, P. V. D. Questões controvertidas no Código de Defesa do Consumidor: principiologia, conceitos, contratos. Porto Alegre: Livraria do Advogado, 1998.

BORGES, R. C. B. Direitos de personalidade e autonomia privada. 2 ed. São Paulo: Saraiva, 2007, p. 20.

BRASIL. Código Civil. Porto Alegre, Verbo Jurídico, 2002.

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

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: < https://presrepublica.jusbrasil.com.br/legislacao/91577/codigo-civil-lei-10406-02>. Acesso em 08 mar. 2021.

BRASIL. TJ-MG. AC: 10000204652572001 MG. Relator: Cláudia Maia, Data de Julgamento: 19/11/2020, Câmaras Cíveis / 14a CÂMARA CÍVEL, Data de Publicação: 19/11/2020. Disponível em: < https://tj-mg.jusbrasil.com.br/jurisprudencia/1127918729/apelacao-civel-ac-10000204652572001-mg>. Acesso em 11 mar. 2021.

BRASIL. TJ-RS. AC: 70082870973 RS. Relator: Carlos Eduardo Richinitti, Data de Julgamento: 20/11/2019, Nona Câmara Cível, Data de Publicação: 22/11/2019Disponível em: < https://tj-rs.jusbrasil.com.br/jurisprudencia/936065749/apelacao-civel-ac-70082870973-rs>. Acesso em 11 mar. 2021.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Apelação Cível nº 20120111804179. Relator: Romeu Gonzaga Neiva. Brasília, 19 de julho de 2017. Disponível

CASTELLS, M. A sociedade em rede. 6. ed. rev. e ampl. Tradução: Roneide Venâncio Majer. São Paulo. Paz e Terra. 1999.

CAVALIERI FILHO, S. O direito do consumidor no limiar do século XXI. Revista de Direito do Consumidor. Revista dos Tribunais, n. 35, jul-set, p. 97-108, 2000

COTS, M. Lei Geral de Proteção de Dados Pessoais Comentada /Márcio Cots e Ricardo Oliveira. 3.ed. atual e ampl. São Paulo: Thomson Reuters Brasil, 2019

DAVENPORT, T. Big data no trabalho: derrubando mitos e descobrindo oportunidades, Elsevier, Rio de Janeiro, 2014.

DE LUCCA, N. Aspectos da responsabilidade civil no âmbito da internet. São Paulo: Saraiva, 2009. E-book.

DE LUCCA, N. et al. Direito & Internet III – Tomo II: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015, p. 307- 320

DE SOUZA, A. The Application of Rome II on the Internet Torts. Masaryk University Journal of Law and Technology, 2014, v. 8, n. 1, p. 39.

DINIZ, M. H. Curso de Direito Civil Brasileiro: Responsabilidade Civil, 26ª ed. Saraiva – São Paulo, 2012.

DONEDA, D. C. M. A proteção de dados pessoais nas relações de consumo: para além das informações creditícias. Brasília: Secretaria de direito econômico/Departamento de proteção e defesa do consumidor, 2010.

FERRAZ JR., Tércio Sampaio. Sigilo de dados: O direito à privacidade e os limites à função fiscalizadora do Estado. Revista da FD-USP, v. 88, 1993, p. 440.

FILHO; C. R. P. L. Direito & Internet III – Tomo II: O Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 277-305.

FINKELSTEIN, M. E. R. Aspectos Jurídicos do Comércio Eletrônico. Porto Alegre: Editora Síntese, 2004.

FINKELSTEIN, M. E. R. Direito do Comércio Eletrônico. 2. Ed. Rio de Janeiro: Elsevier, 2011

GAMA, H. Z. Curso de Direito do Consumidor. 1ª Ed – 4ª tiragem. Rio de Janeiro: Forense, 2002.

GARCIA, Leonardo Medeiros. Direito do Consumidor: Código Comentado e Jurisprudência – 5. ed. – Niterói: Impetus, 2009. p. 281.

KHAN, A. G. Electronic Commerce: A Study on Benefits and Challenges in an Emerging Economy. Global Journal of Management and Business Research: B Economics and Commerce, v. 16, n. 1, junho/2016.

LEONARDI, M. Responsabilidade civil dos provedores de serviços de Internet. Tese de Doutorado. USP. 2005. 203 f.

LORENZETTI, R. L. Comércio eletrônico. RT, 2004, p.19. E-book.

MARICHAL, J. De volta à névoa: o futuro do Facebook, 2013.

MARQUES, C. L. O novo direito privado e a proteção dos vulneráveis. 2ª ed. ver., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2014.

MIGUEL, A. Responsabilidade civil no novo código civil: algumas considerações. São Paulo: Revista dos Tribunais, 2003.

MULHOLLAND, C. Responsabilidade civil indireta dos provedores de serviço de Internet e sua regulação no marco civil da Internet. In: Encontro Nacional do CONPEDI, XXIV, 2015

NAKAMURA, R. R. E-Commerce na Internet: Fácil de Entender. São Paulo, Érica, 2001. ISBN 1970- 85-7194-750-3

OLIVEIRA, E. D. A proteção dos consumidores nos contratos celebrados através da Internet. Coimbra: Almedina, 2002. p. 66.

PAESANI, L. M. Direito e internet: liberdade de informação, cidade e responsabilidade civil, 3a ed. São Paulo: Atlas, 2006, p. 36-60

PINHEIRO, P P. Proteção de dados pessoais: Comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

REEDY, J.; SCHULLO, S. Marketing eletrônico: integrando recursos eletrônicos no processo de marketing. São Paulo, Thomson Learning, 2007. ISBN 978-85-221-0535

SCHERTEL, L. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental, Saraiva, São Paulo, 2014, p. 181-182.

SILVA, J. A. Q. C. Código de Defesa do Consumidor: Anotado e legislação complementar. 3. ed. São Paulo: Saraiva, 2003

STJ. Supremo Tribunal de Justiça. RE 1.745.657 – SP 2018/0062504-5. Min. Nancy Andrighi, Julgado em 03/11/2020, Dje: 17/11/2020. Disponível em: <https://www.migalhas.com.br/arquivos/2021/3/87398432fa85bb_emailstjmicrosoft.pdf>. Acesso em 10 mar. 2021.

TEIXEIRA, Jayme Filho. Comercio Eletrônico. Senac nacional. 2001. ISBN 85-8786-408-4

TIAN, Y.; & STEWART, C.M. History of E-Commerce, 2006, p. 177-289.

TURBAN, E.; LANG, J.; LAI, L.; KING, D. Introduction to electronic commerce (2nd ed.). Upper Saddle River, NJ: Prentice Hall, 2009.

VENOSA, S. S. DIREITO CIVIL: responsabilidade civil. São Paulo: Atlas, 2012. 353 p.

VENOSA, Sílvio de Salvo. Direito civil: responsabilidade civil. 3. ed. São Paulo: Atlas, 2003. v. 4.

WARREN, S. D.; BRANDEIS, L. D. The Rights to Privacy. Harvard Law Review, v. 5, p. 193-220, 1980.

Sites Consultados

KARR, D. 20 Key Factors Impacting E-Commerce Consumer Behavior. MARTEC.ZONE, 2019. Disponível em: < https://martech.zone/e-commerce-consumer-behavior/>. Acesso em 08 mar. 2021.

TOREZANI, N. O crescimento do e-commerce no Brasil. E-Commerce BR. Disponível em: <https://www.ecommercebrasil.com.br/artigos/o-crescimento-do-e-commerce-no-brasil/>. Acesso em 06 mar. 2021.

E-commerce brasileiro faturou R$ 61,9 bilhões em 2019, 16,3% acima de 2018. Redação E-Commerce Brasil. Disponível em: < https://www.ecommercebrasil.com.br/noticias/e-commerce-brasileiro-faturou-r-619-bilhoes-em-2019-163-acima-de-2018/#:~:text=acima%20de%202018-,E-commerce%20brasileiro%20faturou%20R%24%2061%2C9%20bilhões%20em,16%2C3%25%20acima%20de%202018&text=O%20ano%20de%202019%20fechou,R%24%2053%2C2%20bilhões.> Acesso em 08 mar. 2021.

LISTA DE SIGLAS

CC	Código Civil
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CP	Código Penal
LGPD	Lei Geral de Proteção de Dados
RESP	Recurso Especial
RVA	Rede de Valor Agregado
SFN	Sistema Financeiro Nacional
SI	Sistema de Informação
SSL	Secure Socket Layers
SSL	Secure Socket Layers
STF	Supremo Tribunal Federal
STJ	Supremo Tribunal de Justiça
TI	Tecnologia de Informação
TIC	Tecnologia da Informação e Comunicação
TJ-AM	Tribunal de Justiça do Amapá
TJ-SP	Tribunal de Justiça de São Paulo
TJ-DF	Tribunal de Justiça do Distrito Federal
TJ-PR	Tribunal de Justiça do Paraná
TJ-RJ	Tribunal de Justiça do Rio de Janeiro
TJ-SP	Tribunal de Justiça de São Paulo