Sthéfano Bruno Santos DIVINO[1]
Taisa Maria Macena de LIMA[2]

Argumenta
Journal Law
n. 34 p. 201-226
jan/jun 2021

RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

TORT LIABILITY IN BRAZILIAN GENERAL DATA PROTECTION REGULATION

RESPONSABILIDAD CIVIL EN VIRTUD DE LA LEY GENERAL DE PROTECCIÓN DE DATOS DEL BRASIL

Como citar este artigo: DIVINO, Sthéfano, LIMA, Taisa. Responsabilidade civil na lei geral de proteção de dados brasileira. Argumenta Journal Law, Jacarezinho – PR, Brasil, n. 34, 2021, p. 201-226.

Data da submissão: 22/05//2020
Data da aprovação: 29/01/2021

SUMÁRIO:

RESUMO:

Apresenta-se como problema de pesquisa o seguinte questionamento: na Lei Geral de Proteção de Dados (LGPD) brasileira, qual a modalidade de responsabilidade civil aplicável aos entes públicos e privados no âmbito do tratamento de dados: objetiva ou subjetiva? Para devida satisfação, objetiva-se, incialmente, inserir o leitor em uma breve discussão temporal e social acerca da privacidade e do tratamento de dados. Posteriormente, abordam-se os aspectos materiais e processuais acerca do âmbito de abrangência de aplicação da LGPD. Em seguida, discorre-se o conceito de dados nos aspectos legais e doutrinários, nacional e estrangeiro, para delimitar o objeto de estudo do presente artigo. Ao final, verifica-se que embora a lei aborde expressamente acerca da responsabilidade dos atos praticados por particulares, é silente com relação à responsabilidade dos entes públicos, se objetiva ou se subjetiva. Para satisfação

1. Universidade Federal de Lavras – Brasil
2. Pontifícia Universidade Católica de Minas Gerais – Brasil

dessa dicotomia, aplica-se o recurso hermenêutico do artigo 37, §6° da Constituição Federal de 1988, designando como objetiva a responsabilidade civil desses entes. Os recursos metodológicos utilizados para a elaboração do artigo cingem-se no caráter dedutivo, e de pesquisa integrada monográfica.

ABSTRACT:

The present article intends to discuss the following question: in the Brazilian GDPR, what is the tort liability modality applicable to public and private entities within the scope of data processing: objective or subjective? For the purpose of satisfaction, it is intended, initially, to insert the reader into a brief temporal and social discussion about privacy and data processing. Subsequently, the material and procedural aspects about the scope of application of Brazilian GDPR are discussed. Next, the concept of data in legal and doctrinal aspects, national and comparative, is delineated in order to delimit the object of study of the present article. In the end, although the law explicitly addresses the responsibility of acts performed by individuals, it is silent regarding the responsibility of public entities, whether objective or subjective. In order to satisfy this dichotomy, the hermeneutic feature of article 37, §6 of the Federal Constitution of 1988, is applied, designating as objective the tort liability of these entities. The methodological resources used for the elaboration of the article are in the deductive character, and integrated monographic research.

RESUMEN:

El presente artículo pretende discutir la siguiente pregunta: en la RBP brasileña, ¿cuál es la modalidad de responsabilidad extracontractual aplicable a las entidades públicas y privadas en el ámbito del procesamiento de datos: objetiva o subjetiva? Con el fin de satisfacer, se pretende, inicialmente, insertar al lector en una breve discusión temporal y social sobre la privacidad y el tratamiento de datos. Posteriormente, se discuten los aspectos materiales y de procedimiento sobre el ámbito de aplicación del PIB brasileño. A continuación, se delinea el concepto de datos en aspectos legales y doctrinarios, nacionales y comparativos, con el fin de delimitar el objeto de estudio del presente artículo. En definitiva, aunque la ley se refiere explícitamente a la responsabilidad de los actos realizados por los

particulares, no dice nada sobre la responsabilidad de las entidades públicas, ya sea objetiva o subjetiva. Para satisfacer esta dicotomía se aplica la característica hermenéutica del párrafo 6 del artículo 37 de la Constitución Federal de 1988, que designa como objetivo la responsabilidad extracontractual de esas entidades. Los recursos metodológicos utilizados para la elaboración del artículo son en el carácter deductivo, y la investigación monográfica integrada.

PALAVRAS-CHAVE:
LGPD; 13.709/2018; Proteção de dados; Tratamento de dados; Responsabilidade Civil.

KEYWORDS:
GDPR; 13.709/2018; Data protection; Data Processing; Tort Liability.

PALABRAS CLAVE:
GDPR; 13.709/2018; Protección de datos; Procesamiento de datos; Responsabilidad civil extracontractual.

INTRODUÇÃO

A importância atribuída ao momento da construção jurídica das informações é referencialmente identificada como um anexo ao direito de privacidade. Identificado as raízes deste direito, que inicialmente foi associado à desagregação da sociedade feudal, a privacidade adquiria uma complexa série de relações ligadas ao seu caráter patrimonial (RODOTÀ, 2008, p. 26).

Em um nível social e institucional, o nascimento da privacidade como preceito jurídico se deu mais tarde. A realização de uma exigência natural adquire tal feição e deixa de ser privilégios por parte de um determinado grupo a partir do momento em que condições materiais da vida incluíram a privacidade na vida da classe trabalhadora (RODOTÀ, 2008).

Logo no início do século XIX, Warren e Brandeis (1890) lançaram o ensaio *The right to privacy*, pela Harvard Law Review. O primeiro impacto jurídico e social foi pela agregação e transformação de algo visto

como disponível e intrinsecamente patrimonial para tornar-se um direito. Warren e Brandeis foram os responsáveis pela feição jurídica da privacidade, adequando-a como um Direito.

Seu desenvolvimento tem uma significação progressista frente o século XX, porém ainda íntima. Embora a temática de tratamento de dados esteja em tônica em nossa sociedade contemporânea, a defesa da privacidade, pelo caminhar mais tímido[1] e lento em meados daquele século, ainda era discutida e construída por grandes autores. Em *Privacy Under Attack*, Madgwick (1968) enunciava horizontes sensíveis aos riscos ligados aos registros de massa. Em *The Death of Privacy,* Rosenberg (1969) dilata para uma dimensão coletiva o tradicional quadro individualista da intimidade, colocando-o sobre fatores de riscos que sublinham impedimentos e restrições materiais que impedem numerosos sujeitos de usufruir de tal direito. No cenário literário, Orwell (2009) postulava a criação do *Big Brother*, uma entidade artificial que vigiava tudo e todos para mantê-los em seu estrito controle. O principal desígnio de sua obra é a demonstração do poder dos sujeitos detentores informacionais. O mesmo pode ser verificado na obra *Panopticon* de Bentham (2000), aperfeiçoada por Foucault (2004), em *Vigiar e Punir*. Assim, apesar de a privacidade ganhar tônica em virtude da consagração do Big Data, sua construção já é datada de, ao menos, um século.

A construção e caracterização de nossa organização social fundamentada cada vez mais sobre a acumulação e circulação de informações elenca novos desafios para as ciências, em especial o Direito. o poder fundado na informação, a dificuldade de individuar certos tipos de informações acerca das quais o cidadão consente em cedê-las e a construção da privacidade ganham uma tônica neste cenário. O tratamento de dados passa a permitir novas concentrações de poder e fortalecimento dos já existentes. Com a substancial intenção de frear, ou pelo menos criar obstáculos a esse cenário, surgem as legislações destinadas à tutela e proteção dos dados pessoais na sociedade em rede (CASTELLS, 2017). Uma das primeiras e com maior patente foi a Diretiva 95/46/CE da União Europeia (1995), que inaugurou um regulamento, já na década de 1990, para o crescimento das necessidades de proteção aos escassos normativos destinados à proteção da privacidade dos sujeitos em rede, salvaguardando-se o frágil tecido dos direitos civis da personalidade[2].

Aproximadamente 20 anos após a Diretiva Europeia estar alargando as possibilidades protetivas da privacidade, ela assume um caráter mais completo e atualizado. O regulamento 2016/679, conhecido como *General Data Protection Regulation* (GDPR) insere na sociedade europeia um rico normativo frente ao seu antecessor. Tecnologias interativas que realizam a coleta e o tratamento de dados dos titulares que a utilizam passam a ser objeto de controle destes. O verdadeiro potencial e a temática passam a ser a construção do papel do cidadão na sociedade informatizada, distribuindo contingências para delimitar a aplicação do *Big Brother* de Orwell.

No Brasil (2018), a temática surgiu com o mesmo espectro, mas tardiamente. A Lei Geral de Proteção de Dados (LGPD) brasileira propõe soluções às consequências negativas da tecnologia através das disposições da Lei 13.709, de 14 de agosto de 2018. Aqui existem inúmeras normas mantendo uma nova temática dentro dos esquemas privatísticos tradicionais seguindo uma lógica protetiva de direitos da personalidade. A defesa da privacidade no sistema jurídico brasileiro alargou-se em uma perspectiva institucional e social, superando a lógica puramente proprietária e possibilitou a integração de controles individuais para com os titulares dos dados coletados e tratados.

Dentro desse mar de possibilidades, existe a responsabilidade civil pelos atos cometidos por agentes públicos e privados no âmbito do tratamento de dados. A essas considerações se estipula o problema desta pesquisa: aplica-se a responsabilidade civil trazida pela Bill 13.709/2018 a esses sujeitos na modalidade objetiva ou subjetiva? Quais são as consequências de sua incidência? A conclusão mais imediata a ser posta para satisfação dos requisitos metodológicos é a aplicação da responsabilidade objetiva, conforme disposição legal. Porém, veremos algumas peculiaridades no decorrer da construção do texto. Define-se, portanto, uma abordagem mais técnica e pragmática próxima ao empirismo do direito, típico das novas tecnologias.

Para a devida construção argumentativa e estética pleiteando os resultados, constroem-se três tópicos. O primeiro será responsável pela abordagem processual acerca do âmbito de aplicação do GDPR brasileiro. O segundo, por sua vez, trata aspectos materiais, discorrendo em uma perspectiva comparada o conceito de dados e os requisitos para sua coleta

e tratamento. Por fim, analisa-se os critérios da responsabilidade civil na LGPD brasileira, se em sua modalidade objetiva ou se em sua modalidade subjetiva, conforme dita o normativo em seus arts. 31-32 (agentes públicos) e 42-45 (agentes privados). Ao final, verifica-se que, embora a lei aborde expressamente acerca da responsabilidade dos atos praticados por particulares, é silente com relação à responsabilidade dos entes públicos, se objetiva ou se subjetiva. Para satisfação dessa dicotomia, aplica-se o recurso hermenêutico do artigo 37, §6° da Constituição Federal de 1988, designando como objetiva a responsabilidade civil desses entes. Os recursos metodológicos utilizados para a elaboração do artigo se cingem no caráter dedutivo e de pesquisa integrada monográfica.

1. ASPECTOS TERRITORIAIS

No momento em que se percebe a necessidade de uma postura que transcenda as fronteiras do país, as normatizações tendem a considerar e elaborar regras sobre circulação de informações que transcendam a ótica territorial nacional. Porém, teme-se que a amplitude exacerbada seja um empecilho para sua efetiva aplicação, pois apesar de inexistir um tratado internacional regulamento isso em âmbito coletivo, a soberania dos países envoltos na jurisdição da legislação de origem passa a ser um desafio às legislações estritamente nacionais. Porém, como muitos são os interesses que se coadunam e se amalgamam para estender essa tutela protetiva aos entes particulares, há um sentimento de colaboração implícito quando se trata de tratamento de dados.

Por esse motivo, o GPDR brasileiro adotou um critério objetivo para sua incidência, aplicando-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a) a operação de tratamento seja realizada no território nacional; b) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou c) os dados pessoais objeto do tratamento tenham sido coletados no território nacional (BRASIL, 2018).

A amplitude dessas três possibilidades é intensa. Primeiramente, devemos compreender o que a lei designa como tratamento de dados.

Isso, entende-se como toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018). Existe um critério ampliativo em que a lei designou todas as situações que se configuram como tratamento de dados. Como tal rol foi incrementado com inúmeras situações, entende-se tratar de um rol taxativo, não se admitindo ou enquadrando como tratamento de dados outras situações fora dos desígnios legais.

Em segundo lugar, o tratamento de dados deve ser realizado no território nacional; ou seja, se configurada qualquer uma das situações acima descritas, já incidirá a aplicação da LGPD. Desde a mera coleta à transferência, difusão ou extração. Desse modo, o dado pessoal tratado por uma empresa de serviço de *cloud computing* que armazene o dado fora do país terá que cumprir as exigências da LGPD (PINHEIRO, 2018, p. 30).

Em terceiro lugar, a LGPD seguiu a regulamentação previamente estabelecida na Lei 12.965/2014, conhecida como Marco Civil da Internet. Ao designar a incidência da Lei 13.709/2018 nas atividades de tratamento que ofertaram ou forneceram bens ou serviços aos particulares no território brasileiro equipara-se ao disposto no art. 11, §3° daquela legislação[3]. Contudo, sem uma restrição: a necessidade de estabelecimento, no Brasil, de uma integrante do grupo econômico que realiza a coleta e o tratamento de dados. A LGPD, portanto, foi além e dispensou tal requisito, amplificando as possibilidades da tutela processual dos dados pessoais dos sujeitos em território nacional.

Por fim, como o legislador coloca a conjunção disjuntiva *ou* entre os incisos II e III, verifica-se uma alternatividade dessas hipóteses, e não a sua cumulatividade. A última hipótese é basicamente um complemento da primeira, em que aplicar-se-á o GPDR brasileiro caso o tratamento de dados tenha como objeto dados pessoais coletados em território nacional. Aqui temos uma importante observação. A legislação designa o titular desses dados como pessoa natural identificada ou identificável. Não faz qualquer discriminação ou restrição direcionada à cidadania ou à nacionalidade dos dados, tampouco a residência do indivíduo titular (PINHEIRO, 2018). Assim, caso algum estrangeiro esteja no Brasil e tenha seus

dados tratados, aplicar-se-á o GPDPR brasileiro.

Isso, pois, a legislação assume um caráter principiológico e abrangente. É sempre a partir dessa lógica que devemos compreender os casos em que as informações pessoais venham ser utilizadas em sistemas de decisões automatizadas para verificação e aplicação da LGPD. Por um lado, isso significa que a legitimação para pedir a tutela ou a proteção desses dados se amplia de forma substancial. Por outro, verifica-se se realmente é possível completar esse objetivo frente aos aspectos de soberania dos inúmeros países envolvidos nessa rede digital. De qualquer forma, isso é temática para alguns anos, em que veremos casos e números empíricos de julgados com ou sem retorno de colaborações internacionais. O foco, neste momento, é uma análise estrita e principiológica das diretrizes da LGPD, em que só o tempo nos dirá acerca de sua eficácia.

Complementando as opções, a legislação designa que se consideram coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. E, no mais, existem situações que, embora tais dados sejam coletados no território e se enquadrem nas situações anteriormente descritas, não incida a aplicação da LGPD. São elas: I) ao tratamento de dados realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II) realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Aos litígios e danos que eventualmente surgirem com relação ao inciso I, aplica-se as disposições gerais do Código Civil (BRASIL, 2002) referente à possibilidade de cessão de dados intrinsecamente ligada aos direitos da personalidade, em conjunto com o art. 5°, X, da Constituição Federal[4]. Deve-se verificar, contudo, que tal conduta não adquire nenhum caráter remuneratório. O segundo inciso está ligado intrinsecamente aos atos de produção intelectual e liberdade de expressão, também protegidos constitucionalmente. Da mesma forma, isso não significa que não haverá

proteção desses dados, mas que será ela outorgada ao regime geral de responsabilidade civil previsto nos arts. 187 e 927 do Código Civil ou nas diretrizes do Código de Proteção e Defesa do Consumidor, caso lá se enquadre, já que, neste caso, a legislação não veda o caráter remuneratório, tal como o faz no primeiro inciso. Já com relação ao terceiro inciso, são hipóteses em que o próprio Estado utiliza e se exime para inaplicação da legislação, principalmente com escusas destinadas à segurança pública ou defesa nacional. Se verificado dentro da ponderação de interesses, o particular será subordinado momentaneamente para cessão de seus dados sem aplicação da LGPD, mas com as mesmas observações relativas ao inciso I e II, devendo o tratamento de dados ser regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. Por fim, aos dados que adentrarem o território brasileiro, em regra, não se aplica a LGPD. Porém, deverá o país de origem proporcionar um grau de proteção equivalente ao previsto na legislação brasileira. Caso contrário, aplica-se a Lei 13.709/2018.

A referência à privacidade, assim, exprime mais uma necessidade da igualdade e uma tendência bem visível de cooperação entre a legislação brasileira e estrangeira. As restrições de aplicação do normativo são poucas, principalmente visando o setor público, em que tais dados, aparentemente, seriam subjugados em detrimentos dos interesses públicos. O que se verifica é que as funções e relações particulares, que possuem uma maior assimetria entre titular, controlador e operador[5], abarcarão as maiores taxas de incidências processuais e protetivas disciplinadas pela LGPD. Portanto, definidos os termos de aplicação territorial da ilustre legislação brasileira, parte-se para análise dos requisitos indispensáveis ao tratamento de dados.

2. REQUISITOS PARA O TRATAMENTO DE DADOS: A TÔNICA DO CONSENTIMENTO

Embora o conceito de dados não esteja elencado nos termos acima, a passagem por sua definição é elementar para delimitar o que e quais são os requisitos legais essenciais. A ênfase desloca-se para a definição legal, trazida pela LGPD brasileira. Aqui, temos o conceito de dado pessoal

como informação relacionada a pessoa natural identificada ou identificável e dado pessoal sensível como aquele 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 (BRASIL, 2018).

Contudo, existem considerações doutrinárias e em outros regramentos estrangeiros de interesse para o estudo do presente artigo. Nas diretrizes do GDPR 2016/679 da União Europeia (2016):

> […] personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Para Doneda (2014, p. 61-78), dado seria algo apresentável em uma conotação mais primitiva, abstrata, fragmentada, podendo sê-lo equiparado à potencial informação, antes de ser transmitida. Ou seja, dado traduz-se em pré-informação. A informação, por sua vez, refere-se a algo além da representação abstrata e fragmentada contida no dado, chegando ao limiar da cognição e, quase como um ato reflexo, estará ligada ao direito de privacidade por uma equação que abstrai menor difusão de informações e acresce maior grau de privacidade. Definição essa inspirada em Wacks (1989). Entende esse autor dados como informações em potencial, passíveis de transformações em informações para serem comunicados, recebidos ou compreendidos. O dado é capaz de se materializar em uma palavra, estimulando o receptor sua compreensão para posterior transformação em informação; se compreendido o dado, poderá se apresentar em atos, sinais ou símbolos, sendo necessário interpretá-lo para adquirir algum sentido. O dado permanecerá como pré-informação até o momento em que alguém compreenda a mensagem nele contida e transmitida.

Nas legislações de proteção de dados latinas existem disposições semelhantes. No México (2010), por exemplo, considera-se dado "*cualquier información concerniente a una persona física identificada o identificable*". Na Colômbia (2013), "*cualquier información vinculada o que pueda aso-*

ciarse a una o varias personas naturales determinadas o determinables". Em qualquer diretriz abordada, deve-se levar em conta que a função e a tutela protetiva não é direcionada aos dados *per se*, mas ao titular, ao seu detentor (MENDES, 2014). Isso, pois, o conceito de dado passa a ser um elemento central para o aperfeiçoamento das legislações em análise, principalmente a LGPD. Aqui serão estabelecidos limites e o campo de atuação da tutela jurídica em questão. Verifica-se que a escolha legislativa se pautou por uma ótica expansionista, prescrevendo de forma sintética e principiológica o vocabulário designado para definição de dados pessoais (BIONI, 2019). Assim, a interlocução entre conceito e eficácia prática aparentemente não ficam prejudicados para com eventuais interpretações restritivas.

Dentre os requisitos indispensáveis para realização do tratamento de dados está a tônica do consentimento. O art. 7° da LGPD dispõe algumas hipóteses alternativas em que seria legítimo o tratamento de dados. Entende-se que, neste momento, como o legislador utilizou a conjunção disjuntiva *ou* no final do inciso IX deste citado normativo, se configurada qualquer uma das hipóteses presente nos demais incisos, seria autorizado o tratamento de dados, independentemente de ter ou não consentimento. Veja-se: em uma leitura hermenêutica, caso o legislador decidisse pela aplicação integral do consentimento nas demais hipóteses prescritas no normativo em questão, teria criado alíneas no inciso I, ao invés de confeccionar outros incisos. Além disso, utilizou da conjunção disjuntiva *ou*, ao tempo em que poderia ter limitado as hipóteses à confecção da primeira. Por essa razão, ainda que não haja consentimento do titular, caso fique configurada qualquer das hipóteses presentes nos incisos II ao X, será legítimo o tratamento de dados, desde que respeitados os demais princípios legislativos.

Foca-se, contudo, na hipótese mais importante, em que o consentimento é a tônica dessa relação. Apesar de a lei conceituá-lo como manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5°, XII), não designa qualquer desses termos, forçando-nos a recorrer aos atos normativos estrangeiros.

Elenca o Manual da Legislação Europeia sobre Proteção de Dados três elementos de um consentimento válido que assegura que as pessoas,

objeto de tratamento de dados, genuinamente autorizam a sua utilização. 1) a pessoa não pode estar sob qualquer pressão quando presta o seu consentimento, assemelhando-se ao disposto no art. 8°, §3° da Lei 13.709, porém este mais completo; 2) a pessoa em causa deve ter sido devidamente informada sobre o objeto e as consequências do consentimento; e 3) o âmbito do consentimento deve ser razoavelmente concreto; sendo tais requisitos aplicáveis de forma cumulativa, condicionando o consentimento válido somente se observado todos os três requisitos acima citados (UNIÃO EUROPEIA, 2014, p. 59).

O termo caráter inequívoco "significa que não devem existir dúvidas razoáveis de que a pessoa em causa pretendia comunicar a sua permissão para o tratamento de dados" (UNIÃO EUROPEIA, 2014, p. 60), sendo a mera inércia é incapaz de constituir um consentimento inequívoco. Com relação à liberdade, "será livre o consentimento se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento foi recusado" (UNIÃO EUROPEIA, 2014, p. 60).

Já direcionado ao consentimento informado, a pessoa em causa deverá possuir informações suficientes acerca do tratamento de dados antes de tomar sua decisão. A (in)suficiência das informações fornecidas somente poderá ser determinada em cada caso concreto. Como regra, essas informações deverão incluir uma descrição rigorosa e facilmente compreensível do objeto do consentimento, bem como das consequências deste se proferido e ou se recusado, devendo a linguagem ser adaptada aos destinatários previsíveis das informações (UNIÃO EUROPEIA, 2014, p. 62).

Por fim, o consentimento deve ser específico. Neste caso, caracteriza-se como a qualidade de informações fornecidas sobre o objeto do consentimento. Para tanto, será considerado o homem médio como padrão de discernimento afim de aferir a especificidade dos escritos destinados ao tratamento de dados. Além disso, se previstas novas operações ou alterações que não estavam pactuadas ou não poderiam ser previstas quando a pessoa em causa forneceu inicialmente o seu consentimento, será necessário requerer-lhe, novamente, seu consentimento (UNIÃO EUROPEIA, 2014, p. 63). No mais, o Regulamento 2016/679 formaliza a necessidade de o consentimento ser explícito, ou seja, expresso na carta

contratual destinada ao tratamento de dados. Poderá, também, a pessoa em causa revogá-lo a todo tempo, não necessitando de justificativa prévia para tanto (UNIÃO EUROPEIA, 2016).

É certo que existem estratégias que se contrapõem a tais lógicas e estruturas organizacionais legais, tal como os moldes contratuais eletrônicos contemporâneos. Estes, considerados *clickwrap*[6] ou *point-and-click* dificultam uma análise mais precisa para verificação dos requisitos acima designados. Porém, a força estruturante das novas tecnologias e sua sinergia com as legislações devem assumir uma postura para que facilite esse fato, tal como a criação de modelos contratuais específicos destinados à cessão facultativa dos dados pessoais pelo titular ao utilizar determinado serviço. Por ora não compensa adentrar nessa discussão, tendo em vista que ela constitui um problema de pesquisa aquém do inicialmente estipulado. O que se deve ter em mente, em primeiro lugar, é que o desígnio do consentimento como lócus do tratamento de dados delineia algumas tendências, principalmente principiológicas, das quais não foram esquecidas pela lei. Pelo contrário, foram elencadas em um rol específico.

Além da presença do consentimento na situação em análise, conforme o artigo 6° da LGPD, o tratamento de dados obrigatoriamente deverá respeitar alguns princípios, dentre eles a finalidade, a adequação e a necessidade. Deverá o operador ou o controlador de dados informar ao titular destes quais as finalidades designadas para com o tratamento de dados, bem como a afinidade de adequação existente entre sua atividade de tratamento de dados e sua atividade econômica. Isso, pois, a privacidade e a disciplina protetiva das informações passam a ter uma ótica mais transparente no tratamento de dados, para com aquela relação ali estabelecida, devendo aquele que realiza o procedimento definir em termos claros a participação dos dados para que o seu titular, em eventuais situações de litígios judiciais ou danos morais e materiais consiga definir onde exatamente ocorreu.

Essa postura é ainda mais nítida quando abordada nos termos dos dados sensíveis, que somente poderão ser coletados e processados nos moldes legais do art. 11 da LGPD. Eles são assim conceituados e particularmente protegidos contra os riscos da circulação em virtude de seu potencial inclinação a serem utilizados com finalidades discriminatórias[7]

(RODOTÀ, 2008, p. 90).

Esses rápidos tracejos mostram que, para além do reconhecimento dos direitos individuais, os normativos destinados à regulamentação da circulação de informações em âmbito virtual determinam e designam a autonomia privada como um forte requisito que deve estar presente nas situações elencadas. Isso, pois, as informações obtidas, originalmente fornecidas, podem acarretar danos patrimoniais e extrapatrimoniais em seu titular caso sejam utilizadas de forma errônea. Aqui concentra-se o problema de pesquisa do presente artigo. Caso um agente público ou particular cometa algum dano ao titular dos dados em uma operação de tratamento de dados, qual será a modalidade de responsabilidade que deverão responder: objetiva ou subjetiva?

3. RESPONSABILIDADE CIVIL PELOS ATOS DOS AGENTES PÚBLICOS E PRIVADOS NA LEI GERAL DE PROTEÇÃO PRIVADA BRASILEIRA

Pode ser que entre a circulação das informações entre o ambiente contratual, inicialmente restrito aos contratantes, e o sólido mercado, a proteção de dados fique prejudicada por algum motivo e cause danos ao seu titular. Uma intervenção legislativa nesse aspecto é pontual, e a LGPD não deixou transpassar o assunto. Não se pode efetivamente duvidar que os interesses ligados à proteção de dados pessoais estejam ligados intimamente aos direitos da personalidade. Estabelecer determinadas obrigações aos agentes ilícitos parece ser, no mínimo, algo legítimo e decisivo para o pleito compensatório. Como estamos falando de direitos da personalidade, em suma, os danos decorrentes do tratamento de dados aparentam ser de ordem exclusivamente moral. Ocorre que, em virtude de alguma negligência, imprudência ou imperícia ou, até mesmo, ato doloso do controlador ou do operador dos dados o ato ilícito cometa algum dano de ordem material, como é o caso de vazamento de dados bancários sigilosos, incluindo contas e senhas.

Pode-se verificar, portanto, que ambas as esferas, material e imaterial, estão protegidas por eventuais danos que venham a acometê-las. Agora, quais são as diretrizes específicas da legislação com relação a isso? A LGPD distingue duas situações: 1) do tratamento de dados pessoais pelo poder público (arts. 23-30) com sua respectiva seção de res-

ponsabilidade (arts. 31 e 32); e 2) dos agentes de tratamento de dados pessoais, com sua respectiva seção de responsabilidade (arts. 42-45). Apenas por essa primeira inferência, podemos verificar que a legislação optou por uma separação dos sujeitos de direito, em seu âmbito público e privado. Como existe essa dicotomia aparente na legislação, embora doutrinariamente seja questionável com fundamentos na unicidade do direito, o legislador também optou pela separação da responsabilidade civil desses entes. Sob o espectro hermenêutico, portanto, podemos afirmar que a responsabilidade civil dos atos praticados pelo poder público será, a princípio, tutelada pelos artigos em seu respectivo capítulo (arts. 31 e 32), enquanto a responsabilidade dos particulares pelos arts. 42 ao 45. E quais são as consequências disso?

Primeiramente abordaremos as situações envolvendo os particulares (arts. 42-45). Em complemento ao inicialmente estipulado anteriormente, o controlador ou o operador que, em razão do exercício da atividade de tratamento de dados, causar ao titular dos dados, dano moral, individual ou coletivo, violando o GPDR brasileiro, será obrigado a repará-lo. Neste prisma, a legislação brasileira reconhece a possibilidade da existência de danos coletivos pelos atos ilícitos causados pelo controlador ou operador. Exemplifica-se como o vazamento de dados pessoais que deveriam ser tutelados por instituições financeiras.

No mesmo sentido, para assegurar a efetiva indenização ao titular dos dados pelos danos inicialmente acometidos, o operador responderá de forma solidária pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados, ou quando não tiver seguido as instruções lícitas do controlador. Além disso, os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados também responderão solidariamente. Nessas duas últimas hipóteses, existem excludentes de responsabilidade, mas são ocasiões específicas que serão delimitadas oportunamente.

Como nesse tipo de relação contratual, em geral *clickwrap*, temos partes em grande desigualdade, seja técnica, econômica ou jurídica, ou seja, vulneráveis, poderá o juiz de direito, durante a análise do caso concreto, verificar tal situação e inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiente para fins de produção de prova ou quando a produção de pro-

va pelo titular resultar-lhe excessivamente onerosa. A inspiração deste dispositivo é a mesma presente no art. 6°, VIII do Código de Proteção e Defesa do Consumidor. Trata-se da chamada inversão *ope judicis*. Não se configura distribuição do ônus da prova. Essa está regulamentada, como regra, no art. 373, I, do CPC/2015, cabendo ao autor provar os fatos constitutivos de seu direito. porém, como estamos diante de uma relação de extrema vulnerabilidade, admite-se a inversão probatória a critério do magistrado, que poderá ser realizada, preferencialmente, na fase de saneamento do processo.

Em uma pequena analogia ao direito do consumidor, através do diálogo das fontes, como a inversão do ônus da prova adquire um caráter procedimental, poderá ela ser realizada, inclusive, nos tribunais de segunda instância. Porém, para evitar eventuais prejuízos para a parte que deveria produzi-la e não o fez, sua estipulação durante o saneamento processual é mais pertinente. Trata-se de uma tendência determinada por fenômenos interdependentes: de um lado a proteção e defesa dos titulares dos dados e de outro a verificação do excessivo poderio econômico, técnico ou jurídico do controlador ou operador. Em uma situação comum, a vulnerabilidade técnica é a mais verificável, pois os procedimentos algorítmicos existentes para realização do tratamento de dados somente podem ser compreendidos por aqueles que o realizam.

Prosseguindo, o inciso 3° permite que as ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput do normativo em questão podem ser exercidas coletivamente em juízo. Aqui, caso fique verificado danos a interesses sociais e individuais indisponíveis, entende-se pela possibilidade de ingresso do Ministério Público como agente de defesa da ordem jurídica, nos termos do art. 127 da CRFB c/c art. 178 do CPC/2015.

Uma importante consideração também resguardada pela LGPD é a possibilidade de regresso de um dos operadores ou controladores de dados que compensaram ou repararam o dano ao titular dos dados. Trata-se da modalidade de sub-rogação presente nas diretrizes gerais do código civil, mas que a lei preferiu esclarecer que deverá tal responsabilização ser regredida na medida da participação no evento danoso. Então, se verificada uma culpa pequena ou mínima diante de um extenso dano cometido por um concurso de agentes, aquele que vier a compensar ou reparar o

dano deverá agir em regresso aos demais na medida de sua culpabilidade. Portanto, entende-se que deve analisar os graus de culpa (se leve, média, grave ou gravíssima) dos agentes envolvidos.

O principal ponto que é pertinente ao discorrer argumentativo do presente artigo é o que está delimitado no art. 43 da LGPD. O caput diz expressamente que "os agentes de tratamento só não serão responsabilizados quando provarem [...]". Ora, a própria legislação delimitou as hipóteses excludentes de responsabilidade para os atos ilícitos cometidos pelos agentes. Entende-se, dessa forma, que a responsabilidade pelos ilícitos praticados pelos controladores e operadores particulares no tratamento de dados é, em regra, objetiva. Isso quer dizer que não se analisa culpa (negligência, imprudência ou imperícia) para eventual esquiva reparatória ou compensatória. Os agentes somente serão isentos da responsabilidade civil quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

A primeira hipótese é mais nítida. Naqueles casos em que ao agente é imputado um ilícito, poderá ele se esquivar alegando e comprovando de forma fática e jurídica que o tratamento realizado não foi de sua autoria. A segunda situação é mais complexa, pois embora o titular dos dados tenha feito todos os procedimentos em rigor ao GPDR, causou danos ao titular. Mesmo nesse caso, será o agente escuso da compensação ou reparação dos danos. Entende-se, a princípio, que os casos fortuitos ou de força maior se enquadrariam neste inciso[8]. Por fim, caso o titular dos dados atue exclusivamente de forma culposa, cedendo sua senha ou seus dados pessoais para um terceiro que venha acometer algum dano a ele, o controlador e o operador também não deverão ser responsabilizados por esses atos. Como a LGPD estipulou culpa exclusiva, em qualquer caso que haja culpa concorrente entre o titular dos dados e o controlador/operador que não se enquadre nas hipóteses dos incisos I ou II, serão estes responsabilizados.

Uma última consideração é que o GPDR brasileiro resguardou que as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas no

CDC. Aqui, como temos uma teoria do diálogo das fontes extremamente fortes, entende-se que deve aplicar este artigo com apenas uma observação: às situações jurídicas que o CDC fornece uma melhor resolução para aquela situação ilícita restringe-se a esse normativo. Contudo, nos casos em que a lei de proteção de dados oferecer uma proteção de grau equivalente ou maior, deve-se aplicar o diálogo das fontes e, se possível, amalgamar os dois normativos para garantia da efetiva proteção do titular dos dados.

Dessa forma, verificada a responsabilidade objetiva dos agentes particulares envoltos nos atos ilícitos do tratamento de dados, passa-se à análise da responsabilidade do tratamento de dados pessoais pelo poder público. Nessa situação, a legislação foi bem sintética e abstrata, discorrendo sobre o assunto em apenas dois artigos. O primeiro afirma que "quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação". Já o segundo descreve e advoga que "a autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público" (BRASIL, 2018).

O particular interesse é que o normativo brasileiro nada dispõe acerca da modalidade de responsabilidade para os entes públicos, se objetiva ou se subjetiva. Como a responsabilidade objetiva advém de uma prescrição legal, não podendo sê-la subentendida ou presumida, a princípio parece que, nesse caso, deverá ser aplicada sua modalidade subjetiva. Aqui, portanto, deveria verificar se houve participação de culpa no ato do poder público que eventualmente causou dano ao titular dos dados. Toda a remissão que a legislação faz para a Autoridade Nacional de Proteção de Dados é referente às tutelas inibitórias. Não trata, sequer, de eventuais danos materiais ou imateriais, individuais ou coletivos acometidos pelo Estado. Isso, parece ser problemático.

A solução hermenêutica encontrada é salvaguardar-se na própria constituição. A administração pública deve seguir diretrizes principiológicas pautadas na legalidade, impessoalidade, moralidade, publicidade e eficiência. Além disso, existe uma peculiaridade muito importante no art. 37 da CRFB que preencherá a lacuna deixada pela LGPD. Não cremos

que fora lacuna, talvez tenha sido algo intencional do legislador para esquivar o poder público de eventuais indenizações. Porém, prescreve o art. 37, §6° que "as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa". Ora, se estamos falando em coleta e tratamento de dados pelo poder público, através de uma pessoa jurídica de direito público, ou mesmo de direito privado prestadoras de serviços públicos, todas elas se submetem a esse normativo. Portanto, embora a legislação não tenha tratado expressamente da modalidade de responsabilidade desses entes, por força do normativo supracitado deverá ela também ser objetiva.

E quais são as hipóteses excludentes de ilicitude? Neste sentido o legislador se esqueceu e não elencou. Portanto, entende-se que em qualquer hipótese em que o poder público seja o responsável pelo tratamento de dados e algum dano venha a ser cometido ao titular desses dados em virtude dessa prática, a administração pública responderá de forma objetiva, sem análise de culpa.

Uma observação deve ser feita com relação aos moldes teóricos da responsabilidade civil adotados pelo legislador. Na esfera da responsabilidade objetiva são duas teorias predominantes no ordenamento jurídico brasileiro. Em primeiro lugar, a responsabilidade objetiva pelo risco da atividade. Nesse caso, pauta-se a atribuição do ônus indenizatório ao agente causador do dano em razão do risco que sua atividade produz socialmente. Tal modalidade é adotada tanto pelo Código Civil, em seu art. 927, parágrafo único[9], bem como pelo CDC, quando positivas as normas relativas à proteção e à segurança do consumidor, em seus arts. 8°-10°. Nesse sentido, admitem-se excludentes de responsabilidade civil próprias que são capazes de romper com o nexo de causalidade entre o dano e o agente que o sofreu. Verificam-se algumas hipóteses, por exemplo, no fato acometido por culpa exclusiva da vítima, ou mediante atuação de fato exclusivo por terceiros. No CDC essa hipótese pode ser vislumbrada no art. 12, §3°, III, quando dispõe que: "o fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar a culpa exclusiva do consumidor ou de terceiro".

Lado outro, a teoria da responsabilidade civil em sua modalidade

do risco integral tem como preceito ontológico a mesma disposição do risco da atividade. Contudo, não se admitem hipóteses de excludentes de ilicitude. Ainda que se enquadre nos casos acima explicitados (culpa exclusiva da vítima ou culpa de terceiro), o agente causador do dano, ainda que sem *culpa lato sensu*, será obrigado a reparar ou compensar o dano acometido. Tal disposição é comumente utilizada no direito ambiental, nos termos do art. 14, §1°, da Lei 6.938/1981 (BRASIL, 1981), que dispõe sobre a Política Nacional do Meio Ambiente, nos seguintes termos:

> Art 14 - Sem prejuízo das penalidades definidas pela legislação federal, estadual e municipal, o não cumprimento das medidas necessárias à preservação ou correção dos inconvenientes e danos causados pela degradação da qualidade ambiental sujeitará os transgressores:
>
> § 1º - Sem obstar a aplicação das penalidades previstas neste artigo, é o poluidor obrigado, independentemente da existência de culpa, a indenizar ou reparar os danos causados ao meio ambiente e a terceiros, afetados por sua atividade. O Ministério Público da União e dos Estados terá legitimidade para propor ação de responsabilidade civil e criminal, por danos causados ao meio ambiente.

Com relação à aplicação dessas teorias na LGPD, o legislador considerou o risco que a atividade carrega consigo, já que direcionada em sua grande parte a direitos da personalidade, mas relativizou as hipóteses de responsabilidade, positivando algumas excludentes de ilicitude e consagrando a Teoria do Risco Objetivo no art. 43 da referida legislação:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
>
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
>
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (BRASIL, 2018).

Assim, embora a proteção de dados esteja ligada intrinsecamente a direitos indisponíveis, caso os agentes de tratamento de dados comprovarem as hipóteses descritas no art. 43, serão eles eximidos de responsabi-

lidade. Contudo, ressalva-se que tais hipóteses não são taxativas. Embora o texto do referido dispositivo se exaure nas três hipóteses elencadas, por força do art. 45[10], quando se tratar de relação consumerista aplicar-se-ão as normas contidas no CDC, principalmente as regras voltadas à responsabilidade pelo fato do produto, bem como a utilização do diálogo das fontes para as demais legislações compatíveis com a LGPD.

Dessa forma, o problema de pesquisa incialmente estipulado fora satisfeito: a responsabilidade pelos atos cometidos, tanto pelos agentes públicos, quanto por agentes privados, é objetiva. No primeiro caso, por força constitucional do art. 37, §6°. No segundo caso por força do art. 43 da LGPD. Eventualmente poderão e irão surgir novas interpretações e hermenêuticas variadas. Creio que, porém, em todas elas, a proteção da privacidade e dos dados pessoais, em conjunto com a personalidade da pessoa natural deverá ser o centro argumentativo e a tônica construtiva.

CONSIDERAÇÕES FINAIS

Observando a utilização dos dados pessoais, é possível descobrir quais são os poderes que se manifestam nos titulares e na sociedade que os utilizam no tratamento de dados. A diversidade das dinâmicas traz contingências que devem ser estruturadas e sanadas para evitar a fragmentação do sujeito. O problema de pesquisa inicialmente proposto foi: aplica-se a responsabilidade civil trazida pela Lei 13.709/2018 aos agentes públicos e privados responsáveis pelo tratamento de dados na modalidade objetiva ou subjetiva?

Para a efetiva consagração da resposta delineamos, primeiramente, o âmbito de abrangência da legislação brasileira. Verificou-se que, em virtude de sua análise protetiva, pleiteando garantias adequadas para todos e quaisquer cidadãos presentes no território nacional, e que são alvos do tratamento de dados, confia-se a uma ampla abrangência, sendo que não poderá ela ser aplicada nas hipóteses do art. 4°, discorrido anteriormente. Em segundo lugar, abordou-se o conceito de dados, delimitando conceitualmente um dos objetos do presente estudo. A delimitação técnica revela caminho que conduz a renovadas formas de avanço científico, principalmente dentro do Direito. Fez-se um estudo comparativo sobre as definições em âmbito internacional e no aspecto doutrinário, demonstrando que tanto as referências legislativas destinadas aos assuntos de âm-

bito nacional quanto internacional se constroem através de uma definição ampliativa, tentando abarcar todo e qualquer tipo de dado presente e extraído do titular. Lado contrário, a definição de tratamento de dados é limitada, elencada exaustivamente em lei, pelo menos na LGPD, assim entendemos. Justamente para evitar que processos semelhantes, fora das situações descritas, configurem-se como tanto.

Por fim, para satisfação da problemática inicial abordamos os arts. 31-32 e 42-45 da LGPD. Com relação aos atos ilícitos praticados pelos particulares, temos que a responsabilidade é objetiva, pois expressa no art. 43 as hipóteses em que tais sujeitos não serão responsabilizados apenas se provarem as situações ali descritas. Nesse sentido, não se verifica culpa ou dolo, apenas a incidência deste instituto se contabiliza. Lado outro, a legislação é omissa com relação aos atos ilícitos cometidos pelos entes públicos no tratamento de dados. Em um primeiro momento, aparentemente a responsabilidade parece ser subjetiva, pela ausência de descrição e tipificação específica legal na LGPD. Demonstrou-se que, contudo, se realizada uma interpretação hermenêutica através do método hermenêutico concretizador, utilizando-se também o diálogo das fontes, a própria constituição federal, em seu art. 37, §6°, delimita a responsabilidade na modalidade objetiva para os entes de direito público pertencentes ao quadro administrativo. Por essa razão, embora a legislação esteja silente quanto aos moldes da responsabilidade dos entes públicos, entende-se pela aplicação objetiva, não admitindo-se hipóteses de excludentes em virtude do silêncio do legislador acerca do tema.

Em todo caso, são riscos concretos que tanto o agente controlador/operador e o titular dos dados sofrem nesse tipo de atividade. A internet e suas transformações. As tecnologias da informação e da comunicação podem tornar mais práticas as tarefas da vida cotidiana, mas trazem consigo amplas possibilidades, que vão desde à opacidade à transparência. Dentre essas opções, pleiteamos pela última, em que governo e administração pública, em conjunto com particulares, sejam quaisquer suas posições devem atuar em conjunto para que as múltiplas experiencias digitais se deem de forma contínua e com sinais de democracia. Em todo caso, o posicionamento e a interpretação aqui adotados é apenas uma das múltiplas portas hermenêuticas que tendem a se abrir nos futuros próximos. Esperemos que nenhuma delas se fechem.

REFERÊNCIAS

BRASIL. **Constituição Federal**. Brasília: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 11 abr. 2019.

BRASIL**, Lei 6.938**, de 31 de agosto de 1981. Dispõe sobre a Política Nacional do Meio Ambiente, seus fins e mecanismos de formulação e aplicação, e dá outras providências. DF: 31 ago. 1981. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: Acesso em: 10 nov. 2019.

BRASIL. **Lei 10.406**, de 10 de janeiro de 2002. Institui o código Civil. Diário Oficial da República Federativa do Brasil. Brasília, DF: 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 11 abr. 2019.

BRASIL**. Lei. 13.709**, de 14 de agosto de 2018. Diário Oficial da República Federativa do Brasil. Brasília, DF: 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-

2018/2018/lei/L13709.htm>. Acesso em: Acesso em: 11 abr. 2019.

BENTHAM, Jeremy. **O panóptico**. Belo Horizonte: Autêntica, 2000.

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

CASTELLS, M. **A sociedade em rede**. Trad. Roneide Venancio Majer. 18. ed. São Paulo: Paz e Terra, 2017.

COLÔMBIA. **Ley Estatutaria** *1581 de 2012 Reglamentada parcialmente por el Decreto Nacional 1377 de 2013: por la cual se dictan disposiciones generales para la protección de datos personales*. Disponível em: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>. Acesso em: Acesso em: 11 abr. 2019.

DE CUPIS, Adriano. **Os Direitos da Personalidade**. São Paulo: Quorum, 2008.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães (Org.). **Direito Privado e Internet**. São Paulo: Atlas, 2014.

FOUCAULT. Michael. **Vigiar e punir**. 29. ed. Petrópolis: Vozes, 2004.

FRANÇA, Rubens Limongi. Direitos da personalidade: coordenadas fundamentais. **Revista dos Tribunais,** São Paulo, v. 72, n. 567, p. 37, jan. 1983.

MADGWICK, D. **Privacy under attack**. London: National Council for Civil Liberties (NCCL), 1968.

MARTINS, Guilherme Magalhães (Org.). **Direito Privado e Internet**. São Paulo: Atlas, 2014.

MARTINS, G. G. **Contratos Eletrônicos de Consumo**. 3. ed. São Paulo: Atlas, 2016.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MÉXICO. **Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 5 de julio de 2010.** Disponível em: <www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>. Acesso em: Acesso em: 11 abr. 2019.

MILLER, A. R. **The assault on Privacy**: computers, data banks and dossiers. New York: New American Library, 1972.

ORWELL, George. **1984.** São Paulo: Companhia das Letras, 2009.

PARENT, W. A. **Recent work on the Concept of privacy**. *American Philosophical Quarterly,* n. 4, vol. 20, p. 341-355, oct. 1983.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

RODOTÀ, S. **A vida na sociedade da vigilância***:* a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSENBERG, J. M. **The Death of Privacy**. New York: Random House, 1969.

UNIÃO EUROPEIA, Agência dos Direitos Fundamentais. **Manual da Legislação Europeia sobre Proteção de Dado***s*. Luxemburgo: Serviço das Publicações da União Europeia, 2014, p. 39. Disponível em: <https://rm.coe.int/16806ae65f>. Acesso em: 11 abr. 2019.

UNIÃO EUROPEIA, **Directiva 95/46/CE do Parlamento Europeu e do Conselho**. 1995. Disponível em: <http://eur-lex.europa.eu/legal-content/

PT/TXT/?uri=celex:31995L0046>. Acesso em: 11 abr. 2019.

UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho**. 2016. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: Acesso em: 11 abr. 2019.

WACKS, Raymond. **Personal information**: privacy and the law. Oxford: Clarendon Press, 1989.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, 1890.

'Notas de fim'

1A abordagem da privacidade, até então enclausurada desde o ensaio The Right to Privacy de Warren e Brandeis (1890), retomou os rumos de sua construção teórica indicando que "any adequate definition of privacy must allow for the possibility that persons can exibit a lack of respect fot their on" (PARENT, 1983, p. 341-355).

2Personalidade refere-se a "uma suscetibilidade de ser titular de direitos e obrigações jurídicas" (DE CUPIS, 2008, p. 19). Os direitos a ela atribuídos são "faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem assim seus prolongamentos e projeções" (FRANÇA, 1983, p. 37).

3Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 2o O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. (BRASIL, 2014)

4X - 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).

5V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

6"Como modalidade particular de contratos de adesão, no campo da contratação eletrônica, impende destacar as chamadas licenças clickwrap ("clickwrap agreements" ou "point-and-click agreements"), usualmente submetidas à concordância do usuário do produto ou serviço, contendo cláusulas acerca da sua prestação, sendo assim denominadas, pois sua validade se baseia no ato de apertar o botão de aceitação (frequentemente por intermédio do mouse), guardando grande similitude para com as licenças shrinkwrap utilizadas na comercialização de software, nas quais a aceitação ocorre no ato da abertura da embalagem que contém os suportes físicos onde se encontra o programa" (MARTINS, 2016. p. 131).

7O art. 6º, IX, da Lei nº 13.709/2018 assim dita: IX - não discriminação: impossibilidade

de realização do tratamento para fins discriminatórios ilícitos ou abusivos; (BRASIL. 2018).

8Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

9Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (BRASIL, 2002).

10Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.