Revista Brasileira de Direito Civil em Perspectiva

Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 30.07.2022
Aprovado em: 11.09.2022

CONTORNOS SOBRE A RESPONSABILIDADE CIVIL DAS GRANDES EMPRESAS DE TECNOLOGIA "BIG TECHS"EM CASOS DE VIOLAÇÃO AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

Fabrício Veiga Costa[1]
Frederico Kern Ferreira Bastos[2]
João Manoel Miranda Gomes dos Santos[3]

Resumo: O objetivo da pesquisa é investigar a possibilidade de responsabilidade civil das *big techs* quanto à utilização indevida e abusiva de dados de pessoas físicas e jurídicas para fins comerciais, políticos e econômicos. A escolha do tema é relevante sob o ponto de vista jurídico, haja vista que dialoga com as premissas do Estado Democrático de Direito. Por meio da pesquisa teórico-bibliográfica e documental concluiu-se pela responsabilidade civil objetiva das grandes empresas de tecnologia pelo uso indevido de dados de pessoas, adotando-se como critério de quantificação do dano a teoria do *punitive damage*.

Palavras-chave: Responsabilidade civil; *Punitive damage*; Big techs; Proteção de dados; LGPD.

OUTLINES ABOUT THE CIVIL LIABILITY OF LARGE "BIG TECHS" TECHNOLOGY COMPANIES IN CASES OF BREACH OF THE FUNDAMENTAL RIGHT TO DATA PROTECTION

Abstract: The objective of the research is to investigate the possibility of civil liability of big techs regarding the improper and abusive use of data of individuals and legal entities for commercial, political and economic purposes. The choice of theme is relevant from a legal point of view, given that it dialogues with the premises of the Democratic State of Law. Through theoretical-bibliographic and documentary research, it was concluded that the large technology companies are objectively liable for the misuse of personal data, adopting the punitive damage theory as a criterion for quantifying the damage.

Keywords: Civil responsability; Punitive damage; Big techs; Data protection; GDPR

1. Introdução

[1] Professor do Programa de Pós-graduação *Stricto Sensu* em Proteção dos Direitos Fundamentais pela Universidade de Itaúna. Doutorado e mestrado em Direito Processual. Pós-doutorado em psicologia e educação. E-mail: fvcufu@uol.com.br
[2] Mestrando em Proteção dos Direitos Fundamentais pela Universidade de Itaúna. E-mail: fredericobarros.adv@gmail.com
[3] Advogado e especialista em Direito no Estado de Minas Gerais. E-mail: joaomanoelmgsantos@gmail.com

O objetivo geral da pesquisa é investigar a responsabilidade civil das grandes empresas de tecnologia, denominadas "*big techs"*, recortando-se o espectro analítico no que atine à utilização e compartilhamento indevido de dados de pessoas físicas e jurídicas, sem seu consentimento prévio, para fins comerciais, políticos e econômicos. A escolha do tema se justifica em razão de sua relevância jurídica, política, social e econômica, haja vista que vivemos numa sociedade global e tecnológica, ressaltando-se que o manuseio e a utilização dos dados podem ser vistos como estratégia comercial ou política, dependendo de sua finalidade.

Inicialmente foram realizadas breves considerações sobre o microssistema jurídico de proteção de dados, evidenciando os fundamentos jurídico-legais considerados essenciais para a análise do objeto da pesquisa. Em seguida, desenvolveu-se um estudo sobre a natureza jurídica da responsabilidade civil, nos casos de violação de dados administrados pelas grandes empresas de tecnologia, de modo a delimitar a abordagem proposta e, assim, problematizar questões consideradas relevantes sob o ponto de vista jurídico-legal.

O estudo das controvérsias acerca da possibilidade de aplicação da excludente de ilicitude (força maior e fato de terceiros), no que atine especificamente à responsabilidade civil das grandes empresas de tecnologia, referente ao manuseio e à utilização indevida dos dados de terceiros, também constituiu objeto de análise da pesquisa em tela para, assim, demonstrar, de forma clara e objetiva, os desdobramentos específicos da temática exposta no campo da responsabilidade civil.

Ao final, foi desenvolvido um estudo sobre os critérios jurídico-legais de quantificação do valor indenizatório, especificando as proposições expostas no contexto da teoria do *punitive damages*, como alternativa para punir, inibir e prevenir eventuais abusos no que tange à utilização indevida e abusiva de dados pelas grandes empresas de tecnologia.

A delimitação do objeto da pesquisa apresentada ocorreu a partir da seguinte pergunta-problema: quais são os critérios e os fundamentos jurídico-legais utilizados como parâmetro para o reconhecimento da responsabilidade civil das grandes empresas de tecnologia no que tange à utilização indevida e abusiva de dados de terceiros para fins comerciais, econômicos e políticos?

Com relação à metodologia, utilizou-se da pesquisa teórico-bibliográfica e documental, mediante a adoção das análises temáticas, teóricas, interpretativas e comparativas

para, assim, viabilizar a abordagem crítica do tema em questão e, assim, apresentar as aporias existentes.

2. Breves considerações sobre o microssistema jurídico de proteção de dados no brasil

O advento da Internet promoveu profundas transformações em praticamente todos os aspectos da vida em sociedade, permitindo uma troca instantânea de informações em nível mundial, fenômeno denominado de sociedade informacional.

Essa nova sociedade informacional, ancorada no uso massivo das redes sociais, tais como Facebook, Instagram e Twitter (FIORILLO, 2015), rumam a um processo ainda não bem delineado de transformação cultural, pois cada interação virtual entre os usuários, isto é, uma curtida, um gostei ou não gostei (*like*), um comentário, é uma informação em potencial que pode ser devidamente tratada e monetizada para finalidade de direcionamento de estratégias de *marketing* e venda de produtos.

Não há dúvidas de que está em curso uma verdadeira revolução comunicativa de interação social, em que o principal instrumento de poder se tornou a gestão da informação e do conhecimento. Basta verificar que diversas empresas voltadas ao processamento de dados e tecnologia da informação, como GOOGLE, MICROSOFT E META (proprietária do *Facebook*) figuram no *ranking* das maiores empresas do mundo (LONGO, 2021).

O tratamento de dados tornou-se um ativo valioso administrado, principalmente, por um reduzido número de grandes empresas de tecnologia, denominadas BIG TECHS, que, em regime de monopólio, realizam a coleta e o tratamento dos rastros digitais deixados pelos usuários. Com isso, podem traçar perfis de consumo, estilos de vida, preferências pessoais e políticas, influenciando um grande mercado digital (BARROS, 2021).

A realidade é que a sociedade está sendo monitorada diuturnamente mediante os rastros digitais (*footprints*) que são coletados, dos quais muitos são dados pessoais de natureza sensível, utilizados sem o devido consentimento e, na maioria das vezes, sem que o usuário tenha ciência de que está involuntariamente participando de um "*big brother*" virtual com efeitos na vida real.

É raro conhecer alguém que nunca tenha recebido uma ligação ou mensagem de uma instituição financeira ou de alguma empresa de *marketing* que lhe ofereceu produtos, ainda que nunca tivesse compartilhado seus dados pessoais com essa empresa, e mesmo que nunca houvesse tido qualquer relacionamento anterior, sendo prática comum o compartilhamento e uso indevido de informações pessoais contidas em banco de dados públicos e privados.

Martin Hilbert, em entrevista para a rede BBC News, relata que não há mais privacidade no mundo virtual e as grandes empresas conhecem o usuário melhor do que ele mesmo; ele alerta que "vivemos em um mundo onde políticos podem usar a tecnologia para mudar mentes, operadoras de telefonia celular podem prever nossa localização e algoritmos das redes sociais conseguem decifrar nossa personalidade melhor do que nossos parceiros" (LISSARDY, 2017, s.p.).

Ademais, a privacidade, mais do que um direito, é uma necessidade humana para o desenvolvimento da sua personalidade, a qual não vem sendo respeitada pelas grandes empresas de tecnologia, que, em sua maioria, coletam e compartilham dados de forma ilimitada e sem qualquer limitação legal.

E o que é ainda pior, não asseguram a inviolabilidade destes dados, permitindo sucessivos vazamentos ao não prover a segurança necessária das informações sobre sua guarda, tal como aconteceu recentemente com o caso de vazamento de dados pessoais de usuários do *Facebook* em diversos países do mundo, inclusive no Brasil, com a exposição e utilização indevida por terceiros de dados de 443 (quatrocentos e quarenta e três mil) usuários brasileiros da plataforma, o que resultou na aplicação de uma multa no importe de R$ 6,6 milhões pela Secretaria Nacional do Consumidor do Ministério da Justiça (VALENTE, 2019).

Para corroborar tal afirmação, basta lembrarmos do volume de dados que podem ser armazenados e processados por ferramentas como o *"big data",* o qual foi amplamente utilizado em campanhas presidenciais recentes nos Estados Unidos, buscando traçar o perfil e a tendência dos eleitores de cada estado, influenciando sua forma de votar. Este é um exemplo para se possa compreender que a coleta de dado extrapola a mera órbita econômica, tendo papel relevante na modulação e comportamento das democracias em todo o mundo.

Portanto, não se pode ignorar os benefícios gerados pelo tratamento de dados e, na mesma medida, não se pode esquecer de que tal atividade não opera sem limites e em contrariedade aos direitos e garantias fundamentais do usuário. Assim, é pertinente a ponderação de que os dados, quando processados, são um ativo, e por reunir informações úteis e necessárias à atividade econômica geram valor, pela monetização da informação processada de forma qualificada.

Por outro lado, é preciso compreender a engrenagem que envolve a coleta de dados. Ademais, se os cidadãos não conseguem saber quais dados estão sendo coletados, quando isto está ocorrendo, invariavelmente não conseguem compreender quais as destinações destes dados e como isto afeta sua vida (FRAZÃO, TEPEDINO, OLIVA, 2020).

Nesse contexto, não obstante a inequívoca relevância dos dados produzidos no meio digital, o ordenamento jurídico brasileiro, até um passado recente, não provia correspondente proteção legal e constitucional proporcional ao seu valor material e imaterial. Os dados eram tratados como "terra de ninguém" e um espaço desregulamentado e propício ao abuso por parte das empresas de tecnologia, especialmente pela ausência de qualquer previsão, impondo sanções legais aos agentes faltosos.

Esta realidade mudou sensivelmente com a aprovação da Lei nº.13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), a qual foi um divisor de águas normativo em termos de avanço na proteção dos dados pessoais e de garantia de segurança jurídica ao usuário, não apenas no âmbito privado, mas principalmente no âmbito público.

Em linhas gerais, considerando não ser objetivo deste artigo tecer detalhes e comentários sobre o texto da LGPD, a novel legislação contemplou importantes princípios estruturantes, como o respeito à privacidade e à inviolabilidade da intimidade, honra e imagem, e encarregou-se também de conceituar e delimitar figuras como agentes de tratamento, dado pessoal sensível, dado anonimizado, etc., consoante dispõe o art.5º da Lei. Também é digna de registro a proteção especial conferida aos dados pessoais, com um capítulo destinado a regular a matéria, além de uma seção prevendo as hipóteses de responsabilização do controlador e operador.

Por sua vez, destaca-se a criação da Autoridade Nacional de Proteção de Dados (ANPD), dotada de autonomia técnica e com natureza jurídica própria de agência reguladora, com atribuição para fiscalização quanto a uso dos dados pessoais, assim como quanto ao cumprimento da legislação vigente.

Por fim, o legislador deu um passo importante ao inserir a proteção de dados pessoais no rol dos direitos e garantias fundamentais com a aprovação da Emenda Constitucional nº.115/22, o que representou elevação deste direito ao *status* de norma constitucional, portanto, não passível de reforma por se tratar de cláusula pétrea (art.60, IV, CF/88), além do inegável avanço na proteção jurídica não apenas dos dados pessoais, mas dos demais direitos e garantias fundamentais conexos a estes, tais como o direito à privacidade e a proteção da honra e imagem (art.5, X também da CF/88).

3. Natureza jurídica da responsabilidade civil em caso de violação de dados administrados pelas grandes empresas (*BIG TECHS*).

A responsabilização civil encontra-se bem delimitada no ordenamento jurídico brasileiro, contando com normatização constitucional (art.37, §7º) e infraconstitucional, a exemplo do Código Civil, consoante previsão constante dos artigos 927 e seguintes, tendo sido dedicado um título inteiro destinado regular a matéria, sem mencionar a legislação esparsa não codificada que regulamenta oportunamente a questão. Contudo, o fato social sempre anda a frente do direito, em busca de equivalência inalcançável entre o ser e o dever ser, de modo que novas situações conclamam novos debates, novos conflitos e a presença do legislador, buscando garantir um mínimo de segurança jurídica e pacificação social. É o caso da LGPD, que almejou, entre outros objetivos, garantir um mínimo de segurança e privacidade ao usuário de internet.

Porém, nos casos em que ocorre a violação a este dever de cuidado e de segurança quanto à conservação dos dados pessoais de terceiros, tal como previsto no art.6, incisos VII e VII da LGPD[4], resta saber, ou ao menos buscar diretrizes sobre qual a natureza da responsabilidade civil das grandes empresas de tecnologia (*BIG TECHS*), em caso de violação ou vazamento de dados pessoais, tal como preconiza o inciso X, do mencionado dispositivo. Gisela Sampaio e Rose Meireles (2020) alertam para a lacuna existente na LGPD, a qual poderia ter sido mais clara ao definir e delimitar a responsabilidade civil dos agentes de tratamento de dados, se de natureza subjetiva ou objetiva, considerando que fora dedicada uma seção inteira a regular a matéria. Este vazio gera insegurança e terceiriza o trabalho de delinear o instituto ao campo doutrinário.

Na visão das Autoras, pela interpretação do teor dos arts.42 e 43 da referida Lei, ao se criar o extenso rol de deveres de cuidado, não faria sentido uma responsabilização sem analisar culpa, isto é, sem averiguar se houve o descumprimento dos deveres legalmente elencados. Na verdade**, s**eria um contrassenso, pois a lógica da responsabilidade objetiva é oposta, haja vista que apenas o fato de se admitir que um dever foi descumprido já é suficiente para gerar responsabilidade civil, contrariando as premissas trazidas pela lei geral de proteção de dados. Ainda, reforçam seus argumentos afirmando que a Lei, ao adotar um regime de *standart* de condutas, ou seja, incorporando princípios como o da responsabilização e da prestação de contas, os quais devem ser observados nas atividades de tratamento de dados a luz do art.6, ou seja, ao se apresentar tais características, acaba por se aproximar mais do regime da responsabilidade civil de natureza subjetiva e, consequentemente, se afastando do regime próprio à responsabilização objetiva. Concluem sua linha de raciocínio ao relembrar a tramitação do Projeto de Lei que deu origem ao diploma em comento, o qual teve o seguinte histórico legislativo:

> A primeira pista é o próprio histórico de tramitação do Projeto de Lei que deu origem à LGPD, que mostra a opção do legislador pela responsabilidade subjetiva. A versão inicial do PL 5.276/2016 trazia no Capítulo sobre "Transferências internacionais de dados", uma regra geral expressa de responsabilidade solidária e objetiva desses agentes pelos danos causados em virtude do tratamento de dados (art. 35). Além disso, na Seção sobre

[4] 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; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

> "Responsabilidade e Ressarcimento de danos", havia uma abordagem ampla sobre os sujeitos obrigados a reparar o dano ("todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais causar a outrem dano") (art. 42), e outra regra igualmente ampla prevendo a solidariedade entre todos os agentes da cadeia de tratamento, sem qualquer distinção entre controlador e operador:[...] [n]os casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados (art. 44)[5].

Uma segunda vertente[6] doutrinária oposta a essa defende a responsabilização de natureza objetiva, com base na teoria do risco, o qual seria intrínseco à atividade de armazenamento de dados pessoais de terceiros, tendo como um dos expoentes adeptos desta visão os Autores Danilo Doneda e Laura Schertel Mendes. Ao explorar e se filiar à visão dos Autores, Caitlin Mulholland (2021) destaca a incorporação pela LGPD dos deveres de segurança e prevenção (*compliance*) insculpidos no art.6, inciso VII e VIII, e da obrigação de prestação de contas (accountability), inseridos no inciso X do mesmo dispositivo da Lei, impondo aos agentes de tratamento o dever de minimizar os riscos mediante a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais sob pena de responsabilização. A autora (2020) também lembra que a Lei faz referência à mitigação de riscos como uma capacidade do pretenso ofensor de reconhecer previamente os riscos relacionados a sua atividade e, com isso, prevenir a ocorrência de violação dos dados evitando, consequentemente, danos aos direitos fundamentais, tais como privacidade, imagem e honra dos usuários. Aduz, também, que o regime adotado pela LGPD, à luz do disposto no art.42, milita em prol da responsabilização de natureza objetiva, independente de análise de culpa ou dolo. Segundo a compreensão da autora acerca do tema:

[5] A autora complementa o histórico de tramitação do PL. 5.276/2016: Diferentemente desse primeiro texto, todas as versões subsequentes do Projeto, até a versão finalmente sancionada da LGPD, passaram a não mais mencionar, como regra geral, um regime de solidariedade ou objetividade na responsabilidade pelos danos decorrentes do tratamento de dados pessoais. A referência expressa à responsabilidade objetiva foi completamente eliminada do texto legal.

[6] Alguns autores apresentam uma terceira vertente de que a responsabilidade seria de natureza ativa ou proativa, ou seja, nem objetiva e nem subjetiva. Para explorar e conhecer melhor esta terceira vertente recomenda-se a leitura apresentado pelos autores: MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. IN: Cadernos Adenauer, volume 3, Ano XX, 2019.

> Significa dizer que os danos resultantes da atividade habitualmente empenhada pelo agente de tratamento de dados, uma vez concretizados, são quantitativamente elevados - pois atingem um número indeterminado de pessoas - e qualitativamente graves - pois violam direitos que possuem natureza personalíssima, reconhecidos pela doutrina como direitos que merecem a estatura jurídica de direitos fundamentais. (MULHOLLAND,2020, s.p.)

Também sobre a responsabilização objetiva, são válidos os seguintes apontamentos:

> A LGPD está alicerçada na ideia do risco, de modo que sua observância requer abordagem baseada nesse elemento. Assim, os agentes de tratamento são encorajados pelo texto legal à tomada proativa de medidas aptas à mitigação de riscos. [...] Se há o risco, resta aos agentes de tratamento o dever de minimizá-lo. Nesse ensejo, para a lei, a construção do programa de governança em privacidade tem alicerce nos ideais de segurança e prevenção, conforme remissão a tais princípios inserida no artigo 50, § 2º (PALHARES, 2021, p.18).

Outro argumento relevante que reforça a tese que milita a favor da responsabilização de forma objetiva é a similaridade de regime entre a LGPD e o Código de Defesa do Consumidor, a exemplo da possibilidade de inversão do ônus da prova (art.42, §2 LGPD), previsto em ambos os microssistemas, sem mencionar o teor do art.43, que se aproxima muito da redação do art.12, §3º do CDC[7], "de modo que a analogia com o Código de Defesa do Consumidor torna-se, portanto, compreensível, tanto mais caso se considera a assimetria informacional entre os titulares dos dados e os agentes de tratamento" (CUEVA, FRAZÃO, 2021, s.p.).

[7] 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.
§ 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste; III - a culpa exclusiva do consumidor ou de terceiro.

Filia-se, deste modo, ao entendimento perfilhado acima, considerando que proteger os dados pessoais atualmente significa proteger a própria personalidade jurídica e digital do usuário, identidades que se misturam ao se relacionar vida pessoal e virtual. Ademais, considerando o grau de inserção de dados pessoais no meio digital a privacidade passa a ser um valor fundamental para desenvolvimento da autodeterminação informacional e da dignidade do usuário. Não sem razão, a proteção de dados foi elevada à condição de direito fundamental, *status* já reconhecido pelo Supremo Tribunal Federal antes mesmo da aprovação da referida emenda, ao analisar a Arguição de Descumprimento de Preceito Fundamental de nº.6387/ DF (2020), na qual havia sido reconhecido o caráter de direito fundamental implícito à proteção de dados.

À luz das referidas considerações e do caráter de direito fundamental não apenas da proteção de dados, como também dos direitos a ele anexos, como a privacidade, a honra e a imagem, e dos fortes princípios estruturantes consagrados pela LGPD, tais como inviolabilidade da intimidade, o desenvolvimento da personalidade, juntamente com os padrões protetivos a serem observados pelos agentes de tratamento de dados e a exemplo da premissa de necessária transparência e segurança quanto ao manejo dos dados, não restam dúvidas quanto ao enquadramento da responsabilidade civil de natureza objetiva em caso de violação de dados por parte das *BIG TECHS*, dado o grande risco que envolve o usuário em caso de violação a estes dados, e, por outro lado, o volume de ganho financeiro, que representa a administração destes dados por essas grandes corporações.

3.1. Controvérsia sobre a possibilidade de aplicação de excludente de ilicitude relativo a força maior e o fato de terceiros.

Em razão da divergência existente entre a (in)aplicabilidade da excludente de ilicitude sobre o vazamento de dados por questões de força maior ou por fatos de terceiros, no contexto da Lei de Proteção de Dados, optou-se, neste estudo, por uma análise do instituto da privacidade sob a ótica filosófica. A definição do direito constitucional fundamental à privacidade e intimidade, no parâmetro das matérias infraconstitucionais que pesam sobre a responsabilização e ocorrência de ilicitude, será melhor compreendida partindo-se da reflexão do ato de exposição dos dados particulares nas organizações sócias, norteada pela filosofia, visto que ela tem como instrumento regente a relação do eu com mundo.

Desta forma, para uma análise da excludente de ilicitude e a possibilidade de gerar responsabilidade por ocorrência da exposição de dados privados em face do direito à privacidade, compreende-se como imprescindível a problematização da relação entre indivíduo e os complexos empresariais[8] de coleta de dados. Assim, para estabelecer as questões de excludente de ilicitude e suas responsabilidades, ou a sua aplicação direta, entende-se viável para solução desta controvérsia a necessidade de implementação de parâmetro do conceito filosófico da individualidade do eu para o mundo, que viabilizam mecanismos de gerenciamento entre o indivíduo e as grandes empresas de tecnologia, para que unilateralmente seja estabelecido de tempos em tempos a linha entre a responsabilização de atos (i)lícitos ou a exclusão de eventual violação.

A filosofia tem como objeto científico o "conjunto das reflexões particulares que buscam entender a realidade, a partir da razão" (DICIO, 2022). O desenvolvimento da problemática do direito fundamental à privacidade e intimidade, na ótica do espaço do indivíduo na relação social e seus limites de liberdade, está diretamente relacionado à identidade humana, que, por sua vez, vincula o direito fundamental na forma, modo e estilo de vida em que lidamos com as questões políticas, religiosas, profissionais no contexto social.

Diante dos critérios expostos, sob a perspectiva de uma sociedade líquida mutável[9] (BAUMAN, 2007), as esferas do privado e público, e os indicativos de transformação individual em razão do complexo social, são alterados rapidamente, a ponto de dificultar a formatação do direito à privacidade nas hipóteses de violação. Em razão da complexidade de definir cientificamente a privacidade, utiliza-se o estudo social realizado pelo filósofo Zygmunt Bauman, que tem como marco de seus trabalhos as relações sociais maleáveis, para desenvolver uma melhor compreensão do eu indivíduo, nos meios sociais (BAUMAN, 2005), estabelecendo premissas que evidenciam que no estudo do direito à privacidade não pode haver limitação conceitual.

Emergido na compreensão do trabalho social de Bauman, para analisar a excludente de ilicitude e a possibilidade de gerar responsabilidade na ocorrência da exposição de dados privados, o trabalho da professora Carissa Véliz evidencia a problematização da relação entre

[8] Grandes empresas de tecnologia.
[9] O conceito de **modernidade líquida** foi desenvolvido por **Zygmunt Bauman, que relaciona** uma nova época em que **as relações sociais, econômicas são frágeis e maleáveis**, como os líquidos. Tendo como período de iniciou após a Segunda Guerra Mundial, mas com mais evidencia a partir da década de 1960.

indivíduo e os complexos empresariais, visto que, por meio de sua obra, foram coletados diversos registros que demonstram a fragilidade dos dados particulares e como constantemente estão sendo oferecidos sem qualquer censura aos segmentos da sociedade.

Por meio deste conteúdo pode-se relacionar alguns mecanismos de violação, oportunizando, de igual forma, realizar o comparativo das violações de dados da atualidade, com o contexto do artigo "Direito à Privacidade"[10] (WARREN; BRANDEI, 1890), que descreve, nas proporções do avanço da tecnologia da época, as dificuldades na classificação e entrega do direito à privacidade, em um momento histórico em que não se discutia as relações intimas do homem e a sensibilidade do privado, demonstrando-se que a controvérsia dos contornos do que é público e privado tem-se mantido ao longo do tempo sem uma resposta objetiva.

A problemática das atividades das grandes empresas de tecnologias, em coletar dados particulares, possui elo direto com as questões do vazamento de dados, elegendo, por coerência, a sensibilidade da temática do direito à privacidade a uma intensa complexidade.

Pela conexão existente entre as atividades de coleta de dados e sua publicidade indevida, torna-se relevante delimitar o objeto de estudo proposto, associando o vinculo existente entre a coleta de dados pessoais, os serviços das redes sociais, os sistemas de assinatura, as tecnologias inteligentes e o momento em que o indivíduo sofre a violação da exposição.

Partindo deste ponto da analise eleito[11], apesar de peremptória a afirmativa de Bauman (2005, p. 16) quanto ao objetivo da construção reflexiva do conceito de identidade individual ser "alcançar o impossível", percebe-se correta tal afirmativa. Esse entendimento é seguido por alguns juristas constitucionais quando abordam a temática do direito à privacidade, visto "que não se logrou até o momento definir com precisão em que consiste o direito à privacidade, devendo refutar toda e qualquer catalogação prévia e fechada de situações que possam se enquadrar no seu âmbito de proteção" (SARLET; MARINONI; MITIDIERO 2018, p. 469).

É claro que diante da existência da pluralidade de pessoas, a tentativa, mesmo que remota, em construir conceitos sobre o direito à privacidade, objetiva o risco da autodefinição

[10] The Right to Privacy

[11] Que o instituto da privacidade será avaliado sob a ótica filosófica, posto que, a reflexão da definição do direito constitucional fundamental da privacidade e intimidade não possui delimitação.

e, assim, excluir grupos que hodiernamente fazem parte do contexto social. Logo, diante os posicionamentos indicados, é possível concluir a definição dos critérios individualidade do eu para o mundo, viabilizando o raciocínio da discussão da excludente de ilicitude na violação de dados, certo que a perspectiva da violação estará associada às questões de identidade, à ideia da exposição e ao sentimento de "pertencimento", que resulta das decisões que o próprio indivíduo toma (BAUMAN, 2005, p.17). Seguindo Bauman, o marco do que é privado, intimo, público está diretamente relacionado com as escolhas individuais e, estas escolhas, estão diretamente ligadas à (in)viabilidade da (in)aplicação da excludente de ilicitude na exposição de dados.

Partindo-se da reflexão filosófica desenvolvida, em que os contornos do direito à privacidade estão diretamente associados às escolhas do indivíduo, a negativa ou a ausência da possibilidade de escolher, monitorar, controlar os dados coletados pelas grandes empresas de tecnologia, torna-se inviável a tese da excludente de ilicitude e qualquer discussão da isenção de responsabilidade, ao passo que, na transferência do gerenciamento das informações para o indivíduo, seguindo as conclusões baseadas a reflexão filosófica, isentaria os atos de ilegalidade as empresas de tecnologia. Posto tais referências, a responsabilidade das empresas de tecnologia está correlacionada com a destinação das informações particulares coletadas. Assim, consequentemente, a forma como é coletado, comercializado os dados particulares, no comércio de informações, sem o expresso consentimento do uso das informações para os fins comerciais que são destinados, violam a orbita da privacidade, não se limitando, portanto, a excludente de ilicitude aos fatos e atos de hackeamento e violações de força maior.

Como referência à exposição dos dados privados, no trabalho da Professora Carissa Véliz, em seu livro Privacy is Power[12] a autora, por meio da pesquisa bibliográfica, relaciona diversas publicações que diante todo conteúdo possibilita deduzir a violação do universo particular e privado, através das grandes empresa de tecnologia no uso das informações pessoais coletadas na atividade comercial ilícita. Segundo informações, no comércio de dados estão sendo exportadas as instituições da sociedade de forma silenciosa, monitorando os usuários nos produtos de consumo, recolhendo todo o tipo de informação (VELIZ 2020, p. 9,10).

[12] Privacidade é Poder

Como exemplo, temos as TVs inteligentes SAMSUNG com o sistema de coleta de dados, que por meio da tecnologia chamada "reconhecimento automático de conteúdo" (ACR), foi possível verificar uma conexão por meio da TV em mais de 700 endereços de internet distintos, depois de ser usada por 15 minutos, estando previsto nos termos de adesão da política de privacidade, que expressamente as palavras faladas, inclusive de conteúdo pessoal e outras informações confidenciais, seriam capturadas e transmitidas a terceiros.

Na mesma ordem em uma publicação do jornal The Guardian (2018)[13], escrita por Sam Wolfson, constata-se que as nossas conversas são ouvidas a todo instante, conforme aconteceu com o dispositivo ALEXA da AMAZON, que capturou conversas particulares e enviou a conversa gravada para uma pessoa da lista de contatos. Diante de tais informações, a dedução que é possível desenvolver é que a constância do monitoramento das conversas particulares registradas e ouvidas por terceiros, sem qualquer filtro, refletem na reprodução de publicidade nos e-mails, nas redes sociais, em tantas outras formas que a tecnologia permite customizar a comunicação publicitária, deixando explícito que o princípio de que é inviolável a vida privada e o domicilio previsto na Constituição Federal (1988)[14], não está adequado aos comportamento adotado pelas empresas de tecnologia, na comercialização das informações monitoradas e informadas a terceiros.

Além de sermos ouvidos, o que escrevemos, clicamos é monitorado "tudo o que fazemos no Facebook é rastreado, desde o movimento do mouse, até as coisas que escrevemos e decidimos excluir antes de uma postagem (nossa autocensura)" (VELIZ, 2020, p. 11)[15], ficando ainda mais ostensivo o uso dos dados pessoais quando a reunião dos dados, possibilita influenciar uma organização social, como descrito na publicação do jornal BBC NEWS (2018)[16], pois é utilizada a publicação com base no estudo realizado por Cambridge Analytica, o gigante Facebook, que entre 2007 a 2014 processou informações pessoais de 87 milhões de pessoas, para fins políticos.

[13] Amazon's Alexa recorded private conversation and sent it to random contact

[14] Na Constituição de 1988, no seu artigo 5º incisos X e XI, apresenta-se o conceito de privacidade como direito fundamental inviolável a intimidade, a vida privada, a honra e a imagem das pessoas, assim como a inviolabilidade da casa.

[15] Everything you do while on Facebook gets tracked, from your mouse movements to the things you write and decide to delete before posting (your self-censorship).

[16] Researcher Dr Aleksandr Kogan and his company GSR used a personality quiz to harvest the Facebook data of up to 87 million people. Some of this data was shared with Cambridge Analytica, which used it to target political advertising in the US.

Assim, é possível conceber que a demanda do comercio de dados, das grandes empresas de tecnologia, sem o expresso consentimento do uso das informações coletadas, possuem valor comercial, que, por sua ordem financeira, incentiva o abuso da violação, tal como fomenta uma invasão de dados por meio de hacker, sendo possível relacionar o interesse de terceiros destas informações, haja vista que a reportagem do jornal The Guardian (2018)[17], feita pelo jornalista Dan Tynan, retrata sobre as frequentes violações do sistema na busca de informações pessoais em plataformas como o FACEBOOK, onde descreve na publicação o acontecimento de hackeamento de 14 milhões de usuários.

A relação existente entre o vazamento de dados por meio das empresas de tecnologia e por terceiros, pelo que se pode apurar, está associada diretamente ao sistema de coleta de dados particulares, ressaltando-se, ainda, que a relação entre a demanda de mercado na comercialização dos mesmos, violando em ambas as situações a órbita da privacidade, não se limita, portanto, à excludente de ilicitude aos fatos e atos de hackeamento e violações de força maior. Ou seja, a utilização de dados mapeados pelas empresas de tecnologia, para fins comerciais, sem a autorização dos usuários, constitui ato ilícito passível de responsabilidade no campo do direito brasileiro, razão essa que compromete a aplicabilidade da tese da excludente de ilicitude, tal como debatido no presente item da pesquisa científica desenvolvida.

Em conformidade com as informações bibliográficas apresentadas, é possível desenvolver a compreensão de que as grandes empresas que coletam dados particulares, como as redes sociais, representam um valor financeiro pelo poder das informações coletas, fato esse que desestimularia a implementação de políticas de preservação da privacidade, podendo construir a dedução a partir da publicação do jornal Forbes (2018)[18], escrita pelo Executivo e

[17] According to Facebook VP of Product Management Guy Rosen, attackers were able to access name and contact information for half of the hacked accounts. For 14m, the attackers were also able to scrape virtually all the other data available on members' profile pages. One million victims got away without any information being stolen.

[18] In my last Forbes post, I observed that the real reason Facebook is committed to its ad-based revenue model is that the price advertisers are willing to pay Facebook to invade users' privacy is vastly greater than the price most consumers would be willing to pay Facebook to protect their privacy. Facebook's uncanny ability to accurately target users in its vast user database to maximize advertising effectiveness has enabled the company to build arguably the best business model in the world. Facebook has achieved the trifecta of high scale and high growth and high-profit margins unmatched by any other high tech company, including Google, Amazon, Apple, and Netflix. Facebook's extraordinary financial success is captured by the mnemonic 50/50/50/500: approximating a $50 billion annual revenue run rate, growing at 50% per year with a 50% operating profit

Professor da Universidade da Columbia Len Sherman, que apresenta como referência os motivos que o Facebook nunca mudaria o seu modelo de negócio, relacionando, ainda, o porque que Zuckerberg[19] sempre tem quebrado as promessas de implementação de medidas de controle da privacidade para os usuários.

Sherman também aponta uma interessante proposição de que a receita baseada em anunciados pelo Facebook, está diretamente associada ao preço que terceiros estão dispostos a pagar pelas informações privadas, enquanto que os indivíduos que tem os seus dados violados não estão dispostos a pagar pela preservação de sua privacidade, o que tem segmentado o mercado da companhia em uma avaliação de US$ 500 bilhões de dólares, deixando claro que empresas com o modelo de negócio, como o do Facebook, ao implementar políticas de restrições dos dados, inversamente estará reduzindo os lucros em razão das vendas publicitárias dos dados dos usuários.

Diante a controvérsia da violação da privacidade, por meio dos sistemas tecnológicos atuais, torna-se relevante a análise comparativa do artigo de revista de direito da Universidade Harvard - "Direito à Privacidade" (WARREN; BRANDEI 1890), apesar de sua publicação ter ocorrido há 132 anos. A relevância do texto está em marco temporal histórico do contexto da sociedade em que foi escrito, visto que, os conceitos do direito da privacidade não existiam, pois era valorizada a propriedade e vida, não existindo o ramo especifico do direito fundamental à privacidade, sendo discutido a intimidade e privacidade quando houvesse a violação da personalidade por meio da honra ou por meio de lesão corporal. Logo, o texto aborda a proteção da pessoa no seu direito de "ser deixada em paz", diante do avanço da tecnologia das máquinas fotográficas, das invasões dos jornais aos recintos da vida privada e doméstica, além de outros fatores da época, contribuindo na construção da proteção à privacidade.

Além da comparação de que a tecnologia, em ambas situações violou a individualidade na sua organização do privado, pontua-se que de igual forma a atividade comercial, está associada aos incentivos da violação do direito diante a oferta e demanda (WARREN; BRANDEI 1890, p. 196)[20]. Construindo a reflexão, verifica-se que comparação

margin, generating a market cap of over $500 billion. If you were a member of Facebook's executive leadership team or board, would you want to tamper with such a money-making machine?

[19] Sócio fundador do Facebook.

[20] "In this, as in other branches of commerce, the supply creates the demand".

apresentada de que a (in)aplicação da excludente de ilicitude sobre o vazamento de dados pode ser avaliada pelos parâmetros de destinação da informação e a delimitação personalíssima do indivíduo, quanto o que entende ser público ou privado. Logo, do todo observado, percebe-se que as questões de violação a privacidade continuam sendo as mesmas ao longo do tempo, demonstrando a sensibilidade sobre a matéria durante os anos, sem uma definição adequada (WARREN; BRANDEI 1890, p. 193-195)[21] para indicar quais são os critérios para dizer onde termina ou começa o direito da privacidade.

Diante de todos os modelos de orientação, pode-se concluir que o esteio para aplicar a excludente de ilicitude sobre eventual vazamento de dados deverá ser verificado em cada caso concreto, diante dos limites individuais que cada pessoa entende ter na esteira do privado e do público. No entanto, visto a sensibilidade que tem a publicidade e a necessidade pela privacidade (WARREN; BRANDEI 1890, p. 196)[22], deve-se delimitar o espectro analítico em decorrência do avanço da civilização, parâmetros de controle dos dados coletados, desenvolvendo um gerenciamento das informações obtidas e possibilitando, assim, que cada indivíduo estabeleça os limites subjetivos do eu para o mundo público.

Por outro lado, considerando que a privacidade é um direito fundamental e partindo do pressuposto de que o parâmetros de gerenciamento não serão disponibilizados ao indivíduo para sua administração, seguindo o inciso III do artigo 43 da Lei de Proteção de Dados[23], não pode ser admitido a excludente de ilicitude diante dos atos de terceiro, posto que a ilegalidade dos monitoramentos da vida privada faz das plataformas de dados das grandes empresas de tecnologia responsáveis pelo conteúdo violado ilícito, ainda mais que tais dados são comercializados, o que se eventualmente ocorrer o hackeamento da plataforma, as informações em que não houve expresso consentimento de sua coleta, imputam a responsabilidade para a empresa mantenedora dos dados.

[21] "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society." (…) "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

[22] "The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual".

[23] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
(...) III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Assim, visto que a autonomia do indivíduo em decidir o que é seu e, o que é dado ao público, não pode conferir a qualquer outra pessoa o direito de divulgação sem o seu consentimento, destacando-se a necessidade de impedir qualquer publicação indevida, visto que este direito é "exclusivamente do indivíduo" (WARREN; BRANDEI 1890, p. 205)[24]. Independentemente se os dados particulares são hakeados ou vendidos, a violação e ilegalidade acontecem posto que, violam a privacidade no momento da coleta de informação, sem o controle destas informações por parte da pessoa que tem seus dados coletados.

4. Análise sobre o cabimento da teoria do *punitive damages* na fixação da indenização face a elevada capacidade financeira das *BIG TECHS.*

Tendo sido analisados os principais elementos que norteiam a responsabilidade civil das grandes empresas de tecnologia à luz da LGPD, é necessário se debruçar sobre a viabilidade jurídica de aplicação da teoria denominada "*punitive damages*", em caso de violação de dados por parte destas grandes multinacionais, as quais, em sua maioria, atuam em regime de monopólio.

Para se ter uma pequena noção dos valores que envolvem o mercado digital, a Alphabet, dona do Google, fechou o ano de 2021 com receita de US$ 257,637 bilhões (41% superior a 2020) e lucro líquido de US$ 76,033 bilhões (alta de 89% com relação ao ano anterior), conforme dados do site poder360 (2022), o que demonstra que o tratamento de dados é uma atividade altamente lucrativa para as empresas que atuam neste nicho de mercado, de modo que a exposição indevida de dados certamente enseja violação de ordem moral aos usuários que tiverem sua intimidade afetada.

Torna-se importante ressaltar que a utilização indevida dos dados de pessoas físicas e jurídicas constitui ofensa e violação de direitos de um número indeterminado de pessoas. Trata-se de conduta ilícita que gera repercussões coletivas, não ficando adstrita apenas ao campo meramente individual. Tais elementos devem ser levados em consideração no momento da quantificação dos danos, nos casos de responsabilidade civil.

[24] "Lord Cottenham stated that a man "is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his".

Quando se analisa os critérios de quantificação do dano decorrente da ofensa de direitos fundamentais individuais e metaindividuais, verificam-se dois posicionamentos doutrinários distintos. O primeiro entendimento é aquele que se funda na ideia de que a quantificação do dano deve ter natureza pedagógico-compensatória, de modo a evitar o enriquecimento sem causa do autor da ação. Para essa primeira corrente de pensamento, a finalidade da condenação em perdas e danos é desestimular o agente a praticar novamente a conduta ilícita, além de compensar, de forma proporcional, os prejuízos suportados pela vítima.

A segunda corrente entende que a natureza jurídica da condenação em perdas e danos deve ser punitiva, ou seja, não deve ser meramente pedagógica e compensatória. Para os adeptos dessa segunda corrente, no momento em que o magistrado for quantificar o valor das perdas e danos deverá compensar o prejuízo suportado pelas vítimas, além de punir civilmente o agente pela conduta ilícita por ele praticada. É nesse contexto propositivo que o valor da indenização, nos casos de natureza jurídica punitiva das perdas e danos, costuma ser alto o suficiente para penalizar o agente pela ilicitude por ele praticada.

Sendo a honra, a imagem e a intimidade bens e valores imateriais, aliadas à ausência de critérios legais expressos e objetivos definidores, mostra-se difícil apurar a extensão do dano e, consequentemente, a quantificação do prejuízo suportado pela vítima. Isso permite maior liberdade da inclusão do caráter punitivo neste cálculo, exorbitando a mera ideia de restituição atinente ao dano material para incluir a premissa do efeito pedagógico e punitivo apto à efetiva responsabilização do agente causador do ato ilícito (PÜSCHEL, 2007).

A reprovabilidade da conduta passa a ser fator primordial na fixação do valor da indenização, de modo que, em determinados casos específicos, em que haja danos de natureza moral, parte da doutrina tem caminhado para uma aceitação da indexação à responsabilidade civil de um caráter punitivo, que exorbite a mera seara da restituição, abandonando a literalidade do texto expresso no art.944 do Código Civil, que fixa a indenização apenas considerando a extensão do dano.

Em caso de exposição indevida de dados, diante do caráter altamente lucrativo da atividade de tratamento de dados realizada pelas grandes empresas de tecnologia, somado ao faturamento anual destas empresas, em face de tais particularidades, certamente não seria razoável uma responsabilização na qual a punição seja quantificada e adstrita à extensão do dano, especialmente considerando a tradição do Judiciário Brasileiro em fixar indenizações em quantias módicas, o que serviria como um estímulo à reiteração de condutas ilícitas em uma avaliação matemática entre custo e benefício.

Neste contexto, a aplicação de uma pena complementar faz-se necessária como um apelo ao desestímulo, calcando-se na concepção de prevenção por meio da indenização, sustentada em dois pilares independentes: primeiro, a compensação na medida do dano, e o segundo, de caráter sancionatório, buscando pelo valor da sanção desestimular que a conduta ilícita ocorra novamente (GONÇALVES, 2017).

A sanção civil, decorrente do caráter punitivo do valor da indenização, objetiva penalizar e desestimular as grandes empresas de tecnologia quanto à utilização indevida e abusiva de dados de pessoas físicas e jurídicas para fins comerciais e econômicos. Deve-se fixar o valor de indenização proporcional ao faturamento dessas empresas, de modo a puni-las civilmente, comprometendo seu faturamento e obtenção de lucros pois, dessa forma, possivelmente seriam mais cuidadosas quanto às reiteradas condutas ilícitas praticadas. Se o poder Judiciário fixar valor de indenização desproporcional ao faturamento dessas empresas, em valores considerados módicos, estimulará a prática reiterada de tais condutas ilícitas, não cumprindo o seu verdadeiro papel de desestimular a prática de condutas de utilização indevida de dados de pessoas para fins comerciais e econômico-financeiros.

2. Conclusão

O estudo da responsabilidade civil das grandes empresas de tecnologia, denominadas *big techs,* em razão da utilização indevida e abusiva de dados de pessoas físicas e jurídicas, é de significativa importância política, social, econômica e comercial. Ao longo da pesquisa demonstrou-se que tais empresas devem ser responsabilizadas civilmente pelas condutas ilícitas por elas praticadas, especificamente no que tange ao compartilhamento de bancos de dados para fins econômico-comerciais e, também, políticos.

A teoria do *punitive damage,* que tem como propósito trabalhar a natureza punitiva da quantificação da indenização no campo da responsabilidade civil, é considerada uma alternativa viável para punir e inibir a prática de condutas pelas grandes empresas de tecnologia no que diz respeito à utilização indevida de bancos de dados para fins econômico-financeiros e políticos.

A lei geral de proteção de dados trouxe regramentos específicos no sentido de regulamentar tais práticas, embora seja insuficiente em alguns pontos, como é o caso, por exemplo, da natureza jurídica da responsabilidade civil dessas empresas. Foi demonstrado ao longo da pesquisa a divergência doutrinária, quanto ao fato de se tratar de responsabilidade civil objetiva e subjetiva, ressaltando-se que o posicionamento explicitado na presente pesquisa é no sentido de adotar as premissas da responsabilidade civil objetiva, haja vista que as grandes empresas de tecnologia, pelo fato de administrarem e terem acesso aos bancos de dados, assumirão, consequentemente, o risco decorrente dessa gestão.

No momento em que as *big techs* utilizam indevida e abusivamente os bancos de dados violam os direitos dos administrados, atentando-se contra o direito fundamental à privacidade e intimidade. Além disso, essas empresas auferem lucros com a venda e compartilhamento do conteúdo e das informações contidos nesses bancos de dados, além de interferirem nos processos políticos, sociais e econômicos, constituindo-se verdadeira afronta ao Estado Democrático de Direito.

Problematizar essas questões aqui expostas é uma forma de demonstrar as falhas existentes na legislação vigente e, também, a necessidade de construir novas alternativas no sentido de proteger as pessoas contra os abusos praticados, além da imprescindibilidade de responsabilidade no campo cível tais empresas pelas condutas praticadas.

3. Referências

BARROS, Frederico Kern Ferreira. **Fake News, legislação simbólica e a proteção dos direitos fundamentais e da personalidade digital**. In.: OMMATI, José Emílio Medauar (org.). Escritos de direitos fundamentais. Belo Horizonte: Conhecimento Editora, 2021.

BAUMAN, Zygmunt, **Tempos Líquidos**, Rio de Janeiro, Jorge Zahar Editor Ltda, Ed. 2007, tradução Carlos Alberto Medeiros.

BAUMAN, Zygmunt, **Identidade: entrevista a Benedetto Vecchi**, Rio de Janeiro, Jorge Zahar Editor Ltda, Ed. 2005, tradução Carlos Alberto Medeiros.

BBC, News; **Facebook fined £500,000 for Cambridge Analytica scandal**; BBC News (British Broadcasting Corporation), British, 25 Oct 2018. Disponível em: https://www.bbc.com/news/technology-45976300. Acesso em: 12 abr. 2022 às 22:15

BRASIL; Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 abr. 2022 às 23:01.

BRASIL; **Lei nº 13,709**, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 abr. 2022 às 20:11.

BRASIL.SUPREMO TRIBUNAL FEDERAL. **ADI 6387 MC-Ref** / DF - DISTRITO FEDERAL. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade. Relator(a): Min. ROSA WEBER. Julgamento: 07/05/2020
Publicação: 12/11/2020. Órgão julgador: Tribunal Pleno
Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em 10 abr. 2022.

BRASIL. **EMENDA CONSTITUCIONAL Nº 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em 17 abr. 2022.

CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. **Compliance e política de proteção de dados.** 1. ed. -- São Paulo: Thomson Reuters Brasil, 2021.6 Mb ; ePub Vários autores. 1. ed. em e-book baseada na 1. ed. impressa.

FILOSOFIA. In: **Dicionário Online de Português**. DICIO. Disponível em: https://www.dicio.com.br/filosofia/. Acesso em: 20 abr. 2022 às 14:15.

FIORILLO, C. A. P. **O Marco Civil da Internet e o Meio Ambiente Digital na Sociedade da Informação: Comentários à Lei n. 12.965/2014**. São Paulo: SARAIVA, 2015. E-book.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] - 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

GONÇALVES, Fábio Antunes. A natureza jurídica da reparação dos danos à pessoa humana: da compensação aos danos punitivos. **Revista de Direito Privado**, vol. 78/2017, p. 145 – 168, Jun / 2017.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do Tratamento de Dados. In.: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] - 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

LISSARDY, Gerardo. 'Despreparada para a era digital, a democracia está sendo destruída', afirma guru do 'big data'. In.: **Blog BBC News**, 2017. Disponível em: https://www.bbc.com/portuguese/geral-39535650. Acesso em abril/2022.

LONGO, Laelya. Valor das 100 maiores marcas do mundo cresce 15% em 2021, taxa mais alta em 22 anos. In.: **Blog Valor Investe**, 2021. Disponível em:

https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2021/10/27/valor-das-100-maiores-marcas-do-mundo-cresce-15percent-em-2021-taxa-mais-alta-em-22-anos.ghtml. Acesso em abril/2022.
MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). **Revista Jur. Puc. Rio**, 2021. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em 10 abr. 2022.
MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?** Transcrição de ROSENVALD, Nelson; CORREIA, Atala; MONTEIRO FILHO, Carlos Edison do Rêgo; KHOURI, Paulo Roque; SCHAEFER, Fernanda. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso em 10 abr. 2022.
MUNRO, Dan; **Data Breaches In Healthcare Totaled Over 112 Million Records In 2015**; Forbes, Washington; Dec 31, 2015,09:11pm EST; Disponível em: https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/?sh=43c5c77b07fc. Acesso em: 12 abr. 2022 às 01:21.
PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. **Compliance Digital e LGPD**, 1. ed. -- São Paulo: Thomson Reuters Brasil, 2021. -- (Coleção compliance ; v. 5 / coordenação Irene Patrícia Diom Nohara , Luiz Eduardo de Almeida)6 Mb ; ePub 1. ed. em e-book baseada na 1. ed. impressa.
PODER 360. **Dona do Google fecha 2021 com US$ 76 bilhões de lucro**. 2022. Disponível em: https://www.poder360.com.br/internacional/dona-do-google-fecha-2021-com-us-76-bilhoes-de-lucro/#:~:text=No%204%C2%BA%20trimestre%20de%202021,do%20%C3%BAltimo%20trimestre%20de%202020. Acesso em 15 mar. 2022.
PÜSCHEL, Flávia Portella. A função punitiva da responsabilidade Civil no Direito brasileiro: uma proposta de investigação empírica. **Revista Direito GV**. V. 3 N. 2, p. 017 – 036, JUL-DEZ 2007.
SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel, **Curso de Direito Constitucional**, 7. ed. São Paulo, Saraiva Educação, 2018 p.469.
SHERMAN, Len; **Zuckerberg's Broken Promises Show Facebook Is Not Your Friend**; Forbes, Washington; May 3, 2022 01:38 pm EDT; Disponível em: https://www.forbes.com/sites/lensherman/2018/05/23/zuckerbergs-broken-promises-show-facebook-is-not-your-friend/?sh=1512548d7b0a. Acesso em: 13 abr. 2022 às 00:23.
TYNAN, Dan; **Facebook says 14m accounts had personal data stolen in recent breach**, hackers were able to access name, birthdate and other data in nearly half of the 30 million accounts that were affected, The Guardian, United Kingdom, Fri 12 Oct 2018 21.14 BST, Disponível em: https://www.theguardian.com/technology/2018/oct/12/facebook-data-breach-personal-information-hackers. Acesso em: 12 abr. 2022 às 21:45.
VALENTE, Jonas. Ministério multa Facebook por abuso no compartilhamento de dados In.: **Agência Brasil *on-line***, 2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-12/ministerio-multa-facebook-por-abuso-no-compartilhamento-de-dados. Acesso em 17 abr. 2022.

VÉLIZ, Carissa, **Privacy is Power**, Primeira First published, Great Britain, by Bantam Press and Imprint of Transworld Publishers, 2020. 1 p.
WARREN, Samuel D; BRANDEI, Louis D. **The Right to Privacy**, The Harvard Law Review Association, Vol. 4, No. 5, Dec. 15,1980, p. 193-220 (28 pages), Disponível em https://www.jstor.org/stable/1321160?seq=1. Acesso em 10 abr. 2022.
WOLFSON, Sam; **Amazon's Alexa recorded private conversation and sent it to random contact**, the company, which has insisted its Echo devices aren't always recording, has confirmed the audio was sent, The Guardian, United Kingdom, Thu 24 May 2018 23.09 BST, Disponível em: https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation. Acesso em: 12 abr. 2022 às 23:08.