Editorial Neogranadina

2024
Revista Prolegómenos Vol. 27(53) enero-junio ■ ISSN: 0121-182x · e-ISSN: 1909-7727 ■ pp. 123-140

DOI: https://doi.org/10.18359/prole.7053

Responsabilidade dos provedores pelo tratamento dos dados sensíveis – Uma visão de acordo com as Leis de Proteção de Dados brasileira e europeia*

Cildo Giolo Júnior[a] ■ Moacir Henrique Júnior[b] ■ Pablo Martins Bernardi Coelho[c]

Resumo: No contexto atual, marcado pela expansão digital exponencial, a responsabilidade civil dos provedores no tratamento de dados sensíveis emerge como uma área de pesquisa vital. Esta pesquisa é justificada pela necessidade imperativa de proteger as informações pessoais dos usuários, garantindo que os provedores operem dentro de um quadro legal que promova a segurança dos dados e a privacidade individual. A justificativa é aprofundada ao considerar as disparidades e convergências nos enfoques legais adotados no Brasil e na Europa, duas regiões com marcos legais significativamente desenvolvidos nesta matéria. O objetivo primordial deste estudo é analisar e comparar as estruturas legais vigentes relacionadas com a responsabilidade civil dos provedores no tratamento de dados sensíveis. Espera-se identificar as melhores práticas e possíveis lacunas nas regulamentações existentes, fomentando uma discussão crítica sobre medidas preventivas e corretivas aplicáveis. Posteriormente, será realizada uma análise comparativa crítica para destilar as semelhanças e diferenças fundamentais nas políticas de responsabilidade civil adotadas por ambas as regiões. Este

* Este artigo de investigação
Revela os resultados do desenvolvimento do projeto de pesquisa fomentado pelo Programa de Bolsas de Produtividade em Pesquisa da Universidade do Estado de Minas Gerais (Edital nº 10/2022), e também das discussões provenientes do Centro de Estudos Interdisciplinares de Direito e Inovação da Universidade do Estado de Minas Gerais, grupo de estudos certificado e mantido pelos autores.

a Pós-Doutor em Direitos Humanos pelo «Ius Gentium Conimbrigae" da Universidade de Coimbra - Portugal. Doutor em Direito pela Universidade Metropolitana de Santos. Professor Titular do Curso de Direito da Universidade do Estado de Minas Gerais e da Faculdade de Direito de Franca. Franca, Brasil. Correio eletrônico: cildo.junior@uemg.br ORCID: http://orcid.org/0000-0002-8236-2042

b Doutor en Direito e Ciência Política pela Universitat de Barcelona. Mestre em Criminologia e Sociologia Jurídico Penal pela Universitat de Barcelona. Professor Titular do Curso de Direito da Universidade do Estado de Minas Gerais. Araguari, Brasil. Correio eletrônico: moacir.junior@uemg.br ORCID: https://orcid.org/0000-0002-7226-8706

c Pós-doutorando em Direito pela Universidade Federal do Rio Grande. Doutor e Mestre em História pela Universidade Estadual Paulista. Professor Titular do Curso de Direito da Universidade do Estado de Minas Gerais. Araguari, Brasil. Correio eletrônico: pablo.coelho@uemg.br ORCID: http://orcid.org/0000-0002-7374-2051

estudo tem como objetivo contribuir significativamente para o crescente corpo de literatura legal que busca navegar pelas complexidades do mundo digital em constante evolução. A metodologia empregada nesta pesquisa será dedutiva com um enfoque qualitativo e descritivo, começando com uma revisão bibliográfica extensiva para recompilar dados secundários de literatura, legislação e casos judiciais pertinentes.

Palavras-chave: privacidade; dados sensíveis; legislação brasileira; legislação europeia; responsabilidade dos provedores

Recibido: 09/11/2023 **Aceptado:** 04/12/2023 **Disponible en línea:** 06/05/2024

Cómo citar: Giolo Junior, C., Henrique Júnior, M., & Bernardi Coelho, P. M. (2024). Responsabilidade dos provedores pelo tratamento dos dados sensíveis – Uma visão de acordo com as Leis de Proteção de Dados brasileira e europeia: A perspective in accordance with Brazilian and European Data Protection Laws. *Prolegómenos, 27(53)*, 123–140. https://doi.org/10.18359/prole.7053

Responsabilidad de los proveedores por el tratamiento de los datos sensibles – Una visión de acuerdo a las Leyes de Protección de Datos brasileña y europea

Resumen: En el contexto actual, marcado por la expansión digital exponencial, la responsabilidad civil de los proveedores en el tratamiento de datos sensibles emerge como un área de investigación vital. Esta investigación se justifica por la necesidad imperativa de proteger la información personal de los usuarios, asegurando que los proveedores operen dentro de un marco legal que promueva la seguridad de los datos y la privacidad individual. La justificación se profundiza al considerar las disparidades y convergencias en los enfoques legales adoptados en Brasil y Europa, dos regiones con marcos legales significativamente desarrollados en esta materia. El objetivo primordial de este estudio es analizar y comparar las estructuras legales vigentes relacionadas con la responsabilidad civil de los proveedores en el tratamiento de datos sensibles. Se espera identificar las mejores prácticas y posibles lagunas en las regulaciones existentes, fomentando una discusión crítica sobre medidas preventivas y correctivas aplicables. Posteriormente, se llevará a cabo un análisis comparativo crítico para destilar las similitudes y diferencias fundamentales en las políticas de responsabilidad civil adoptadas por ambas regiones. Este estudio tiene como objetivo contribuir significativamente al creciente cuerpo de literatura legal que busca navegar por las complejidades del mundo digital en constante evolución. La metodología empleada en esta investigación será deductiva con un enfoque cualitativo y descriptivo, comenzando con una revisión bibliográfica extensiva para recopilar datos secundarios de literatura, legislación y casos judiciales pertinentes.

Palabras clave: privacidad; datos sensibles; legislación brasileña; legislación europea; responsabilidad de proveedores

Provider Liability for the Handling of Sensitive Data - A Perspective According to Brazilian and European Data Protection Laws

Abstract: In the current era of exponential digital expansion, the civil liability of data handlers emerges as a crucial area of inquiry. This research is motivated by the imperative need to safeguard users' personal information, ensuring that providers operate within a legal framework that prioritizes data security and individual privacy. The imperative becomes even more apparent deepens when

considering the disparities and convergences in the legal approaches adopted in Brazil and Europe, two regions with significantly developed legal frameworks in this domain. The primary objective of this study is to analyze and compare the prevailing legal structures concerning the civil liability of data handlers. It seeks to identify the best practices and potential gaps in existing regulations, fostering critical discussions about applicable preventive and corrective measures. Subsequently, a comprehensive comparative analysis will be conducted to elucidate the fundamental similarities and differences in the civil liability policies adopted by both regions. This study aims to make a significant contribution to the growing body of legal literature that seeks to navigate the complexities of the constantly evolving digital landscape. The methodology employed in this research will be deductive, utilizing a qualitative and descriptive approach. It will commence with an extensive bibliographic review to gather secondary data from literature, legislations, and pertinent judicial cases.

Keywords: Privacy; Sensitive data; Brazilian legislation; European legislation; Provider responsibility

Introdução

> *If the invasion of privacy constitutes a legal injuria, the elementsç for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation.* (Warren, Brandeis, 1890)1

Foi apenas em 1890 que o conceito de privacidade surgiu como um direito voltado à proteção da personalidade. O marco para tal mudança foi um artigo publicado por Louis Brandeis e Samuel Warren, nos Estados Unidos, com o título "*The Right to Privacy*" que falava sobre o direito à privacidade. Por outro lado, foi somente após a Segunda Guerra Mundial que tal direito foi positivado na Declaração Universal dos Direitos Humanos da Organização das Nações Unidas, que dispõe em seu artigo 12 que "ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

Por muitos anos existiu uma limitação no que diz respeito à informação em massa. Com o surgimento da internet, tudo se modificou, influenciando desde a globalização até a personalidade das pessoas. Verifica-se, assim, que a sociedade atual conta com inovações em todas as esferas, sejam elas culturais, políticas, econômicas ou jurídicas (Giabardo, 2015). Com os avanços tecnológicos, o compartilhamento de ideais e opiniões transcendeu barreiras, expandindo o direito para além dos temas estudados nas universidades. Castells (2002), identifica este período afirmando que vivemos numa sociedade global estruturada em torno de redes digitais de informação e comunicação. Essas redes permeiam todas as esferas, conectando indivíduos, organizações e países. A internet promoveu uma difusão sem precedentes de informações, transcendendo limites e barreiras.

A internet possibilitou a difusão de dados com grande velocidade graças ao seu progresso (Tosi, 2021). A partir disso, começou-se a discutir e refletir sobre os limites desse impacto global, bem como os efeitos do ambiente digital no cotidiano. Com a circulação em massa de informações pessoais, o número de violações de dados cresceu significativamente. O direito à personalidade foi afetado devido à ampla exposição de dados individuais. Dessa forma, muitas práticas passaram a causar preocupação no âmbito jurídico, uma vez que o acesso indevido a informações pessoais se expandia (Marsico, 2022). Entretanto, ao contrário do que erroneamente se afirma, a internet não é uma terra sem lei.

Com novos estilos de vida e acesso irrestrito a todo tipo de conteúdo, de qualquer lugar do mundo (Cohen, 2012), o Direito precisou se adaptar para suprir as novas demandas. Diante de extensas e incontáveis mudanças no âmbito digital, fez-se necessário consolidar uma compreensão no campo jurídico, principalmente no que se refere à responsabilidade civil. É preciso estabelecer limites frente às inúmeras transformações ocorridas com o Direito digital.

Além disso, adaptar normas pré-existentes ao contexto atual foi de suma importância para alcançar o objetivo final. As relações interpessoais geram conflitos que precisam ser solucionados com base no Direito. Se antes a responsabilidade se dava entre duas pessoas, hoje esse número aumentou consideravelmente. Esse debate ganhou força e espaço na esfera jurídica, levantando a questão sobre a amplitude da responsabilidade civil no âmbito digital, sendo necessário analisar quem são os responsáveis pelo tratamento de dados pessoais.

A pesquisa aborda a regulação específica sobre esse tema e como ela influencia a responsabilidade civil segundo o Direito brasileiro e europeu, no que tange ao tratamento dos chamados "dados sensíveis". Com a legislação vigente, percebe-se que o número de responsáveis cresce continuamente, diante das diversas ramificações da rede. O Direito, portanto, entra em cena para fornecer respostas às inúmeras questões envolvendo provedores e usuários da internet.

1 Se a invasão de privacidade constitui uma injúria legal, os elementos para exigir reparação existem, uma vez que já é reconhecido o valor do sofrimento mental, causado por um ato ilícito em si, como base para compensação. (Warren, Brandeis, 1890)

Os marcos regulatórios de proteção de dados na Europa e no Brasil

É importante demonstrar os contextos de proteção de dados - europeu e brasileiro, visto que o foco da presente pesquisa é fazer um corte diametral, verificando como o assunto é tratado em ambas as legislações. Assim, nada mais apropriado do que demonstrar as conjunturas e realidades em que ambos os regulamentos foram gestados.

A Lei Geral de Proteção de Dados ou LGPD brasileira, foi aprovada em agosto de 2018 e entrou em vigor em setembro de 2020 (Lei nº 13.709). Esta lei tem como principal objetivo garantir a privacidade e proteção dos dados pessoais dos cidadãos brasileiros, estabelecendo regras e diretrizes claras para o tratamento e uso dessas informações por parte de empresas e órgãos públicos. Ela foi inspirada no *General Data Protection Regulation* – GDPR (União Europeia, 2016) da porque ambos os regulamentos têm objetivos e abordagens semelhantes na proteção de dados pessoais e na garantia da privacidade dos indivíduos. Por sua vez, a GDPR, que entrou em vigor em maio de 2018, tem sido considerada uma das legislações mais abrangentes e rigorosas em termos de proteção de dados e privacidade no mundo.

Antecedentes Normativos da GDPR

Antes da implementação do *General Data Protection Regulation* (GDPR) em maio de 2018, a legislação europeia sobre proteção de dados e privacidade era regida principalmente pelas seguintes normas:

- A Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais de 28 de janeiro de 1981. Embora não seja uma legislação específica da União Europeia, estabeleceu princípios gerais de proteção de dados para seus Estados-membros. Esta convenção foi a primeira vinculação legal internacional sobre proteção de dados pessoais e continua sendo um importante instrumento no campo da proteção de dados. (União Europeia, 1981);
- A Diretiva de Proteção de Dados (95/46/EC) que foi adotada em 1995, estabeleceu as bases para a proteção de dados pessoais na União Europeia. Ela estabeleceu regras sobre o processamento e o fluxo de dados pessoais e introduziu conceitos como o consentimento do titular dos dados e a obrigação de informar. Cada Estado-membro implementou a diretiva em sua própria legislação nacional. (União Europeia, 1995);
- A Diretiva de Privacidade e Comunicações Eletrônicas (2002/58/EC), também conhecida como Diretiva e-Privacy, foi adotada em 2002 e posteriormente revisada em 2009. Abordava especificamente a proteção de dados e a privacidade no contexto das comunicações eletrônicas. Estabelecia regras sobre o uso de cookies, o envio de comunicações comerciais por e-mail e a proteção de dados em serviços de telecomunicações. (União Europeia, 2002); e,
- Algumas legislações nacionais. Antes do GDPR, cada país da União Europeia tinha sua própria legislação para a proteção de dados pessoais, com base nas diretrizes estabelecidas pela Diretiva de Proteção de Dados (95/46/EC). Por exemplo, na França, a legislação relevante era a Lei de Proteção de Dados de 1978 (modificada em 2004), enquanto na Alemanha, a Lei Federal de Proteção de Dados (BDSG) desempenhava um papel semelhante (Kuner, 2007).

O GDPR foi criado para unificar e fortalecer a proteção de dados na União Europeia, substituindo a Diretiva de Proteção de Dados e harmonizando a legislação de proteção de dados entre os Estados-membros. Ele estabelece requisitos mais rígidos para o processamento de dados pessoais e aumenta significativamente as sanções para o não cumprimento das normas de proteção de dados.

Antecedentes Normativos da LGPD

Por outro lado, os antecedentes legislativos da Lei Geral de Proteção de Dados (LGPD) brasileira podem ser encontrados tanto na legislação nacional quanto nas diretrizes e regulamentações internacionais, incluindo:

- A Constituição Federal de 1988: A Constituição do Brasil já estabelecia a proteção à privacidade como um direito fundamental (artigo 5º, X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação). Embora não fosse específica para a proteção de dados pessoais, a Constituição criou o alicerce para o desenvolvimento de leis nessa área.
- O Código de Defesa do Consumidor (Lei 8.078/1990), também estabeleceu normas de proteção e defesa do consumidor e inclui disposições relacionadas à proteção de dados pessoais, como a obrigatoriedade de informações claras e adequadas sobre o uso de dados pessoais dos consumidores (artigo 43).
- O Marco Civil da Internet (Lei 12.965/2014), ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, muito embora não seja específica para a proteção de dados pessoais, ela aborda aspectos de privacidade e define responsabilidades e obrigações para provedores de acesso e de conteúdo.

Além da influência já aqui narrada da GDPR da União Europeia, que entrou em vigor em maio de 2018, o Brasil também foi inspirado por diretrizes e recomendações internacionais, como as Diretrizes da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, que foram adotadas pela primeira vez em 1980 e atualizadas em 2013. Essas diretrizes servem como um conjunto de princípios comuns para os países membros e não membros desta organização, na proteção de dados pessoais e no equilíbrio da privacidade com outros interesses, como a livre circulação de informações, estabelecendo princípios norteadores para a limitação de coleta de dados, limitações sobre o uso, segurança e transparência, responsabilidade, participação pessoal, dentre outros (OCDE, 2013). Estas orientações, que merecem uma atenção maior em outra pesquisa, têm sido um marco importante no desenvolvimento de leis e regulamentações de proteção de dados em todo o mundo, e seus princípios podem ser encontrados tanto na LGPD brasileira, quanto em outras legislações de proteção de dados, como a GDPR europeia.

Semelhanças e Diferenças entre a LGPD da GPDR

Apesar de contextos geopolíticos díspares, no que tange ao texto das normas, a LGPD brasileira e a GDPR europeia compartilham diversas semelhanças, como: ambas as leis aplicam-se não apenas às empresas e organizações estabelecidas em seus respectivos territórios, mas também às organizações localizadas fora de suas fronteiras, desde que processem dados de residentes do Brasil ou da União Europeia; tanto a LGPD quanto a GDPR estabelecem princípios-chave para o processamento de dados pessoais, como legalidade, lealdade, transparência, limitação de finalidade, minimização de dados, exatidão, limitação de armazenamento, integridade e confidencialidade. Ambas as legislações preveem a figura do controlador e do operador de dados e estabelecem suas responsabilidades e obrigações.

Por outro lado, a LGPD e a GDPR exigem que as organizações obtenham o consentimento explícito dos indivíduos para o processamento de seus dados pessoais, com algumas exceções previstas em lei.

Ambas as leis estabelecem os direitos dos titulares dos dados, como o direito de acesso, retificação, oposição, eliminação, portabilidade e informação sobre o processamento de seus dados pessoais.

Os dois regulamentos previam a criação de autoridades nacionais de proteção de dados com o objetivo de supervisionar e aplicar as respectivas leis. No Brasil, a Lei nº 13.709, de 14 de agosto de 2018, criou a Autoridade Nacional de Proteção de Dados (ANPD), dentre outras previdências. Na Europa, O Comitê Europeu para a Proteção de Dados (CEPD) foi criado pela própria GDPR. O comitê é composto pelos representantes das autoridades nacionais de proteção de dados de todos os Estados-Membros da UE e tem como objetivo garantir a coerência na aplicação do regulamento de proteção de dados em

toda a UE, bem como promover a cooperação entre as autoridades nacionais de proteção de dados.

Muito embora a LGPD e a GDPR compartilhem muitos aspectos e princípios comuns, existem inúmeras diferenças entre os regulamentos, originárias das particularidades que refletem o contexto legal, cultural e político específico de cada região.

No que diz respeito à abrangência geográfica, apesar de o GDPR se aplicar a todos os membros da União Europeia, e a LGPD ser uma lei federal brasileira, ambas as leis têm efeitos extraterritoriais, ou seja, se aplicam a entidades internacionais que oferecem serviços ou coletam dados de indivíduos nos respectivos territórios.

Ambas as leis exigem uma base legal para o tratamento de dados pessoais: o GDPR prevê seis bases legais, incluindo o consentimento, o cumprimento de obrigações legais, a execução de um contrato, a proteção de interesses vitais, o interesse público e o interesse legítimo; a LGPD lista dez bases legais, que são similares às do GDPR, mas incluem algumas especificidades, como a proteção à saúde e a realização de estudos por órgãos de pesquisa.

O GDPR estabelece autoridades de proteção de dados em cada país membro da União Europeia e não unicamente uma supranacional. Autoridades de proteção de dados: A GDPR exige que os países membros da UE tenham autoridades de proteção de dados independentes. No Brasil, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), que era vinculada à Presidência da República. Transformada em autarquia com status de agência reguladora em outubro do ano passado por meio do Decreto Nº 11.348, de 01 de janeiro de 2023. Assim, embora seja autônoma, não é completamente independente do Governo Federal.

O GDPR exige a nomeação de um Encarregado de Proteção de Dados (DPO) em determinadas circunstâncias, como quando a organização realiza tratamento de dados em larga escala, trata dados sensíveis ou monitora sistematicamente indivíduos. A LGPD, por sua vez, exige que todas as organizações nomeiem um DPO, independentemente do tamanho ou natureza dos dados tratados.

O GDPR exige que as violações de dados sejam notificadas às autoridades de proteção de dados em até 72 horas após a descoberta. A LGPD não estabelece um prazo específico, mas determina que a notificação deve ocorrer em um prazo razoável, a ser definido pela ANPD.

Os dois regulamentos definem e protegem dados sensíveis, mas a GDPR tem uma lista mais ampla de categorias, incluindo dados biométricos e genéticos, enquanto a LGPD tem uma lista mais limitada, com uma abordagem mais focada em informações que podem levar à discriminação. Ambas exigem o consentimento explícito do titular dos dados para o processamento de suas informações sensíveis, salvo algumas exceções, como cumprimento de obrigações legais, proteção da vida, tutela da saúde, entre outras. As leis estabelecem que o consentimento deve ser claro, informado e específico quanto ao propósito de processamento desses dados.

Apesar dessas diferenças na categorização de dados sensíveis, ambos os regulamentos buscam proteger informações que podem levar à discriminação ou a outros danos aos titulares dos dados, e impõem requisitos mais rigorosos em relação ao consentimento e às condições para o tratamento desses dados.

Conceito de dados sensíveis e seu devido tratamento

A era do big data trouxe uma mudança de paradigma na coleta e análise de informações. O foco que residia na coleta de dados de indivíduos, graças às tecnologias modernas, com sua capacidade de processar e analisar enormes conjuntos de dados, passou para as análises em larga escala, abordando grupos, comunidades e até nações inteiras, no chamado "*group privacy*" de Floridi (2014). Este cenário sublinha a necessidade urgente de revisar as abordagens tradicionais de proteção de dados, reconhecendo que, mesmo em um contexto de big data, a proteção da privacidade individual e o controle sobre informações pessoais são de suma importância, mas agora devem ser considerados dentro de um contexto mais amplo e coletivo (Mantelero, 2016).

A LGPD define como dados sensíveis aqueles sobre origem racial ou étnica, convicção religiosa,

opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos. A lei brasileira trata como dado sensível, o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (Brasil, 2018).

A GDPR possui definição semelhante, englobando dados sobre origem racial, opiniões políticas, convicções religiosas, filiação sindical, dados genéticos, biométricos, de saúde ou vida sexual. Ambas enfatizam a natureza delicada desses dados e a necessidade de proteção reforçada.

Por sua vez, o artigo 9º do Regulamento (União Europeia) 2016/679 do parlamento europeu e do conselho, de 27 de abril de 2016, aborda o processamento de categorias especiais de dados pessoais, também conhecidos como dados sensíveis, sendo proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (UE, 2016).

Há que salientar que os dados pessoas são mais abrangentes. Diversos hábitos de consumo também são fornecidos para a internet, e a prova disso é a grande massa de anúncios que surgem para nós através das preferências dos consumidores (Bioni, 2019). Situação esta agravada pela redes sociais, como aponta Antreasyan (2016). Esses dados se tornam uma preciosa moeda para quem os detém. Os endereços de IP e os cookies também são dados pessoais que são fornecidos na maioria das vezes.

Segundo Danilo Doneda (2011), o conceito de dados sensíveis é amplamente aceito na legislação de proteção de dados ao redor do mundo. Ele se refere a informações que podem gerar discriminação ou dano relevante ao titular. Já para Laura Schertel Mendes (2021), a categorização de certos dados como sensíveis tem raízes históricas nos riscos de utilização abusiva ou discriminatória.

Para Paul de Hert e Vagelis Papakonstantinou (2016), os dados sensíveis exigem salvaguardas devido ao potencial de comprometer valores fundamentais e a dignidade humana. As categorias previstas na GDPR refletem também a experiência histórica europeia com regimes totalitários que abusaram desse tipo de informação.

Por sua vez, Solove (2008) articula uma visão complexa da privacidade e do tratamento de dados, onde ele destaca que a privacidade deve ser vista como um mosaico de diversas ações e políticas que afetam diferentes áreas da vida de uma pessoa. O tratamento de dados pode, assim, ser visto como um conjunto de atividades que envolvem a coleta, uso, divulgação e manutenção de informações pessoais, que necessitam de uma abordagem multifacetada para garantir a proteção adequada da privacidade. No que tange ao tratamento:

> Somente será autorizado quando autorizado pelo titular e se estiver em conformidade com as dez exigências ou base legal, assinaladas no art. 7º que, relativamente aos dados sensíveis, serão ampliadas pelo art. 11. (in TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. 2019, p.78).

Quando se fala em violação de dados ou *data breach*, significa que os dados confidenciais e sensíveis foram disponibilizados a uma pessoa não autorizada. O *data breach* ou atentado de dados pessoais é "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento." (União Europeia, 2016)

Tais dados podem incluir os dados bancários, logins e até mesmo dados biométricos, sendo, portanto, um grande pesadelo para quem lida com isso. Outra hipótese é referente ao não atendimento correto dos direitos que o titular dos dados possui. Com isso, pode-se acarretar dano moral e até mesmo patrimonial. O spam e o tratamento ilegal dos dados também fazem com que incida sobre os artigos referentes à responsabilidade civil.

Também é importante dispor sobre as violações de dados e como elas acontecem. Há vários ataques cibernéticos atualmente, e é por isso que os dados,

principalmente online, estão tão vulneráveis com o avanço das tecnologias. Os jornais têm relatado milhares de notícias sobre vazamento de milhões de informações das mais diversas empresas. Esse assunto é redundante na imprensa. Recentemente, os casos: Uber, com dados de 57 milhões de usuários; Chatgpt, com 157 mil usuários; a Equifax, em 2017, com 148 milhões de usuários expostos; o Facebook, em 2018, revelou que os dados de 87 milhões de usuários haviam sido compartilhados com a empresa de análise de dados Cambridge Analytica. Esses são apenas alguns exemplos dos muitos vazamentos de dados que ocorrem todos os anos. Os vazamentos de dados podem ter consequências graves para as pessoas afetadas, incluindo fraude, roubo de identidade e chantagem.

A responsabilidade dos provedores

A acelerada revolução tecnológica e digital do século XXI, marcada pela expansão da internet e pela onipresença das redes sociais, trouxe consigo desafios inéditos para a sociedade contemporânea. Neste cenário, os provedores de internet assumem um papel central, pois são os guardiões dos canais pelos quais a informação circula, são os guardiões dos dados sensíveis de milhões de pessoas e, consequentemente, têm um impacto direto na modelagem da cultura, na construção da realidade e na formação de opiniões. No entanto, essa posição privilegiada vem acompanhada de uma série de dilemas éticos e morais. Em que medida os provedores devem ser responsabilizados pelo conteúdo que circula em suas plataformas?

As lei de Proteção de Dados surgiram sendo pautadas por diversos princípios. Dentre eles, há o princípio da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção e não discriminação e da responsabilização, este último sendo o mais importante para o desenvolvimento da presente pesquisa.

Para enfrentar esse desafio, o pensamento do filósofo Hans Jonas, exposto em sua obra "O Princípio Responsabilidade", emerge como uma bússola essencial. Defende que, em uma era de avanços tecnológicos sem precedentes, é imperativo adotar uma ética centrada na responsabilidade, considerando as consequências a longo prazo de nossas ações e a necessidade de proteger o futuro. Seu argumento é de que, em face da incerteza e do poder das tecnologias modernas, a humanidade deve adotar uma postura de precaução, priorizando o bem-estar das gerações futuras (Jonas, 2006).

Assim, ao aplicarmos o pensamento de Jonas ao contexto dos provedores de internet, somos convidados a refletir profundamente sobre o papel e a responsabilidade destas entidades na construção de um futuro digital seguro, ético e inclusivo. Neste sentido, torna-se evidente a necessidade de nortear as práticas e decisões dos provedores a partir de uma ética da responsabilidade, garantindo que as potencialidades da internet sejam aproveitadas de forma benéfica para a humanidade, ao passo que seus riscos sejam minimizados.

Faz-se necessário expor alguns casos em que há a presença da responsabilidade civil, visto que é um tema abstrato para quem não tem muito conhecimento a respeito do tratamento dos dados pessoais.

A responsabilidade civil dos provedores no Brasil

O Marco Civil da Internet (Lei nº 12.965/2014) surgiu, em um passado não muito distante, para regulamentar os direitos dos usuários da internet, assegurando a inviolabilidade da intimidade, assim como a inviolabilidade da vida privada. Essa lei foi desenvolvida a partir da colaboração de vários setores da sociedade e conta com 32 artigos. Ao longo de todos eles, há a presença de direitos e deveres no Direito digital, além de, claro, dispor sobre a responsabilidade e sobre os provedores de acesso. Isso se percebe a partir da leitura do artigo 11. Nele, o princípio da privacidade foi protegido. Portanto, a lei tem como foco principal a inviolabilidade da vida privada e da intimidade, mesmo que na internet. Muitos entendem que a liberdade de expressão foi posta em segundo plano, visto que há um grande foco em proteger os dados pessoais no âmbito da rede de computadores. Todavia, a intenção do MCI é proporcionar aos usuários mais

proteção no armazenamento dos dados pessoais. Na referida lei também está presente o conceito de provedor de conexão e provedor de aplicações de internet. Os provedores de aplicações são pessoas que fornecem as funcionalidades que serão acessadas por meio da conexão com a internet. Resumindo, ele proporciona aos usuários várias funções, como, por exemplo, o armazenamento de dados e disponibildiade de conteúdos.

Nota-se que a Lei nº 12.695/2014 foi a lei pioneira a tratar sobre o uso dos dados pessoais dos usuários. A lei dispôs sobre a obrigação que os provedores de acesso tinham para assegurar a boa utilização dos dados. O Marco Civil trouxe, portanto, segurança jurídica a partir de sua vigência, visto que no Brasil não havia qualquer regulamentação para o assunto. Muitas críticas surgiram com a ascensão do MCI, pois grande maioria acreditava que a lei traria restrição para liberdade.

O MCI focou em delitos praticados apenas online, os chamados crimes cibernéticos. Ele foi responsável por estabelecer garantias e direitos, como da liberdade de expressão e da proteção à vida privada. Analisando a norma, vemos que foi uma forma de regulamentar as questões virtuais que envolvessem o Direito. Foi um meio que a legislação achou para se adaptar à evolução digital e proporcionar aos usuários da internet maior proteção no que diz respeito aos seus dados.

Diferente do que muitos achavam, a Lei nº 12.695/2014 não queria restringir direitos, mas sim garantir direitos que até então não eram existentes. A nova norma se fundamentava na regulamentação da internet, a qual tinha o dever de garantir a aplicação dos princípios, como, por exemplo, os direitos humanos. O foco sempre foi a existência de uma rede de computadores que garantisse a liberdade, mas acima de tudo, os direitos humanos.

O Marco Civil trouxe alguns direitos e garantias aos usuários no que tange à inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; e aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Além disso, o Marco Civil da Internet dispõe sobre a pluralidade e a diversidade, diante do alcance que a internet tem. Com a enorme integração entre povos e a integração entre as tecnologias, o MCI se preocupou em assegurar o que nunca deve ser esquecido, a dignidade da pessoa humana. Cabe ressaltar que os princípios contidos na referida lei, são exemplificativos, desse modo, não há a exclusão de outros princípios previstos no ordenamento jurídico.

Mesmo com o avanço trazido pelo Marco Civil da Internet, muitos pontos ficaram vagos. O intuito da lei jamais foi censurar ou impedir a liberdade de expressão, por isso, o artigo 19 da Lei nº 12.695/2014 expressa que o provedor de aplicações será responsabilizado por danos causados por terceiros apenas se descumprir ordem judicial específica, ou seja, apenas se não tomar as providências cabíveis. Todavia, esse artigo recebe duas críticas.

A primeira delas diz respeito à via judicial. Para os críticos desse artigo, impulsionar a via judicial pra solucionar esse tipo de problema é horrível, visto que os conteúdos são espalhados com grande facilidade com a globalização. Além disso, a restauração dos danos causados à privacidade demoraria de maneira significativa, visto que a via judicial é sempre demorada e isso retarda e inviabiliza a reparação do dano.

Outro ponto importante para se questionar é quando o artigo dispõe a condição de que será responsabilizado no âmbito e nos limites técnicos do seu serviço. Analisando essa parte do dispositivo, entende-se que é uma excludente de responsabilidade, rompendo, portanto, o nexo causal. Por exemplo, se o provedor de acesso conseguir provar que a retirada é inviável ou que não está mais no limite do seu serviço técnico, haverá a exclusão da responsabilidade civil.

Quando paramos para entender a influência do MCI, faz-se necessário analisar o sistem norte-americano. Como dispõem Barreto Júnior e Leite:

> Na década de 1990, nos Estados Unidos da América, houve um grande boom de compartilhamento de conteúdos, o que gerou problemas, a princípio, de ofensa aos direitos autorais, que culminaram em demandas excessivas e sem precedentes contra os provedores de internet. Esse fato fez com que surgisse

> a necessidade de um regramento específico para o setor, sendo, em seguida, editada a diretiva Digital Millenium Copyright Act, que tratava não só dos direitos autorais, mas também de demais atos ofensivos aos usuários, inclusive os causados por terceiros. Essa diretiva acabou por criar imunidades para os provedores, a chamada zona de conforto (safe harbor), que restringiu a responsabilidade dos provedores, tornando-a subsidiária e subjetiva, aplicável apenas em casos de omissão dos detentores de redes sociais, páginas e websites, quando notificados e inertes em retirar o conteúdo ofensivo do ar, ou bloquear o seu acesso. Esse é o chamado sistema notice and take down, que considera válida a notificação extrajudicial, feita diretamente pelo usuário. (2017, p. 431)

Diante do exposto, nota-se que o MCI adotou tanto o sistema norte-americano, quanto o sistema europeu em relação às imunidades disponibilizadas para os provedores de acesso. No entanto, o sistema *notice and take down* foi deixado de lado, o que foi prejudicial para o usuário ofendido, visto que ele passou a ser obrigado a procurar o poder judiciário para validar a notificação. Isso foi um grande retrocesso para os usuários atingidos pela rede de computadores.

Por isso, para muitos doutrinadores, a Lei nº 12.695/2014 já surgiu com esse grande problema, que obviamente poderia ser evitado. Dificultou muito para o usuário ofendido, trazendo mais ônus do que bônus, além de prolongar o processo. No que diz respeito à responsabilidade dos provedores por ato ilícito praticado por eles mesmos, é mais fácil o entendimento, visto que eles responderão de maneira objetiva se for uma relação de consumo.

Portanto, mesmo sendo um grande avanço para a sociedade atual, regida pela tecnologia e informação, o Marco Civil da Internet precisava percorrer um longo caminho para suprir outras necessidades também existentes na rede de computadores e acabar com as críticas específicas em determinados artigos. Era preciso priorizar maior proteção e segurança ao usuário da internet.

Porém, no que diz respeito aos dados pessoais, ao tratamento que esses dados devem receber e à responsabilidade civil para quem descumprir a norma, o MCI falhou, porque ele não dispôs sobre o destino e a comercialização dos dados pessoais. Nesse sentido surge a Lei Geral de Proteção de Dados (LGPD), a segunda lei a ser analisada na minha pesquisa. Ela veio justamente para suprir essas lacunas. A LGPD cria diretrizes que se aplicam tanto nas relações on-line quanto nas off-line, diferente do MCI, que tinha como principal objetivo dispor sobre direitos e garantias para os usuários da internet.

No Brasil, o art. 7º da Lei nº 12.965/2014, enumera diversos direitos dos usuários de Internet em relação direta com a proteção à privacidade, reverberando preceitos constitucionais. O primeiro ressalta a proteção à intimidade e a vida privada, assegurando a indenização por danos materiais e morais decorrentes de sua violação, em mera repetição do inciso X, do art. 5º, da Constituição Federal.

A Carta Magna não especificou em seu texto sobre os dados digitais, hoje tão discutidos. O artigo 5º, inciso X, da Carta Magna, afirma que a intimidade é inviolável, sendo assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação. O sigilo telefônico também é assegurado no inciso posterior.

Com o passar dos anos e com o avanço tecnológico e do Direito digital, já não era suficiente a proteção contida na Constituição brasileira, sendo de suma importância a existência de uma nova regulamentação, a fim de que as informações pessoais tivessem maior proteção, evitando assim, o repasso de informações pessoais sem autorização do titular.

O fundamento do Código de Defesa do Consumidor (CDC), no que diz respeito à responsabilidade, se baseava unicamente no dever de segurança que o fornecedor tinha em relação aos produtos que seriam utilizados pelos consumidores. O Direito comparado foi muito usado nesse sentido, pois a responsabilidade no Direito digital sempre buscava se basear no CDC e no Código Civil. A doutrina e jurisprudência tendiam a inclinar para a adoção de responsabilidade objetiva, a partir da atividade perigosa ou de risco a qual os provedores se submetiam. Conforme preleciona Simão Filho:

> As decisões judiciais vez por outra estão conferindo espécie de responsabilidade ilimitada aos

> intermediários técnicos, seja na aplicação do Código de Defesa do Consumidor ou nas disposições do novo Código Civil, o que demanda um olhar atento aos precedentes encontrados e uma análise crítica sob diversos pontos (2007, p. 49).

O que era parcialmente regulado pelo Marco Civil, foi melhorado com a LGPD brasileira, consolidando de uma vez a proteção dos dados pessoais. O legislador brasileiro só se preocupou em regular de maneira efetiva a proteção de dados pessoais em 2018. Claro que já existiam outras normas que tratavam do tema, mesmo que de maneira sucinta, como o Código de Defesa do Consumidor, o Marco Civil da Internet, entre outras. No entanto, somente com a LGPD, passou-se a dar um novo resguardo ao indivíduo titular dos dados, tornando-o protagonista das relações jurídicas.

Como se percebe, o direito à proteção dos dados pessoais, portanto, já era debatido antes mesmo da vigência da LGPD. A Constituição da República de 1988, o Código Civil de 2002, o Código de Defesa do Consumidor e o Marco Civil da Internet já apresentavam disposições sobre o assunto, sendo a LGPD uma complementação e ajuste, se baseando na atualidade e nas novas adaptações que precisavam ocorrer com o avanço tecnológico.

A LGPD faz com que o usuário tenha o poder de escolha, isso ocorre porque tem que ter o consentimento dele para praticamente todas as ações envolvendo o tratamento de dados. Isso é muito importante, porque se esses dados são vazados a pessoas ou empresas não autorizadas, isso pode trazer sérias consequências, gerando danos à privacidade, à imagem e consequentemente acarretar danos morais e patrimoniais, como ocorreu com o Facebook. Por isso a importância de criar outra lei que seja específica nesse assunto, pois assim há a garantia de maior segurança no que tange aos dados pessoais dos usuários.

Com a Lei nº 13.709/2018, o Brasil entrou para a lista dos países que têm legislação própria para proteção de dados pessoais, surgindo maior vigor em relação ao tratamento dos dados sensíveis, já especificados em tópico anterior. Tais dados só poderão ser armazenados com o consentimento expresso dos usuários. Em seu artigo 12, há uma exceção à proteção dos dados quando estes dados forem anônimos. Vale ressaltar que, mesmo nesses casos, poderá ocorrer a reversão dessa situação e esses dados, que até então são anônimos, serão considerados pessoais e deverão ser protegidos. Outra situação interessante trazida pela LGPD recai sobre as medidas adotadas para proteção dos dados.

De acordo com a referida lei, é dever do controlador e do operador dos dados adotar medidas a fim de que os dados pessoais utilizados sejam protegidos. Essa obrigação ainda ganha uma ampliação e atinge até mesmo as pessoas que intervirem, de alguma forma, no processo de tratamento dos dados. Assim, nota-se que a LGPD foi bem pensada, de modo a ampliar o rol dos envolvidos nas obrigações, trazendo mais segurança aos dados fornecidos pelos usuários.

Conforme pode-se verificar no artigo 7º do texto da lei, será proibido utilizar os dados pessoais se forem para uma finalidade diversa daquela que foi previamente acordada com o cliente, ou seja, o usuário tem direito de escolha com a nova lei. Ou seja, o usuário deve estar plenamente ciente da finalidade daquele uso dos dados. Diante dessas mudanças no cenário de tratamento de dados pessoais, as empresas estão se atentando mais para isso, promovendo políticas cada vez mais transparentes sobre o uso, coleta e armazenamento de dados.

Para que haja uma proteção eficiente, em seu capítulo VIII, a lei estabeleceu algumas sanções para quem descumprir as obrigações impostas. Como já foi analisado anteriormente, o CDC teve uma grande importância no contexto da responsabilidade civil dos provedores de acesso. A nova lei surgiu para complementar as normas anteriores e está diretamente relacionada com a defesa do consumidor.

É preciso dispor que a ideia de usar a responsabilidade objetiva, aplicada no Direito do Consumidor, teria suas falhas de modo natural, visto que as pretensões dos institutos jurídicos citados eram diferentes das pretensões do direito digital. O que ocorria era a tentativa de aplicar regras que eram boas para outras épocas, a fim de preencher as lacunas existentes no MCI. São contextos diferentes, portanto era inevitável haver divergências

de entendimento no que diz respeito a responsabilidade civil dos provedores de acesso.

A responsabilidade civil está disposta na Seção III do Capítulo VI da referida lei. Ali também está expresso sobre o ressarcimento dos danos. O artigo 42 é de suma importância para esse estudo, além dos artigos seguintes. O artigo 46 estabelece, por exemplo, que todos agentes de tratamento devem adotar medidas de segurança, sempre visando à proteção dos dados pessoais dos usários. A responsabilidade civil entra em ação quando há violações das normas jurídicas e técnicas. Quando é causado dano ao titular dos dados, é preciso usar esses artigos para solucionar o caso e reparar os danos.

Por se tratar de um tema teoricamente recente, ainda há muita divergência em relação à responsabilidade civil para os provedores de acesso e de informação. Como já vimos, diante da ausência de normas que perdurou por anos, a doutrina e a jurisprudência se baseava no CDC. Portanto, com o surgimento de uma norma específica, a responsabilidade civil no âmbito do direito digital passou a ser regulada nos artigos 42 a 45 da LGPD. Houve uma inovação trazida pela lei de dados, pois surgiu a figura dos agentes de tratamento, os mais novos responsáveis pelo tratamento de dados, os quais apresentam diversos deveres. Assim, a responsabilidade civil tem seu início na atividade de proteção de dados.

A lei também é responsável por distinguir as responsabilidades dos agentes e de terceiros, as possibilidades de exclusão de responsabilidade e conceitua a responsabilidade solidária, antes não discutida. Como estabelece o artigo 5º da LGPD, os responsáveis pelo tratamento dos dados pessoais correspondem ao controlador, que decide sobre o tratamento de dados, e ao operador, que é o responsável por executar o tratamento de dados. Tanto um quanto o outro deverão obedecer aos artigos 42 ao 45 da referida lei, sendo possível a inversão do ônus da prova, assim como ocorre no CDC.

Com a disposição expressa da responsabilidade civil para os provedores de acesso e aplicação, surgiram algumas correntes que divergem sobre o tema. A discussão gira em torno da possível responsabilidade tendo como base a culpa. Uma das correntes doutrinárias entende que a responsabilidade é sim objetiva, portanto, deve-se levar em consideração o risco da atividade, deixando de lado a subjetividade da intenção do agente. A outra corrente divergente afirma que é preciso observar a culpa do agente, diante das diversas obrigações que foram colocadas na lei.

No que tange à responsabilidade objetiva, é preciso dispor sobre as duas teorias que predominam no nosso ordenamento jurídico. A primeira diz respeito ao risco da atividade. Essa teoria é adotada tanto pelo Código Civil quanto pelo Código de Defesa do Consumidor. Com essa teoria, é possível existir as excludentes de responsabilidade, as quais rompem completamente o nexo causal entre a conduta e o resultado. Em sentido oposto, a segunda teoria da responsabilidade é voltada para o risco integral e, nesse caso, não são admitidas as excludentes de responsabilidade civil. Independente da culpa exclusiva da vítima, por exemplo, sempre haverá a responsabilidade. Essa teoria é bastante utilizada no direito ambiental.

Neste sentido, conclui Mulholland:

> […] apesar do uso de expressões diversas em sua redação, tanto o artigo 42, quanto o artigo 44, da LGPD, adotam o fundamento da responsabilidade civil objetiva, impondo aos agentes de tratamento a obrigação de indenizar os danos causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador. (2020)

Entende-se, portanto, que a teoria utilizada é a do CDC, conhecida como teoria do risco, visto que a atividade que é desenvolvida pelos agentes que fazem o tratamento de dados é de risco. O legislador levou em consideração o risco que a atividade do tratamento de dados gera por si só, todavia, possibilitou que a responsabilidade fosse relativizada, conforme trata o artigo 43 da LGPD.

Mas porque é viável utilizá-la nas relações de consumo? O motivo por esse tipo de principalmente objetiva ser usada, principalmene no CDC, se justifica pela vulnerabilidade e hipossuficiencia do consumidor. O que também acaba acontecendo em relação aos usuários da internet. É nítido que os dados dos usuários são expostos com frequência.

Portanto, mesmo que a LGPD não deixe explícito que a responsabilidade civil pode sim ser objetiva, parte da doutrina conclui que esta será.

Portanto, o maior argumento utilizado por parte da doutrina que entende que a responsabilidade dos agentes de tratamento é objetiva é porque a atividade que eles exercem é de risco. São riscos inerentes à atividade e resultam em danos aos usuários titulares dos dados. Além disso, por causarem danos até mesmo coletivos, é muito justificável a adoção dessa responsabilidade civil. Danilo Doneda (2006) é um dos doutrinadores que entendem dessa maneira.

A outra parte da doutrina que entende que a responsabilidade civil no caso dos agentes provedores de acesso e informação é subjetiva, tendo como base os próprios artigos da lei. De acordo com o entendimento de grande parte dos autores, cabe essa teoria porque na própria omissão de medidas de segurança o agente já está agindo com culpa, nesse caso por negligência. Acontece o mesmo com o descumprimento das obrigações impostas pela LGPD. Nesse caso também ocorre a culpa. Esse é o entendimento de Gisela Guedes e Rose Meireles (2020), por exemplo.

A responsabilidade civil dos provedores na Europa

O GDPR (Regulamento Geral sobre a Proteção de Dados) estabelece várias responsabilidades para os provedores de serviços da Internet que processam dados pessoais de indivíduos na União Europeia. Algumas das principais responsabilidades, cujas discussões demandam um aprofundamento em outras pesquisas, incluem: obter consentimento explícito dos indivíduos para processar seus dados pessoais, e informá-los claramente sobre como seus dados serão usados; proteger dados pessoais que processam e implementar medidas de segurança apropriadas para garantir que esses dados sejam mantidos seguros; nomear um encarregado de proteção de dados (DPO), pessoa responsável por supervisionar a conformidade com a GDPR; responder a solicitações de indivíduos para acessar, corrigir ou excluir seus dados pessoais; notificar as autoridades relevantes e os indivíduos afetados em caso de violações de dados que possam representar um risco para os direitos e liberdades dos indivíduos.

Implementar proteção de privacidade desde o design: Os provedores de serviços da Internet devem implementar proteção de privacidade desde o design de seus serviços, garantindo que a privacidade seja levada em consideração desde o início.

Essas são apenas algumas das responsabilidades dos provedores de serviços da Internet sob a GDPR. A conformidade com a GDPR é importante para garantir a proteção dos direitos de privacidade dos indivíduos e para evitar possíveis penalidades financeiras e reputacionais.

A responsabilidade civil dos provedores de informações ganhou destaque em alguns países, especialmente na União Europeia, onde várias decisões judiciais foram proferidas sobre o tema. Um marco importante na evolução da responsabilidade civil no que tange aos provedores de serviços de internet, tratou do chamado direito ao esquecimento. Em 2014, o Tribunal de Justiça da União Europeia (TJUE), que interpreta o Direito europeu para garantir que este seja aplicado da mesma forma em todos os países da União Europeia, julgou o Google Spain SL e Google Inc. contra a Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, decidindo que os indivíduos têm o direito de solicitar a remoção de links para informações pessoais desatualizadas ou irrelevantes em motores de busca como o Google. Neste caso, um cidadão espanhol, Mario Costeja González, solicitou que informações sobre um leilão de imóveis relacionado ao seu nome fossem removidas do Google, pois a dívida havia sido resolvida há muito tempo e a informação era prejudicial à sua reputação. Essa decisão influenciou diretamente a inclusão do direito ao esquecimento na GDPR, formalizando o direito ao esquecimento no âmbito legal europeu (União Europeia, 2014).

Posteriormente, o caso Delfi AS *versus* Estonia, uma das maiores plataformas de notícias online na Estônia, foi responsabilizada pelos comentários difamatórios postados por usuários em seu site. O tribunal nacional estoniano, e posteriormente o TEDH - Tribunal Europeu dos Direitos Humanos, sustentaram que a Delfi deveria ter exercido maior

controle e moderação sobre os comentários postados em sua plataforma, particularmente porque a empresa tinha o potencial de ganho financeiro através da atração de mais tráfego para o seu site. O estudo deste caso se tornou interessante para esta pesquisa porque, além um estímulo à moderação dos assuntos, ao responsabilizar as plataformas por comentários de usuários, a decisão poderia encorajar uma moderação mais pró-ativa e responsável do conteúdo, ajudando a prevenir a difusão de informações falsas e discursos de ódio (União Europeia, 2015).

Assim, este caso representa uma tentativa significativa de equilibrar os direitos individuais com a liberdade de expressão na era digital. No entanto, ele também levanta questões críticas sobre a extensão da responsabilidade das plataformas online e as implicações para a liberdade de expressão e o debate público. É um caso que serve como um precedente importante, mas também um que pode necessitar de revisitação à luz das mudanças rápidas no ambiente online.

Importante da mesma forma foi o caso Glawischnig-Piesczek *versus* Facebook Ireland Limited. Eva Glawischnig-Piesczek, uma política austríaca, exigiu que o Facebook removesse comentários difamatórios postados por um usuário em sua plataforma. A questão central era se o Facebook poderia ser obrigado a remover não apenas a postagem específica em questão, mas também outras postagens "equivalentes", e se tais ordens poderiam ter um alcance global. (União Europeia, 2018). Da mesma forma, a decisão destaca a necessidade de as plataformas de mídia social assumirem uma responsabilidade maior na moderação de conteúdo, incentivando-as a serem mais proativas na identificação e remoção de conteúdo ilegal.

Juntos, esses casos representam uma tendência crescente na Europa de impor obrigações mais rigorosas aos provedores de internet, para proteger os direitos dos indivíduos contra danos e garantir a legalidade do conteúdo disponível online.

Ao contrário da opinião predominante na Europa, Piraino (2018), aponta que a disciplina em questão não constitui um caso de responsabilidade extracontratual, mas estabelece a regulação de uma esfera de licitude de ação em favor dos ISPs. De forma contrária, Tosi (2019), defende a natureza extracontratual da responsabilidade pelo ilícito do tratamento de dados pessoais.

Esses julgamentos delineiam um caminho de crescente reconhecimento da responsabilidade dos provedores de internet, com uma atenção cada vez maior à proteção dos direitos individuais em um ambiente digital que está em constante evolução. Eles demonstram também uma adaptação e uma resposta normativa dinâmica às complexidades apresentadas pelo espaço digital.

Sob a GDPR, conforme seu artigo 82º, os provedores têm a responsabilidade de garantir a proteção dos dados pessoais que processam. Eles são obrigados a implementar medidas técnicas e organizacionais adequadas para garantir e demonstrar que o processamento de dados está em conformidade com o regulamento.

Entretanto, percebe-se que, aproximadamente vinte anos após a União Europeia estabelecer suas primeiras normas de proteção de dados, ainda persistem dúvidas cruciais sobre a essência e o alcance dessa política da UE, bem como sobre os prejuízos que ela visa evitar (Lynskey, 2015).

Esta pesquisa detalha a responsabilidade dos controladores de dados e processadores em caso de violação das regras de proteção de dados e estabelece o direito de compensação para os titulares dos dados (Tescaro, 2017). A inclusão da responsabilidade solidária é particularmente significativa, pois visa garantir que os titulares dos dados possam efetivamente receber uma compensação, mesmo que a responsabilidade pelo dano seja compartilhada por várias partes. Além disso, o artigo prevê a possibilidade de um direito de recurso, permitindo a distribuição justa da responsabilidade entre as partes envolvidas.

Entretanto, como pondera Arroyo Amayuelas, "De momento, la tendencia es ampliar las obligaciones de control preventivo, siguiendo la estela de decisiones (contradictorias) de los tribunales nacionales que han contribuido a la confusión sobre el nivel de diligencia que debían tener para proteger su puerto seguro" (p. 836, 2020). Por outro lado, Martínez e Porcelli, em defesa dos provedores de internet, salientam que se as suas responsabilidades fossem estabelecidas de forma ampla e

indiscriminada, a continuidade da internet poderia estar em risco:

> [...] porque es imposible para cualquiera de ellos hacerse responsable por todas las cosas dañosas que se digan en la red y por sus eventuales consecuencias económicas; además existe una imposibilidad tecnológica de controlar, por la cantidad, la información que se encuentra en el servidor, siempre y cuando no tenga conocimiento del hecho dañoso, en virtud de una notificación o reclamo previo del interesado, en tal caso reaparece el deber jurídico de removerlo (MARTÍNEZ e PORCELLI, p. 167, 2015).

Ao mesmo tempo, este artigo serve como um mecanismo de dissuasão forte, incentivando os controladores de dados e processadores a cumprir rigorosamente as disposições do GDPR, dado o risco financeiro significativo associado às violações de dados.

Considerações finais

Ao se aprofundar nas responsabilidades dos provedores de internet, instiga-se também a ponderar, de forma criteriosa, o papel e as obrigações desses agentes na moldagem de um futuro digital que seja ao mesmo tempo seguro, ético e abrangente. Assim, destaca-se o imperativo de orientar as ações e escolhas dos provedores sob o prisma de uma ética responsável, assegurando que a vastidão de oportunidades oferecidas pela internet seja capitalizada em benefício da coletividade, enquanto se mitigam os possíveis perigos.

Os provedores de internet, sendo parte integrante da infraestrutura tecnológica moderna, têm um papel fundamental na guarda de informações, na modelagem da informação e da cultura. Assim, eles têm o dever ético de pensar sobre como suas decisões afetarão a sociedade a longo prazo.

Embora haja posições contrárias a respeito da responsabilidade objetiva e subjetiva, o Poder Judiciário já proferiu diversas decisões englobando tanto uma quanto outra. Assim sendo, não podemos afirmar com total propriedade que a Lei Geral de Proteção de Dados escolheu, de fato, a teoria do risco, como já foi exposto anteriormente, nem que adotou a responsabilidade subjetiva. Entretanto, independente da teoria adotada nas decisões proferidas, uma coisa é certa, a cada dia que passa cresce mais a importância de ter segurança dentro das empresas e o bom tratamento dos dados, a fim de evitar riscos envolvendo dados pessoais.

Assim, conclui-se que para assegurar o bom uso dos dados pessoais, faz-se necessário respeitar os deveres impostos pela lei. Caso contrário, deverão prevalecer os artigos que dispõem sobre a responsabilidade civil. Essa restrição ao tratamento de dados de modo inconsequente é de suma importância para o equilíbrio das relações existentes no meio digital. Além disso, é necessário que todos os operadores do direito digital tenham consigo as normas da LGPD, visto que a sua compreensão evita eventuais situações de risco e, consequentemente, ações judiciais. É preciso dispor que cada um tem sua interpretação a respeito das diretrizes da lei acima citada, de modo que a hermenêutica permite que existam vários entendimentos a respeito da responsabilidade civil.

Tendo percorrido o tema proposto, é possível extrair que a recente Lei nº 13.709/2018, em complemento ao arcabouço jurídico preexistente, como o CDC e o Marco Civil da Internet, por ter se incumbido de determinar na atividade de coleta e tratamento de dados, alguns direitos e garantias aos internautas, bem como deveres dos provedores de Internet, pode melhor instrumentalizar a responsabilidade civil, em prol da proteção da privacidade e da segurança jurídica, em face de danos advindos do tratamento de dados pessoais.

O surgimento da Internet e de empreendimentos eletrônicos sustentados por publicidade direcionada renovou a importância de alguns direitos fundamentais, tal como a autodeterminação informativa, i.e., a prerrogativa de controlar a publicidade das próprias informações pessoais, diretamente relacionadas ao direito à privacidade e intimidade.

No que tange aos agentes de tratamento de dados, termo este que engloba inclusive os provedores de aplicações de Internet, instituiu-se um verdadeiro regime de responsabilidade objetiva pelos danos que causarem pela atividade de tratamento de dados pessoais, pautada pela Teoria do Risco da Atividade, explicitamente tratada pelo CDC em seu art. 14, que prevê que o fornecedor de serviços responde objetivamente pelas

inconstâncias que envolvem a prestação falha de seus serviços.

Os tribunais, tanto europeus, como brasileiros, têm evoluído na construção de uma responsabilização concreta dos provedores. É certo que, tratando-se de *Big techs*, há necessidade de se repensar a estrutura de responsabilidade para que possa também atingir a estes provedores, diante da influência que tais corporações podem exercer em todos os campos.

No Brasil, decisões judiciais têm exigido que corporações estrangeiras nomeiem representantes responsáveis por elas no país, para que possam sofrer sanções. As decisões têm aumentado muito, sobretudo no combate à fakenews.

Na Europa, alguns casos representam uma tendência crescente na Europa de impor obrigações mais rigorosas aos provedores de internet, com o objetivo de proteger os direitos dos indivíduos contra danos online e garantir a legalidade do conteúdo disponível. Esses julgamentos delineiam um caminho de crescente reconhecimento da responsabilidade dos provedores de internet, com uma atenção cada vez maior à proteção dos direitos individuais em um ambiente digital. Eles demonstram uma adaptação e resposta normativa dinâmica às complexidades apresentadas pelo espaço digital que está em constante evolução.

Referências

Antreasyan, S. (2016) *Réseaux sociaux et mondes virtuels: contrat d'utilisation et aspects de propriété intellectuelle*. Disponível em: https://archive-ouverte.unige.ch//unige:83548.

Arroyo Amayuelas, E. (2020) La responsabilidad de los intermediarios en internet ¿puertos seguros a prueba de futuro? *Cuadernos de Derecho Transnacional*, *v. 12*, n. 1, p. 808-837. Disponível em: https://e-revistas.uc3m.es/index.php/CDT/article/view/5225.

Barreto Júnior, I; e Leite, B. (2017) Responsabilidade civil dos provedores de aplicações por ato de terceiro na lei 12.965/14 (marco civil da internet). *Revista Brasileira de Estudos Políticos*, v. 115, .

Bioni, B. R. (2019) *Proteção dos Dados Pessoais: A função e os limites do consentimento.* Forense.

Brasil (2002). Lei nº10.406, de 10 de janeiro de 2002. *Código Civil*. https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm.

Brasil, (1990). Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

Brasil, (2018). Lei nº 13.709 de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Brasil, (2014). Lei nº 12.965, de 23 de abril de 2014. *Marco Civil da Internet*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Castells, M. (2002). *A sociedade em rede. A era da informação: economia, sociedade e cultura*. Trad. Roneide Venancio Majer. 6. ed. Paz e Terra. v.1.

Cohen, J. (2012) *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press.

De Hert, P; e Papakonstantinou, V. (2016) The data protection regime in China through the lens of the EU GDPR. *Computer Law & Security Review*, v. 32, n. 3, p. 362-369.

Doneda, D. (2011) A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL],* v. 12, n. 2, p. 91-108.

Doneda, D. (2006). *Da privacidade à proteção de dados pessoais*. Renovar.

Floridi, L. (2014). Open data, Data Protection, and Group Privacy. *Philosophy & Technology*. v. 27. https://link.springer.com/article/10.1007/s13347-014-0157-8.

Giabardo, C. (2015) Tempo e Diritto: alcune considerazioni a proposito della tutela civile dei diritti nell'epoca della globalizzazione. In *Proposte per un Diritto del Terzo Millennio*. : Università Degli Studi Di Perugia.

Jonas, H. (2006) *O princípio responsabilidade: Ensaio de uma Ética para uma Civilização Tecnológica*. Contraponto.

Kuner, C. (2007) *European data protection law: Corporate Compliance and Regulation*. 2. ed. Oxford University Press. p. 152-178.

Lynskey, O. (2015) The foundations of EU data protection law. Oxford University Press.

Mantelero, A. (2016) *Personal data for decisional purposes in the age of analytics: From an individual to a collective*

dimension of data protection. Computer Law & Security review, v. 32, n. 2, p. 238-255.

Marsico, G. (2022) La responsabilità civile dell'internet service provider: sulla dibattuta species del contratto di accesso. *Il Dirittto Amministrativo*. https://www.ildirittoamministrativo.it/pdf/stu/915/25.11.2022-Responsabilit%C3%A0-Intedrnet-service-Provider-di-GIUSEPPE-MARIA-MARSICO.pdf.

Martínez, A. Porcelli, A. (2015) *Alcances de la Responsabilidad Civil de los Proveedores de Servicios de Internet (ISP) y de los Proveedores de Servicios Online (OSP) a nivel internacional, regional y nacional: las disposiciones de Puerto Seguro, notificación y deshabilitación*. Universidad de Buenos Aires. https://www.researchgate.net/publication/316460459_Alcances_de_la_Responsabilidad_Civil_de_los_Proveedores_de_Servicios_de_Internet_ISP_y_de_los_Proveedores_de_Servicios_Online_OSP_a_nivel_internacional_regional_y_nacional_Las_disposiciones_de_Puerto_.

Mulholland, C. S. (2020). A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? *Migalhas*. 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.

OCDE. (2013) *Guidelines on Privacy Protection and Cross-Border Flows of Personal Data*. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

Piraino, F. (2017) *Spunti per una rilettura della disciplina giuridica degli internet service provider* (Ideas for a new reading of the law regulation of internet service providers). d/SEAS Working Paper No. 18-7. http://dx.doi.org/10.2139/ssrn.3206527.

Solove, D. (2008) *Understanding Privacy*. Harvard University Press, p. 147-166.

Tescaro, M. (2017) *La responsabili tà civile dell'internet provider in Italia: attuazione della Direttiva europea sul commercio elettronico contro tendenze della giurisprudenza*. https://revistas.faa.edu.br/FDV/article/view/151/123.

Tosi, E. (2019) *Responsabilità Civile per Illecito Trattamento Dei Dati Personali e Danno Non Patrimoniale*. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR. Giuffrè Francis Lefebvre.

Tosi, E. (2021) *Diritto privato delle nuove tecnologie digitali. Riservatezza, contratti, responsabilità tra persona e mercato*. Giuffrè Francis Lefebvre.

União Europeia, (1981) *Convenção 108*, adotada em 1981. https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf.

União Europeia, (1995) *Directiva 95/46/CE do Parlamento Europeu e do Conselho*, de 24 de outubro de 1995. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046.

União Europeia, (2002) *Directiva 2002/58/CE do Parlamento Europeu e do Conselho*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058.

União Europeia, (2014) *Tribunal de Justiça da União Europeia (TJUE)*. Caso Google Spain SL x AEPD. https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT.

União Europeia (2018) *Tribunal de Justiça da União Europeia* (TJUE). Caso Glawischnig-Piesczek versus Facebook Ireland Limited.. https://curia.europa.eu/juris/document/document.jsf?docid=218621&doclang=PT.

União Europeia. (2015) *Tribunal Europeu dos Direitos Humanos* (TEDH). Caso Delfi AS x Estonia. Disponível em: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-155105&filename=001-155105.pdf.

União Europeia. (2016) *Regulamento Geral sobre a Proteção de Dados*. Regulamento 2016/679 do Parlamento Europeu e do Conselho. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN.

Tepedino, G; Frazão, A; Oliva, M (Coords.). (2019) *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*.Thomson Reuters (Revista dos Tribunais)

Warren, S.; e Brandeis, LD. (1890) The right to privacy. Harvard Law Review, v.4, n.5. pp. 193-220.