LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA E *GENERAL DATA PROTECTION REGULATION* EUROPEIA: RESPONSABILIDADE CIVIL DOS PROVEDORES[1]

GENERAL BRAZILIAN DATA PROTECTION LAW (LGPD) AND GENERAL EUROPEAN DATA PROTECTION REGULATION (GDPR): CIVIL RESPONSIBILITY OF PROVIDERS

Cildo GIOLO JÚNIOR[2]

Pablo Martins Bernardi COELHO[3]

ISSUE DOI: 10.21207/1983-4225.2021.1438

[1] Este artigo é resultado de pesquisa fomentada pelo Programa de Bolsas de Produtividade em Pesquisa, Edital nº 06/2021 PQ/UEMG, da Pró-Reitoria de Pesquisa e Pós-Graduação (PROPPG) da Universidade do Estado de Minas Gerais e das discussões do Centro de Estudos Interdisciplinares de Direito e Inovação (CEINDI) da Universidade do Estado de Minas Gerais, grupo de estudos certificado pelo CNPq, mantido pelos autores.

[2] Pós-Doutor em Direitos Humanos pela Universidade de Coimbra (Portugal). Doutor em Direito pela Universidade Metropolitana de Santos (Brasil). Doctor en Ciencias Jurídicas y Sociales pela UMSA, Buenos Aires (Argentina). Mestre em Direito Público (Brasil). Professor da Universidade do Estado de Minas Gerais (Frutal - Minas Gerais) e da Faculdade de Direito de Franca (São Paulo) e Advogado. Currículo: http://lattes.cnpq.br/9079687915501476. E-mail: cildo.junior@uemg.br

[3] Pós-doutorando em Direito pela Universidade Federal do Rio Grande - FURG. Doutor em História Política pela UNESP/Franca. Mestre em História Política pela UNESP/Franca. Especialização em Direito Público pela EBRADI. Possui graduação em Direito pela UNIRP. Possui graduação em Ciências Sociais pela UNESP/Araraquara. Professor da Universidade do Estado de Minas Gerais (Frutal - Minas Gerais) Currículo: http://lattes.cnpq.br/0584374185581812. E-mail: pablo.coelho@uemg.br

RESUMO
Esta publicação é resultado de pesquisa que se explica pela preocupação em como as informações e dados pessoais serão utilizados no dia a dia. Tem também o condão de verificar quem é legitimado para acessar estes dados, apurando-se o nexo de causalidade entre o início do tratamento e a finalidade dele. Além disso, busca comparar o instituto da responsabilidade civil destes provedores de acordo com a Lei Geral de Proteção de Dados brasileira (LGPD) e a General Data Protection Regulation Europeia (GDPR), contribuindo com a discussão e a interpretação destas leis.
Palavras-chave: Proteção de dados; Responsabilidade Civil; Provedores de Acesso; Provedores de Aplicações.

ABSTRAT
This paper is the result of research that is explained by the concern with how information and personal data will be used on a daily basis. It also has the power to verify who is entitled to access these data, establishing the causal link between the beginning of the treatment and its purpose. In addition, it seeks to compare the institute of civil liability of these providers according to the Brazilian General Data Protection Law and the European General Data Protection Regulation, contributing to the discussion and interpretation of these laws.
Keywords*: Data protection; Treatment Agents; Civil responsability; Access Providers; Application Providers*

1 INTRODUÇÃO

> "There are only two types of companies: Those that have been hacked and those that will be hacked." (MÜELLER, 2018)

Por muitos anos houve uma limitação no que tange a informação em massa. Com o surgimento da internet tudo mudou, influenciando desde a globalização, até mesmo na personalidade das pessoas. A sociedade atual conta com inovações em todas as áreas, sejam inovações culturais, políticas, econômicas ou jurídicas. Com o avanço da tecnologia o compartilhamento de ideais e opiniões transcendeu, rompendo diversas barreiras e, consequentemente, ampliando o direito para além das matérias estudadas nas universidades.

A internet, com seu avanço, possibilitou difusão de dados com grande velocidade e muitas pessoas. A partir disso começou a discussão e reflexão no que tange os limites desse impacto global e em relação aos efeitos do ambiente digital no dia a dia. Com a circulação em massa de informações pessoais, o aumento no número de casos de violações de dados foi significante. O direito da personalidade foi atingido, visto que há muita exposição de informações pessoais. Portanto, muitas práticas vinham despertando a preocupação no âmbito jurídico, visto que o acesso indevido a dados pessoais estava crescendo. Diferente do que dizem, a internet não é uma terra de ninguém.

Com uma nova forma de vida e acessos ilimitados a qualquer tipo de conteúdo de qualquer lugar do mundo, o direito precisou se adaptar para suprir as novas necessidades que surgiram. Diante de uma vasta e incontável mudança no âmbito digital, foi preciso consolidar um entendimento no direito, principalmente o que diz respeito a responsabilidade civil. Faz-se necessário estabelecer um limite diante das incontáveis mudanças ocorridas com o direito digital.

Além disso, foi de suma importância adaptar normas já existentes em um contexto atual, a fim de atingir o objetivo final. As relações pessoais geram conflitos que precisam ser resolvidos tendo como base o direito. Se antes a responsabilidade era entre duas pessoas, hoje isso aumentou consideravelmente. Esse debate ganhou força e espaço no âmbito jurídico e o grande questionamento é: até onde vai a responsabilidade civil no direito digital? É preciso analisar quem são os responsáveis pelo tratamento de dados pessoais.

A pesquisa trata da regulação específica para esse assunto e como ela influencia a responsabilidade civil no direito brasileiro. Com a legislação vigente percebe-se que o número de responsáveis cresce cada vez mais, diante das diversas ramificações da rede. O direito, portanto, entra em cena para dar a resposta que falta para tantos problemas envolvendo servidores e usuários da internet.

O objetivo geral e principal da presente pesquisa diz respeito a análise da responsabilidade dos provedores de acesso sob a ótica da *General Data Protection Regulation* europeia (GDPR) e a Lei Geral de Proteção de Dados brasileira (LGPD).

A metodologia do trabalho se baseia na técnica analítica, com foco principal no ordenamento jurídico e nas duas leis específicas. Terá a grande presença da hermenêutica interpretativa, visto que a meta é compreender as normas acima citadas e analisar com afinco o tópico de responsabilidade civil de destas as leis.

2 A LEGISLAÇÃO DE PROTEÇÃO DE DADOS NO BRASIL E NA EUROPA

2.1 *GENERAL DATA PROTECTION REGULATION* (GDPR)

O Regulamento Geral de Proteção de Dados europeu (EUROPA, 2016) é uma normatização abrangente de proteção de dados que foi adotado pela União Europeia (UE) em 2016, entrando em vigor em 25 de maio de 2018. O GDPR substitui a Diretiva de Proteção de Dados anterior de 1995 e foi idealizado para fortalecer e unificar a proteção de dados para indivíduos dentro da UE.

Ele se aplica a qualquer indivíduo ou organização que processe dados pessoais de residentes da UE, independentemente de sua localização. Isso inclui controladores e processadores de dados, sejam eles baseados na UE ou não, que processam dados pessoais de indivíduos localizados na UE.

O regulamento define dados pessoais como qualquer informação relacionada a um indivíduo identificado ou identificável, como nome, endereço, endereço de e-mail, número de telefone, endereço IP e outros dados semelhantes.

Ao abrigo deste regulamento, os indivíduos têm o direito de aceder aos seus dados pessoais, solicitar a correção de dados inexatos, opor-se ao tratamento dos seus dados, solicitar a eliminação dos seus dados e solicitar a portabilidade dos seus dados para outro prestador de serviços.

As organizações devem cumprir vários princípios, como minimização de dados, limitação de finalidade, transparência, segurança e responsabilidade. O GDPR também exige que as organizações obtenham o consentimento explícito dos indivíduos antes de processar seus dados e adotem medidas para garantir a segurança e a confidencialidade dos dados pessoais. Além disso, é importante salientar que, para atender aos seus requisitos e se isentar de responsabilidade, as empresas devem demonstrar que estão em conformidade com os princípios do GDPR.

O não cumprimento do GDPR pode resultar em multas de até € 20 milhões ou 4% da receita global da organização, o que for maior. Além disso, os indivíduos têm o direito de entrar com ações judiciais buscando indenização por violações de seus direitos de proteção de dados.

No geral, o GDPR visa proteger a privacidade e os dados pessoais de indivíduos na UE e promover uma cultura de proteção de dados e privacidade em toda a UE. Este regulamento tornou-se o padrão global para proteção de dados e privacidade, e muitos países adotaram leis semelhantes com base em seus princípios, como ocorreu com o Brasil.

2.2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Entre nós, a Lei Geral de Proteção de Dados (LGPD) é uma legislação abrangente de proteção de dados que rege a coleta, uso, armazenamento, processamento e compartilhamento de dados pessoais no Brasil. A lei foi aprovada em 14 de agosto de 2018 e entrou em vigor em 18 de setembro de 2020.

O surgimento de tão necessária normatização, foi impulsionado pelos escândalos mundiais de vazamento de dados, como o caso de Edward Snowden (G1, 2013), que fomentou a criação do Marco civil da Internet, Lei nº 12.965, de 23 de abril de 2014, que estabeleceu os primeiros princípios norteadores, garantias primordiais, direitos e deveres para o uso da Internet no Brasil. Posteriormente, a LGPD foi aprovada em 14 de agosto de 2018, tinha previsão de entrar em vigor no dia 14 de agosto de 2020, mas entrou em vigor somente em 18 de setembro de 2020.

Esta norma se aplica a qualquer indivíduo ou organização que processe dados pessoais no Brasil, independentemente de sua localização. Isso inclui controladores e processadores de dados, sejam eles baseados no Brasil ou não, que processam dados pessoais de brasileiros localizados em território nacional.

Ela define dados pessoais como qualquer informação que identifique ou possa ser usada para identificar um indivíduo, como nome, endereço, endereço de e-mail, número de telefone, endereço IP e outros dados semelhantes.

Assim, de acordo com esta lei, os indivíduos têm o direito de acessar seus dados pessoais, solicitar a correção de dados inexatos, opor-se ao processamento de seus dados, solicitar a exclusão de seus dados e solicitar a portabilidade de seus dados para outro provedor de serviços.

Por outro lado, as organizações, tanto públicas como privadas, devem cumprir vários princípios, como minimização de dados, limitação de finalidade, transparência, segurança e responsabilidade. A LGPD também exige que as organizações obtenham o consentimento explícito dos indivíduos antes de processar seus dados e adotem medidas para garantir a segurança e a confidencialidade dos dados pessoais.

O descumprimento da LGPD pode resultar em multas de até 2% da receita bruta da organização no Brasil, limitadas ao máximo de R$ 50 milhões (aproximadamente US$ 9 milhões de dólares americanos). Além disso, os indivíduos têm o direito de entrar com ações judiciais buscando indenização por violações de seus direitos de proteção de dados.

De modo geral, a LGPD visa proteger a privacidade e os dados pessoais dos indivíduos no Brasil e promover uma cultura de proteção de dados e privacidade no país.

Percebe-se que, tanto a Lei Geral de Proteção de Dados brasileira, assim como, a General Data Protection Regulation europeia, são, sobretudo, leis principiológicas, o que significa dizer que constituem uma série de princípios que possuem como objetivo maior conferir proteção aos dados dos cidadãos, que são os vulneráveis, impondo todo o amparo jurídico concedido ao titular dos dados é, na prática, a efetiva aplicação de um princípio contemplado.

Existem outras normas que tratam de forma direta, ainda que setorial sobre proteção de dados pessoais, como a Lei do Cadastro Positivo (Lei nº 12.414/11), o Marco Civil da Internet (Lei nº 12.965/14) e a LAI – Lei de Acesso à Informação (Lei nº 12.527/11).

3 CONCEITO DE DADOS PESSOAIS E SEU DEVIDO TRATAMENTO

Enquanto a LGPD conceitua dados pessoais em seu art. 5º, I, como "informação relacionada a pessoa natural identificada ou identificável." Destaca de forma genérica que os dados sensíveis são as informações de "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" (art. 5º, II).

Salienta MENESES e COLAÇO:

> Anteriormente à lei, essa prática estava situada no vasto campo da licitude, sendo integralmente permitida até que esbarrasse nos limites do que estivesse expressamente proibido por lei. Agora a situação se inverteu e o tratamento dos dados passa a se sujeitar a objetivos, finalidades, interesses e princípios próprios. 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).

No conceito de dados, inclui até aquelas informações que não se prestam a identificar a pessoa quando usadas isoladamente (IP, faixa etária, altura etc), mas que poderão fazê-lo se conjugadas com outros dados, são, portanto, identificáveis".

Diferente do que chama de dado anonimizado que é aquele que não implicará, em definitivo, a identificação do seu titular, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (art. 5º, III).

A lei estabelece as hipóteses que autorizam o tratamento de dados pessoais. As hipóteses são as bases legais, previstas em lei, que deverão ser utilizadas para justificar o tratamento dos dados pessoais. Isto quer dizer que a coleta de dados pessoais, deverá ter uma finalidade específica e uma base legal legítima que justifique o seu tratamento.

O tratamento de dados envolve as ações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Ao realizar esse tratamento de dados, caberá ao controlador a obrigação de fundamentar cada atividade de tratamento em uma das bases legais estabelecidas pela lei. Portanto, o tratamento feito de forma discricionária, será considerado ilícito.

Assim, há um rol exemplificativo que dispõe que os dados pessoais consistem em nome, RG, CPF, gênero, data de nascimento, local de nascimento, filiação, telefone, endereço residencial, cartão ou até mesmo dados bancários. Sobre isso o artigo 5º da Lei nº 13.709 de 2018 dispõe que:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

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 nossas preferências. Os endereços de IP e os cookies também são dados pessoais que são fornecidos inconscientemente na maioria das vezes. Dentre todos esses dados, a LGPD também deu atenção aos dados

pessoais sensíveis. Estes dados são relacionados à origem étnica e racial, opiniões políticas, convicções religiosas e, até mesmo, dados relacionados à saúde e orientação sexual, além de condenações penais, filiação a sindicato ou organização de caráter religioso, filosófico ou político e até mesmo genéticos.

Não se pode esquecer que os sistemas operacionais alimentam seus servidores, como é o caso do Google, como milhares de informações sensíveis sobre os seus usuários. Tais como, informações sobre nos procura de informações pelos usuários nos motores de busca, o que gera um perfil de consumidor desses usuários. Este perfil é negociado com fornecedores de produtos. É oferecer a quem quer vender, usuários que querem comprar.

Além desses, também há dados que muitos fornecem mesmo que de maneira inconsciente. Um bom exemplo é a localização via GPS, muito comum em nossos aparelhos de telefonia celular. Se estas informações sobre as nossas localizações não forem consideradas como dados sensíveis e não serem protegidas pela inviolabilidade, pessoas maliciosas poderiam ter acesso a dados sobre a localização em tempo real de pessoas, o que ocasionaria uma uma insegurança global e generalizada. Mas, a questão do que são os chamados dados sensíveis e o que deveriam ser assim considerados, mas ainda não são, deve ser objeto de uma maior e detida consideração em outra pesquisa.

Também é importante dispor sobre as violações de dados e como elas acontecem. Há vários ataques cibernéticos atualmente, por isso que os dados, principalmente online, estão tão vulneráveis com o avanço das tecnologias. Um caso que ficou mundialmente conhecido e consequentemente fez com que empresários ficassem com medo foi o que aconteceu com o Facebook. Foi um caso que só se deu por negligência e causou o vazamento de dados de milhões de usuários da rede social para uma empresa britânica de marketing político. A empresa foi condenada a pagar US$ 5 bilhões nesse caso específico. (THE GUARDIAN, 2021).

A lei protege informações relacionadas aos dados sensíveis dos usuários, dentre outros. De acordo com a LGPD, é direito do usuário ter acesso a absolutamente todos seus dados pessoais, sendo possível, portanto, seu pedido para atualização, bloqueio ou até mesmo eliminação dos dados. Isso não exclui o fato de que há a oportunidade de se requerer reparação dos danos no poder judiciário.

4 A RESPONSABILIDADE CIVIL DOS PROVEDORES

4.1 BRASIL

No Brasil, a Lei de proteção de dados foi antecedida pelo Marco Civil da Internet (Lei nº 12.965/2014), que surgiu como referência 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.

Conforme prevê o artigo 11 da referida lei:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Nesse dispositivo legal, percebe-se que o princípio da privacidade foi protegido. Verifica-se, portanto, que 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 marco civil foi 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 buscadas por meio da conexão com a internet. Resumindo, ele proporciona aos usuários várias funções, como por exemplo o armazenamento de dados e disponibilidade de conteúdos.

Nota-se que a Lei nº 12.695/2014, o chamado Marco Civil da Internet, 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.

Esta lei focou em delitos praticados apenas online, os chamados crimes cibernéticos. Ela 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 a 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.

Alguns direitos e garantias dos usuários no MCI: 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 da 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. A Lei nº 12.965/2014 dispõe em seus artigos 18 e 19, respectivamente:

> Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
>
> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

Como já foi visto anteriormente, 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 a 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 de que a restauração dos danos causados a privacidade demoraria de maneira significativa, visto que a via judicial é sempre demorada. 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 dispõe os autores Irineu Francisco Barreto Junior e Beatriz Salles Ferreira 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, como o sistema europeu em relação as imunidades disponibilizadas para os provedores de acesso. No entanto, o sistem *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 a 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 a 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, a segunda lei a ser analisada na minha pesquisa. Ela veio justamente para suprir essas lacunas. A LGPD cria diretrizes que sea aplicam tanto nas relações on-line e off-line, diferente do MCI que tinha

como principal objetivo dispor sobre direitos e garantias para os usuários da internet.

Entre nós, 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 e 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 repasse de informações pessoais sem autorização do titular.

O fundamento do Código de Defesa do Consumidor, 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 Lei nº 13.709/2018, que criou a Lei Geral de Proteção de Dados Pessoais (LGPD), 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 e 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 os dados pessoais dos usuários.

Com a Lei nº 13.709/2018, o Brasil entrou para a lista dos países que tem 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.

O artigo 7º desta lei dispõe que:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Verifica-se pelo conteúdo do dispositivo legal, que será proibido utilizar os dados pessoais se forem para uma finalidade diversa daquela que foi previamente acordada com o cliente, ou seja, o usuário que 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 a 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 baseavam no Código de Defesa do Consumidor. 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 outro deverão obedecer aos artigos 42 ao 45 da referida lei, sendo possível a inversão do ônus da prova, assim como ocorre no CDC. A LGPD prevê que:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao

> controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

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 a 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.

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, pois de acordo com o artigo 43 da LGPD:

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

Mas porque é viável utilizá-la nas relações de consumo? O motivo por esse tipo de responsabilidade objetiva ser usada, principalmente no CDC, se justifica pela vulnerabilidade e hipossuficiência 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 deixa 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 a 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. POsicção essa defendida por Doneda (2016).

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 descumprimento das obrigações impostas pela LGPD. Nesse caso também ocorre a culpa.

4.1 EUROPA

O Regulamento Europeu Geral de Proteção de Dados (GDPR) é um marco da legislação que fornece uma estrutura abrangente para proteger os dados pessoais de indivíduos na Uunião Europeia. Ele estabelece regras para empresas e organizações em relação à coleta e processamento de dados pessoais e dá aos indivíduos o direito de acessar e controlar os dados coletados sobre eles. O GDPR também fornece maior transparência, responsabilidade e segurança para todas as atividades de

processamento de dados pessoais, ajudando a garantir que os dados dos indivíduos sejam tratados com responsabilidade e respeito à sua privacidade. Ao implementar o GDPR, a UE se estabeleceu como líder em proteção de dados e lei de privacidade e deu o exemplo para outros países ao redor do mundo. O regulamento é considerado complexo, extenso e sua linguagem muitas vezes ambígua, o que dificulta sua interpretação e implementação.

A lei proteção de dados brasileira, surgiu sendo pautada por diversos princípios, sugestionada pelo regulamento de dados europeu, que, alías, influenciou a legislações de muitos países sobre esse assunto.

Entre 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. 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.

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 conforme tratado no artigo 4.º, alínea 12 do GDPR 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, por exemplo, 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 ensejar dano moral e até mesmo patrimonial. O *spam* e o tratamento ilegal dos dados também fazem com que incida os artigos referentes a responsabilidade civil.

Alguns comparativos entre os textos das leis são necessários, visto que, no que tange ao tratamento de dados sensíveis, a LGPD, em seu art. 11, II, ‘b’ e ‘g’, prevê proteção especial aos chamados dados sensíveis, sendo que este tratamento apenas poderá ocorrer nas hipóteses previstas na lei, independente do consentimento do titular. Neste memo ponto, a GDPR,

em seu art. 9º, §2º, ‘d’ e ‘e’, proíbe o tratamento de dados sensíveis, estabelecendo sobretudo algumas exceções. No que diz respeito aos dados de envolvendo crianças e adolescentes, a LGPD, em seu art. 14, §1º, estabelece que o tratamento de seus dados pessoais deverá ser realizado com o consentimento específico de um dos pais ou pelo responsável. A GDPR já aceita o consentimento dado por adolescentes, desde que tenham pelo menos 16 anos e para os menores de 16 anos, o consentimento deve ser dado pelos pais, conforme o art. 8º, §1º.

Podemos concluir, então que, tanto o GDPR quanto a LGPD, preveem garantias de que as previsões normativas sejam efetivamente observadas. A distinção prevista por ambas as leis, no tocante ao tratamento dos dados sensíveis, é um indicativo do desejo do legislador de impedir a utilização de dados para finalidades discriminatórias ou para obtenção de vantagem econômica, como é bastante comum acontecer. No entanto, a identificação da correta utilização desses dados, não nos parece ser tarefa simples.

Como exemplo, Carlos Nelson Konder levanta a questão da nacionalidade, “como uma informação que poderia não ser comumente qualificada como sensível, mas que, se questionada em um determinado contexto, pode ser um indicativo de estigmatização.” (Carlos Nelson Konder apud TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. 2019, p.455).

5 CONCLUSÃO

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 que evite 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 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 esta 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 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 provedores de acesso à internet podem ser responsabilizados de várias maneiras, tanto no campo civil, como também na seara criminal, incluindo: a calúnia, injúria ou difamação, quando hospedam ou transmitem conteúdo atentatório à honra das pessoas;

Por outro lado, também podem ser imputada responsabilidade por atos de censura, ao restringir o acesso a conteúdo legal. Da mesma, forma pode ser repreendido quando, por ordem emanada de autoridade competente, não limitar o acesso à informação falsa, fraudulenta ou distorcida, que cause prejuízos alheios.

Assim, da mesma forma a negligência é motivo sancionador. Tanto na negativa de se restringir dados como em não fornecer medidas de segurança adequadas para proteger os dados do usuário, como ocorrer nas

situações de invasão de privacidade, quando nção mantém medidas assecuratórias de possam inviabilizar a exposição de dados, violando-se assim os direitos de privacidade de seus usuários. Ocorrendo também na forma ativa, ao divulgar informações pessoais dos usuários.

Não de pode olvidar da violação de direitos autorais quando conscientemente fornecerem acesso a material pirateado.

Verificou-se que responsabilidade dos provedores de acesso à internet varia de acordo com a jurisdição e as circunstâncias específicas de cada caso. É importante que os servidores de rede entendam as leis e regulamentos que se aplicam aos seus negócios e tomem medidas para minimizar sua possível exposição à responsabilidade civil.

REFERÊNCIAS

Agência PF (Notícias Antigas), 2016. **PF combate crime de pornografia infantil na DeepWeb.** Disponível em: <http://www.pf.gov.br/agencia/noticias/2016/11/pf-combate-crime-de-pornografia-infantil-na-deep-web>. Acesso em: 10 set.2019.

BARRETO JÚNIOR, Irineu Francisco; LEITE, Beatriz Salles Ferreira. 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, 2017.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **civilistica. com**, v. 9, n. 3, p. 1-23, 2020.

BRASIL, **Lei n º 10.406, de 10 de janeiro de 2002**. Institui o Código Civil.

BRASIL, **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências.

BRASIL, **Lei nº 13.709 de 14 de agosto de 2018**. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL, **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Direito digital e proteção de dados pessoais**, São Paulo, ano 21, n. 53, jan - mar 2020. Cadernos Jurídicos, p. 163-170.

DIVINO, Sthéfano Bruno Santos; DE LIMA, Taisa Maria Macena. Responsabilidade Civil Na Lei Geral De Proteção De Dados BRASILEIRA. **Revista Em Tempo**, v. 20, n. 1, 2020.

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

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2016.

EUROPA. **General Data Protection Regulation (GDPR).** Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 10/09/2022.

G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. Mundo. Disponível em: https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 10/09/2022.

GODOY, Claudio Luiz Bueno de. **Responsabilidade Civil pelo Risco da Atividade**. 2. ed. São Paulo: Saraiva, 2010.

GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 15ª ed. . São Paulo, Saraiva, 2014.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** 2. ed. São Paulo: Revista dos Tribunais, 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **Lei geral de proteção de dados - comentada**. São Paulo: Revista dos Tribunais, 2019.

MARQUES, Paula Cristina Mariano, FRANCISCO, José Carlos. Ma**rco civil da internet e responsabilidade civil na violação a direitos da personalidade**. 2015. Disponível em: http://dspace.mackenzie.br/handle/10899/23874 Acesso em: 06/10/2022.

MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à nova lei de proteção de dados** (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. REVISTA DE DIREITO DO CONSUMIDOR, v. 120, p. 555, 2018.

MIRAGEM, Bruno. A lei geral de proteção de dados (lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais, São Paulo, v. 1009, p. 173-224, nov. 2019.

MUELLER, Robert S. in Dynamic Business. There are two types of companies: Those who know they've been hacked & those who don't. BARNES, Stephen. Disponível em: https://dynamicbusiness.com/locked/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html. Acesso em: 06/10/2022.

MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas**. 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: 11. ago. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de Direitos Fundamentais: uma análise à luz da Lei geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 2018.

NOVAES FILHO, Pedro Paulo Vieira de. A lei geral de proteção de dados: a responsabilidade civil dos fornecedores pelo tratamento inadequado dos dados pessoais. 2020. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade de Direito de Vitória, Vitória, 2020. Disponível em: http://repositorio.fdv.br:8080/handle/fdv/996. Acesso em: 06/12/2021.

SANTIAGO, NAJLA DE FARIA. A responsabilidade civil dos provedores de serviços de internet A responsabilidade civil dos provedores de serviços de internet.

SHIMABUKURO, Rafael Mitsuo Suyama. A RESPONSABILIDADE CIVIL NA NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. **Intertem@ s ISSN 1677-1281**, v. 38, n. 38, 2019.

SIMÃO FILHO, Adalberto. Sociedade da informação e seu lineamento jurídico. In: PAESANI, Liliana Minardi (Coord.). **O direito na sociedade da informação.** São Paulo: Atlas, 2007.

SOUZA, Carlos Affonso Pereira de**. Responsabilidade Civil dos Provedores de Acesso e de Aplicação de Internet**: Evolução Jurisprudencial e os Impactos da Lei Nº12.965/2014 (Marco Civil da Internet). São Paulo: Atlas, 2014.

SOUZA, C. A.; LEMOS, R. **Marco civil da internet**: construção e aplicação. V. 1. 1ª ed. Juiz de Fora: Editar, 2016.

TEFFÉ, Chiara Antonia Spadaccini. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros, de acordo com o Marco Civil da Internet. **Revista Fórum de Direito Civil-RFDC, Belo Horizonte, ano**, v. 4, p. 3, 2015.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters (Revista dos Tribunais), 2019.

THE GUARDIAN. **Facebook data leak: details from 533 million users found on website for hackers.** Mon 5 Apr 2021 06.30 BST. Disponível em: https://www.theguardian.com/technology/2021/apr/03/500-million-facebook-users-website-hackers. Acesso em 01/05/2021.

TRISTÃO, Manuela Albertoni; PEDROSO, Temis Chenso da Silva Rabelo. RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, v. 16, n. 16, 2020.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados**. Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN. Acesso em 06/12/2021.

VENOSA, Sílvio de Salvo. **Direito civil responsabilidade civil.** 11ª ed. São Paulo: Atlas, 2011.