2022
FLUXO CONTÍNUO
Ed. 36 - Vol. 2. Págs. 492-513

JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL ISSN: 2526-4281 - QUALIS B1

LEI DE PROTEÇÃO DE DADOS: A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS NA RELAÇAO DE CONSUMO

DATA PROTECTION LAW: THE CIVIL LIABILITY OF PERSONAL DATA PROCESSING AGENTS IN THE CONSUMER RELATIONSHIP

Lucas da Silva SOARES
Faculdade Católica Dom Orione (FACDO)
E-mail:
lucasdasoares@catolicaorione.edu.br

Daniel Cervantes Angulo VILARINO
Faculdade Católica Dom Orione (FACDO)
E-mail:
danielcervantes@catolicaorione.edu.br

RESUMO

Este artigo tem como propósito ponderar sobre a repercussão da instituição da Lei Geral de Proteção de Dados (LGPD) e no direito do consumidor brasileiro, em particular no que se refere à responsabilidade civil no tratamento inadequado de dados pessoais por agentes de tratamento de dados. Inicialmente, o direito que frisa a proteção de dados pessoais antecede a LGPD, que pode ser verificada na Constituição Federal 1988, Código Civil de 2002, Código de Defesa do Consumidor e Marco Civil da Internet. A LGPD vem acrescentar a legislação anterior. Em ato contínuo, analisa a Responsabilidade civil no direito brasileiro. Por fim, analisando a legislação e doutrina, este trabalho sopesa os agentes de tratamento de dados são objetivamente responsáveis pelos danos causados pelo incumprimento das suas atribuições de proteção de dados pessoais que estão presentes no referido regulamento.

Palavras-chave: Dados Pessoais. Lei de proteção de dados. Privacidade. Responsabilidade Civil.

ABSTRACT

The purpose of this article is to consider the impact of the implementation of the General Data Protection Law (LGPD) and on Brazilian consumer law, in particular not referring to civil liability in the inappropriate treatment of personal data by data processing agents. . Initially, the right that emphasizes the protection of personal data precedes the LGPD, which can be verified in the Federal Constitution 1988, Civil Code of 2002, Consumer Defense Code and Marco Civil da Internet. The LGPD adds to the previous legislation. In a continuous act, it analyzes civil liability in Brazilian law. In order to work, analyzing the legislation and the doctrine, this legislation aims at those responsible for the processing of data by data are compliance with the agencies responsible for the protection of personal data that are present in the said regulation.

Keywords: Personal Data. Data Protection Act. Privacy. Civil responsability.

INTRODUÇÃO

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) adveio para regulamentar e fiscalizar em qualquer relação que haja tratamento de informações enquadradas como

dados pessoais. Em particular, no que diz respeito á responsabilidade civil do tratamento indevido do fluxo e monitoramento dos dados pessoais por agentes.

Em ato contínuo, verifica-se a responsabilidade civil brasileira. No período de 1916, o Código Civil dispunha a responsabilidade subjetiva era a padrão. No entanto, isso mudou com o surgimento da Lei de Defesa do Consumidor, em que passou a estipular a responsabilidade civil objetiva dos fornecedores.

O Código Civil de 2002, ainda que preveja a responsabilidade como regra subjetiva, reconhecendo a responsabilidade civil objetiva quando exigido por lei, ou quando o dano causado pelo autor acarrete em risco aos direitos de outros.

A LGPD não é clara quanto à responsabilidade civil aplicável em caso de danos ocasionados por os agentes de tratamento de dados, por não cumprir com seus termos. No entanto, a doutrina difere no formato da responsabilidade civil no teor da Lei Geral de Proteção de Dados (LGPD). Uma corrente apoia que a responsabilidade é subjetiva, desde que suceda a evidência de violação da lei.

Portanto, este artigo não pretende ser exaustivo sobre os tópicos, em primeiro lugar momento sugeriu que fosse trazido à tona e abordado os artigos da Lei Geral de Proteção de Dados (LGPD), inerentes á responsabilização dos agentes de tratamento.

Como resultado da pesquisa, o artigo conterá os principais argumentos, por sua vez, por um lado, aqueles que acreditam que o sistema aplicável é de responsabilidade subjetiva, e por outro ponto de vista atual da defesa da responsabilização objetiva dos agentes que provém de uma abordagem civil-constitucional, doutrina analítica, legislação e as filosofias a contar da perspectiva das convicções e valores constitucionais.

Com base em pesquisas desenvolvidas sob a perspectiva de caráter dedutivo, com base em bibliografias e estudos existentes sobre leis norteadoras sobre o tema.

Este artigo empreende analisar certos aspectos da Lei Geral de Proteção Dados (LGPD). A principio este artigo, será delineado os aspectos históricos da Lei Geral de Proteção de Dados, abarcando os dispositivos além daqueles inerentes á responsabilidade civil.

Portanto, verifica-se que há outros diplomas protetivos para lidar com a proximidade sistêmica da nova lei. Em sequência, trata-se de algumas minúcias do novo regime, a contar da experiência jurídica anterior.

A EVOLUÇÃO LEGAL DA PROTEÇÃO DE DADOS NO BRASIL

Segundo Doneda (2020), os direitos e garantias encontram-se disciplinados no artigo 7º da Lei nº 12.965 de 23 de abril de 2014, designada como Marco Civil da internet, ipsis verbis:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV – não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V – manutenção da qualidade contratada da conexão à internet; VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; XII – acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e XIII – aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet (BRASIL, 2014. grifo nosso).

Verifica-se que há trezes incisos elencados no artigo 7º do Marco Civil da internet, mas apenas oito incisos aludem sobre a proteção de dados pessoais, já as demais versam da não suspensão da conexão a internet, com ressalva ao débito (inciso IV), qualidade do serviço (inciso V), direito a informação sobre politicas de uso (inciso XI), acessibilidade (inciso XII) e a utilização do Código de Defesa do Consumidor (inciso XIII).

Como se observa, a Lei supracitada versa nos três primeiros incisos a inviolabilidade do fluxo de comunicações efetuados pela internet e da confidencialidade das comunicações privadas amarzenados.

Conforme a leitura do inciso II, as conversas movimentadas através do e-mail,podem ser controladas no caso de serem determinadas por autorização judicial. Ademais, no caso do celular de alguém for apreendido, poderá ter acesso ao Whatssap ou outro meio de comunicação, apenas se for levantado por meio de detrminação judicial (inciso III).

Porventura, se essas garantias não sejam atendidas, a pessoa que foi prejudicada poderá pleitear o compensação por danos materiais e morais que deriva da sua ofensa (inciso I) e a comprovação que eventualmente aquirida passará a ser ilicita.

Dispõe o inciso VI, sobre o direito a informação precisa e completas nos contratos de prestações de serviços, com enfâse para o registros de conexões e transcrições de acesso a aplicações de internet.

O decreto nº 8.771 de 11 de maio de 2016 regido a Lei 12.965/2014 e veio complementar a lei nº 12.965, versando sobre guarda e proteção de dados de usuários por provedores de conexão e aplicação, in verbis:

Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I – o estabelecimento de controle estrito sobre o acesso aos dados me- diante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II – a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III – a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e IV – o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

> [...] Art. 16. As informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, respeitado o direito de confidencialidade quanto aos segredos empresariais (BRASIL, 2016).

Já o inciso VII discorre sobre a possibilidade dos dados serem fornecidos a terceiros, por sites colaboradores dos provedores de conexão ou aplicação, se possuírem anuência livre taxativo e informado.

Portanto, o usuário possui o direito de recusar a transferência de seus dados, do mesmo modo o relatório da navegação, a terceiros.

Ademais, é necessário que possua informações claras sobre coleta, uso, armazenamento, tratamento e proteção dos dados, nos moldes do inciso VIII, que ele só pode ser usado para os fins que de seu recolhimento, sem vedação, e de acordo com o indicado nos termos de uso.

Em conformidade com o inciso IX, versa sobre ‘‘a coleta, uso, o armazenamento e qualquer tratamento de dados pessoais’’ (BRASIL, 2016). No qual incorre sob consentimento expresso do interessado. Em função disso, o tratamento de dados necessita autorização na janela especifica, sendo insadisfatório o consentimento em geral disponibilizado da adesão aos termos de uso e politicas de privacidade da empresa.

Nos moldes do artigo 7º da Lei nº 12.965/2014, a qual prescreve no artigo 13 do Decreto nº 8.771/2016, in verbis:

> Art. 13. Omissis. [...] § 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos: I – tão logo atingida a finalidade de seu uso; ou II - se encerrado o prazo determinado por obrigação legal.

Verifica-se reiteradas afrontas praticadas por empresas no tratamento de dados pessoais. A precaução de dados consolidados no meio digital, não submetendo a limitação, ainda comportando outras normas utilidades em legislação, consoante o Código de Defesa do Consumidor e as leis do Cadastro Positivo nº 12.414/2011 e acesso á informação nº 12.527/2011, sem descuidar da garantia fundamental á vida privada, resguardada no artigo 5º, X, da Constituição Federal.

Foi moroso o ordenamento jurídico brasileiro em preceituar sobre o direito digital, vez que retardou em usufruir de alguma tutela os dados pessoais no espaço cibernético em algum diploma legislativo (PURKYT, 2018).

Não estatuiu a Constituição Federal de 1988 de modo especifico o conteúdo de proteção de dados no ciberespaço, vez que a lei maior ser antecessora a difusão da internet como forma de propagação de informação. O texto constitucional abrange os fundamentos

para a proteção de dados pessoais, e versa sobre um regulamento que se aproxima da noção atual da proteção de informações pessoais que é o Habeas Data, quer dizer, obtenha os dados. (PURKYT, 2018).

Conforme a Constituição Federal no artigo 5º, inciso LXXII, a qual discorre sobre o habeas corpus elencado nos direitos fundamentais:

LXXII - conceder-se-á habeas data:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (BRASIL, 1988).

Dessa maneira, o artigo sipracitado aduz que o Habeas Datas possui certa delimitação cerca da proteção de dados pessoais, vez que autoriza que apenas o sujeito obtenha acesso as bases em bancos de dados governamentais ou então natureza pública, decorrendo quaisquer propósitos em relação ao banco de dados privados.

Posteriomente em 11 de setembro de 1990, foi validada a Lei nº 8.078 o Código de Defesa do Consumidor CDC, que discorre no artigo 43 sobre o cadastro dos consumidores inserido em bancos de dados, o qual devem fornecer as informações aos consumidores do conteúdo em cadastros, fichas, registros com dados e informações de consumo arquivados sobre ele, tanto quanto devendo indicar sobre a origem dos dados auferidos. Outrossim, o § 2º, determina que as empresas informem o consumidor quando for feito um cadastro sobre ele, mesmo que não o requisite (BRASIL,1990).

Nossa legislação processual penal brasileira abriga os dados transferidos através de ligação telefônica ou informática sob Lei 9.296 de 24 de julho de 1996, intitulada como lei de interceptação telefônica que norteia o inciso XII do artigo 5º da Constituição Federal (BRASlL, 1996).

A lei não exprime minuciosamente sobre a proteção de dados pessoais transmitidos através do telefone ou internet, mas resguarda ao movimento de comunicação exercido por tais meios, conhecendo da intercepção sem autorização judicial ou para fins não autorizados por lei (FORTES, 2016).

Foi instituído em 2002 o Código Civil Brasileiro regulado pela Lei nº 10.406, que confere o capítulo II integral aos direitos pertinentes à personalidade dos indivíduos, reportando o dispositivo constitucional remotamente contido de proteção da vida privada, e

até mesmo proporcione a atuação judicial para tomar as medidas necessárias para impossibilitar ou interromper qualquer meio de violação de tal preceito, como se retira do artigo 21 do Código (BRASIL, 2002).

Segundo Fortes (2016), a Lei nº 12.527 sancionada em 18 de novembro de 2011 denominada como Lei de Acesso a Informação.

A diretriz ocorreu para regulamentar o acesso á informação na forma dos artigos 5º inciso XXXIII, 37 § 3º inciso II, e 216,§ 2º da Constituição Federal de 1988 (BRASIL, 1988).

Todavia, a lei supracitada revela um avanço no que tange a legislação pertinente ao direito digital no Brasil e regularmentação sistemática dos dados pessoais.

Ademais, a Lei 12.527/2011 impõe os entes subordinados a esta, a versarem os dados pessoais com feitio claro, atentando aos direitos fundamentais de intimidade, vida privada, honra e imagem dos indivíduos. Do mesmo modo, restringe o dominio das informações, oferecendo um prazo até 100 (cem) anos para obtenção aos dados, tal como garante o acesso ou exposição a terceiros apenas neste caso de consentimento do titular das informações (BRASIL, 2011).

Em 2011 sobreveio a Lei 12.414/2011, Lei do Cadastro Positivo, estipulando regimento sobre os dados decorrentes de operações e pagamentos financeiros ao consumidor, que proporcionam a autorização de crédito (KRIEGER, 2019).

Trata-se de lei que estabelece o desenvolvimento da concepção da independência informativa no ordenamento, já que conduz o consentimento como indispensável para o distribuição de dados ser lícito.

Seguindo a trilha temporal da legislação brasileira sobre dados, cumpre verificar, em particular a relevância ao Marco Civil da Internet. Esse regimento alcançou supremacia e dispôs seu procedimento legislativo celére depois do evento chamativo de espionagem descoberto por um ex-analista, Edward Snowden da Agência Nacional de Segurança dos Estados Unidos (KRIGER, 2019).

Foi verificado que ocorreu divulgação dessa espionagem no solo brasileiro, o que ensejou a manifestação da presidente Dilma em aderir o regulamento de urgência da lei, resultando na aquiescência do Marco na reunião de governança de muito setores da internet (FORTES, 2016).

Nesta lei, o consentimento e sua adjetivação foram mencionados explicitamente, considerando que, especialmente após o escândalo, busca-se proteção especial para o titular dos dados para envolvê-lo no processo de processamento de dados.

Contudo, esclarece Malheiro (2017), ainda não existe legislação que trate diretamente da proteção de dados propriamente dita, que falta uma legislação mais abrangente que possa delinear normas sobre proteção de dados, especialmente diante da Regulação Geral de Proteção de Dados (GDPR) da União Europeia, que gerou influência em outros países, através da Diretiva 95/46/CE, que é o regimento característico sobre a proteção de dados pessoais e tratamento destes, que vigora desde 1995.

Sendo posteriormente espelhada pela General Data Protection Regulation GDPR Regulação Geral de Proteção de Dados, trazendo uma variedade de definições significantes, com tal força jurídicas que nem ferramentas da área de informação, que fornecem a direção para interpretação da normativa (FORTES, 2016).

Entre outros, a definição de dados pessoais disposto no artigo 2º, que conforme a diretiva são:

> Dados pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa);é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social (UNIÃO EUROPEIA, 1995).

Da mesma forma da concepção do diploma europeu, agora em âmbito nacional, a Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/18, revela em no artigo 5º, inciso I, que ‘‘dado pessoal: informação relacionada à pessoa natural identificada ou identificável’’ (BRASIL, 2018).

Verifica-se que a lei brasileira também expõe um conceito amplo, sem rol exemplificativo, de maneira que viabiliza categorizar qualquer dado como sendo um dado pessoal, independentemente do seu suporte e formato, seja ele apartado ou em grupamento, contanto que possa nomear-se uma pessoa natural.

Os dados pessoais contribuem em abundância de informações, advindo de dados cadastrais nome, endereço e e-mail, a título ilustrativo até dados mais particulares, como raça, saúde, política e informações biométricas do seu titular (MALHEIRO, 2017).

Foi sancionada a primeira criada com o intuito de Lei Carolina Dieckmann (Lei nº 12.737), no dia 30 de novembro de 2012, em decorrência de arquivos copiados e fotos intimas divulgados sem autorização, sendo denominada como Lei de Crimes Cibernéticos, que concede sobre a classificação de crimes praticado pela internet e modifica o Código Penal Brasileiro (BRASIL, 2012).

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave (BRASIL, 2012).

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representacao, salvo se o crime e cometido contra a administracao pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municipios ou contra empresas concessionarias de servicos publicos (BRASIL, 2012).

Ao incorporar os artigos 154-A e 154-B no Código Penal e alterações dos artigos 266 e 298, todos do Código Penal, os legisladores autorizam penalidades aos infratores que cometeram crimes sem o consentimento da vítima hackiada através dos equipamentos de informática para se obter, destruir ou alterar informações pessoas no dispositivo (GONÇALVES, 2020).

Embora tenha sido a lei supracitada criada, com intuito de coibir os delitos virtuais, apontando sanções e regulamentos dos procedimentos. Entretanto, não logrou êxito, vez que houve aumento da incidência destes delitos, e por isso a ineficácia de identificar os infratores.

E todas as evidências encontradas em ambientes virtuais são frágeis e podem gerar danos ou perda de provas coletadas. Todos os esforços de coleta de evidências devem ser realizado por profissional habilitado, pois é difícil encontrar autores (DONEDA, 2020).

A investigação começará com a Notitia Criminis (notícia do crime), que informará policiais, juízes ou promotores sobre o crime, para que engaje uma fase técnica na qual serão verificadas as informações que chegaram às autoridades, o fato de a própria vítima

ser exposta, passando a procurar objetos e materiais que corrobore a prática da atividade criminosa, seja um computador, telefone, dentre outros (DONEDA, 2020).

Quando o objeto causador do ato for encontrado, a polícia fará uma busca no local. Por meio de autorização judicial, como ordem de busca e apreensão de itens será proferida pelo juiz competente para os demais atos investigativo (GONÇALVES, 2020).

Todas essas investigações dependem em parte do que será autorizado pelo magistrado, o que resultará em atraso na busca e poderá acarretar em problemas com a detecção de provas digitais, ações executadas por o delegado de polícia nesta fase inicial, em seguida irá começar a segunda fase da perquirição penal, a ação penal (ANDRADE; MOURA, 2019).

Percebe-se que essas ações causam danos irreparáveis às vítimas, e as consequências são inimagináveis. Intentam invadir sua liberdade e privacidade, porque se sentem vulneráveis, até mesmo há uma sensação de impunidade. Lamentavelmente, a legislação não interveio nesses crimes, as penalidades são as menores em comparação com todas as suas perdas de exposição pessoal, perda de dados pessoais e muitas outras restrições (ANDRADE; MOURA, 2019).

Devido o isolamento social e restrições de ir e vir, de forma imediata, as pessoas usam mais ferramentas sociais, inclusive em ante a epidemia, ademais trabalhar em casa se tornou cada vez mais comum. Os crimes cibernéticos mais comuns são fraude de seguros, roubo dados e informações diversas das pessoas, golpes de benefícios governamentais, roubo de senha e uso indevido de cartões de crédito, dentre outros (DONEDA, 2020).

Outro grande vilão que promove esse tipo de atividade criminosa é a falta de conhecimento em segurança de mídia digital. No Brasil, a população aumentou o acesso a plataformas de tecnologia digital, mas por outro lado não monitoram o processamento e notificação sobre anúncios, ou debates sobre o tema nas escolas. Na realidade, as pessoas estão apenas começando a ter mais acesso a recursos digitais, mas não aprendendo a se resguardar (BIONI, 2020).

Resumindo a gravidade da situação, janeiro de 2021, a maior violação de dados historicamente documentada. Os dados pessoais de cerca de 223 milhões de pessoas foram comprometidos, incluindo informações sobre os mortos. É um grande problema que assola as pessoas e desafia as autoridades (FIGUEIREDO, 2021).

Dessa maneira, é necessário avaliar todos os instrumentos de proteção do ordenamento jurídico fornecido, pois algumas condições estão fora de controle e podem

resultar em danos vítima. Portanto, para dar aos humanos uma maior sensação de segurança no ambiente virtual, É necessário tomar medidas de segurança, incluindo prevenção, para evitar ser vítima desses tipos de crimes.

Conforme Fortes (2016), ressalta que os legisladores estão começando a fortalecer a proteção de dados pessoais, tornando crime hackear equipamentos de computador sem autorização do proprietário.

De acordo com Doneda (2020) o legislador brasileiro teria se guiado através do principio de informação justa (Fair Information Principles), e grande parcela da doutrina nomeia a lei como sendo referência normativa dos princípios de proteção de dados pessoais no Brasil.

No entanto, a legislação do consumidor ainda está mais preocupada em regular as bases de dados do que realmente com a necessidade de consentimento.

Segundo Andrade e Moura (2019), preceitua as leis consumeristas,apesar de que estava mais sensibilizado em regulamentar os bancos de dados, ao invés de considerar como indispensabilidade o consentimento prévio ou arquivamento.

Refere-se a legislação abrange todos os bases de dados que permitem o livre desenvolvimento da personalidade dos consumidores.

Conforme a Lei nº 13.709/18, trata das subespécies sobre dados pessoais definidas como dados sensiveis no Art. 5º, inciso II, da Lei Geral de Proteção de Dados, considera-se dados sensiveis os que tangem sobre raça, saúde, politica, informações biométricas, entre outros (BRASIL, 2018).

Por conseguinte, aqueles dados atinente a uma pessoa determinada ou determinavel que, quando denominada e processadas, têm a capacidade de promover propósito discriminatório ou prejudicial, revelando amplas ameaças para o titular ou então a coletividade, de tal forma que devem ser classificados como sensíveis e ter um tratamento particularizado quanto ao manejo sobre seus usos (ANDRADE; MOURA, 2019).

Conforme Bioni (2020), destaca a matéria exibida pela Universidade de Cambridge, difundido na revista científica PNAS (Proceedings of National Academy of Sciences), que verificou que, com base nas curtidas dos utilizadores na rede social Facebook, possibilitou desenvolver perfis dos usuários, inserindo seus gostos e predileções.

Em desfecho da matéria, os pesquisadores apontam ainda, de acordo com Marineli que “a grave ameaça presente à privacidade da pessoas, decorrentes da utilização desses dados por empresas e instituições governamentais” (MARINELI, 2017, p.200).

Dessa maneira, os dados classificados como de grave ameaça seriam mais cuidadosos e teriam suas pretenções verificadas para impedir maiores transtornos.

Nota-se, a grandeza para tratamento especial de dados confidenciais, atribuindo à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) resguardar uma seção privativa no Capítulo II, Seção II, para proceder sobre as excluivas possibilidades de uso e manipulação dessa subespécie.

Vale destacar que a referida lei, com o propósito de driblar litigios, descarta da espécie de dados pessoais os dados anonimizados (art. 5º, inciso III), que nem aqueles que sucedem por processo de anonimização (art. 5º, inciso XI), ja que não podem eles verificar seus titulares, embora possam se referir à pessoa fisica (BRASIL, 2018).

O referido artigo foi cauteloso ao suscitar uma ressalva no seu artigo 12, cujo dados anonimizados serão classificados pessoais quando o processo empregue para ser revertido, considerando que não há como assegurar a total extinção de nexos de identificação dos dados (BRASIL, 2018).

Deste modo, dada a relevância dos dados pessoais entre à sociedade da informação, em especial aos dados sensíveis, a sua proteção é primordial para abrigar os direitos de seu titular.

Uma grande etapa ao indivíduo estar no comando de suas informações, contudo é indispensável analisar que instituir o consentimento é uma atividade complicada, carregada de desafios e adversidades. Apesar de que há uma extensa trajetória para pôr em prática o princípio da autonomia informativa e conceder uma eficiente proteção ao titular de dados.

Sob o ângulo positivo, é pertinente observar o recente julgamento da Medida Provisória 954/2020, na qual trata a respeito do compartilhamento de dados sobre empresas de telecomunicações que oferecem consultas sobre serviços de telefonia fixa e serviços móveis pessoais juntamente com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) no decorrer da COVID-19, como fundamento de alicerce ao desenvolvimento de estatísticas (BRASIL, 2020).

O julgamento, que estabeleceu a suspensão da Medida Provisória, foi consagrado como um símbolo histórico da proteção de dados no Brasil e revelou uma precaução com o princípio da isonomia informativa e com o conteúdo da Lei Geral de Proteção de Dados Pessoais (LGPD), mesmo que a Lei não esteja ainda em vigor. Entre um dos propósitos que motivou o julgamento, o qual também esteve presente o julgamento no Brasil, o

Tribunal sustentou que havia recolhimento excessivo de dados, além da finalidade adequada (BRASIL, 2020).

A decisão foi significativa em determinar a relevância da Lei de Geral de Proteção de Dados para o ordenamento jurídico e remete ao entendimento de que há um trajeto longo para permitir que o titular dos dados esteja praticamente protegido e imerso na sociedade da informação em que vive, mas que já possui viabilidade e a LGPD é um marco inicial para se realizar a proteção de dados pessoais no Brasil.

REGIME DE RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO Á LUZ DA LGPD

Responsabilidade Civel Subjetiva ou Objetiva dos Agentes de Tratamento

Primeiro, a limitação do proposito de aplicação da responsabilidade civil ao resguardo da Lei Geral de Proteção de Dados. Em outras palavras, é imperativo verificar em que circunstâncias as discussões sobre a falta de clareza relevantes da Lei Geral de Proteção de Dados (LGPD) sobre a natureza do regime de responsabilidade (GONÇALVES, 2020).

Seção III da LGPD, denominada “Da Responsabilidade e do ressarcimento de danos", que traz as principais regras sobre responsabilidade civil, regerá o processamento envolvendo dados pessoais. este item é tratado no art. artigos 42 e 45 da Lei. Como dito anteriormente, isso não esclarece a natureza da responsabilidade civil empregada, cabendo ao legislador decidir, seja ele objetivo ou subjetivo.

O primeiro argumento formal da corrente subjetivista histórica seguindo a tramitação do projeto de lei que teceu a Lei Geral de Proteção de Dados (LGPD). Isto porque quando no processo, algumas referências á responsabilidade objetiva foram removidas. Assim, tem-se argumentado que se o objetivo dos legisladores é estabelecer a responsabilidade objetiva não faz essas alterações (DONEDA, 2020).

Nesse sentido, vale a pena atentar para o artigo 45 da LGPD, segundo o qual "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente” (BRASIL,2018).

De fato, conforme estabelece o art. 14 da Lei de Proteção ao Consumidor, a obrigaç civil é inerentemente objetiva no que tange o consumo entre o agente de processamento e o titular dos dados. Nestes casos, há uma obrigação na administração ilícita de dados

pessoais e consequente prejuízo ao titular dos dados a compensação ocorre quer o agente considere ou não conduta culposa no tratamento dos dados.

Nesse caso, é importante mencionar que a primeira decisão no tocante a obrigação civil por uso impróprio de dados pessoais, foi deliberada por a juiza Tonia Yuka Koroku da 13ª Vara Cível da Justiça Estadual de São Paulo, no processo autos1080233-94.2019.8.26.0100,publicado em 29 de setembro de 2020. Em conclusão, a decisão destaca:

> [...] a responsabilidade da ré é objetiva (arts. 14, caput, CDC e 45, LGPD). Inexiste suporte para a exclusão de responsabilidade (art. 14, § 3º, I a III, CDC), de sorte que caracterizado o ato ilícito relativo a violação a direitos de personalidade do autor, especialmente por permitir e tolerar (conduta omissiva) ou mesmo promover (conduta comissiva) o acesso indevido a dados pessoais do requerente por terceiros. Irrelevante se a ré possui mecanismos eficazes para a proteção de dados, seja porque se sujeita às normas consumeristas em relação à sua responsabilidade, bem como pelo fato de que houve utilização indevida dos dados do requerente em decorrência do contrato firmado entre as partes. Sendo a responsabilidade objetiva, não há suporte para se inquirir a existência de culpa ou a presença de suas modalidades (imperícia, negligência ou imprudência) (BRASIL, 2020).

A discussão supracitada envolvia uma relação contratual entre os cidadãos e uma empresa do setor imobiliário, a qual utilizou dos dados cadastrais da empresa constantes do contrato, a fim de transmitir a terceiros sem consentimento e autorização, causando danos extrapatrimoniais.

As divergências sobre a natureza jurídica dos regimes de responsabilidade são limitados, porque as circunstâncias em que não há inter - relação de consumo entre o titular e o agente de tratamento, desde que nestes casos, o regime de responsabilidade previsto no Código Defesa do consumidor predomine.

Desde que enumerado os princípios da LGPD, a lei tem se preocupado em lidar com a responsabilização dos agentes, acima de tudo quando determina que as atividades de tramento devem seguir, entre outras, principios da segurança,prevenção e da responsabilização.

Especiamente em relação ao regime estipulado no artigo 42, sob a qual estabelece que “O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em

violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (BRASIL, 2018).

Com o objetivo de expandir as possibilidades para as vítimas obterem indenização, a LGPD esclareceu dois casos em que a responsabilidade por indenização por danos civis é solidária.

A primeira delas é a solidariedade entre o controlador e o operador (Art. 42, §1º, I), no que deste "descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador" (BRASIL, 2018)

Por sua vez, será analisada a segunda hipótese sobre a solidariedade, onde duas ou mais controladores pelo tratamento está diretamente envolvido no tratamento de dados pessoais, conforme o artigo 42.º, § 1, II (BRASIL, 2018).

Em continuidade, o artigo 43 esclarece a exclusão da responsabilidade dos agentes de tratamento.

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).

De acordo com os regulamentos, o agente de tratamento só podem ser responsabilizados , no caso de: (i) não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou (iii) o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III- as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (BRASIL, 2018).

Portanto, vale notar que o legislador, na verdade, optou por não aclarar o regimento de responsabilidade extensível. Embora as críticas nesse ponto de vista, a doutrina enaltece a técnica legislativa por não definir exaustivamente o que poderia ser considerado a avaliação pode levar em conta as singularidades de cada caso particular de acordo com a imparidade da Lei Geral de Proteção de Dados (LGPD).

Responsabilidade Cível Objetiva no CDC E LGPD

A doutrina ao refletir a principal influência que moldou a Lei Geral Proteção de Dados (LGPD), confirma que ela foi inspirada em primeiro lugar a referência europeu de proteção de dados, impactando a legislação brasileira, em particular no Código de Defesa do Consumidor (CDC).Nesse caso, a semelhança entre os dois diplomas reside em mais um fundamento aventado pela doutrina para defender a opção de um sistema de responsabilização objetiva (MALDONADO; BLUM, 2020).

Antes de entrar na discussão, é primordial expor a conceituação de consumidor expresso no art. 2° do Código de Defesa do Consumidor:

> Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo (BRASIL, 1990).

Além de definir o conceito de consumidor, também é importante elucidar que o Código de Defesa do Consumidor é uma das regras que administram as relações de consumo, que impõe responsabilidade objetiva, de forma culpada ou não dos fornecedores em favor dos consumidores (GONÇALVES, 2020).

Primeiro, parece que a lógica da ação de tratamento dos dados são baseados em ideias de vulnerabilidade do indivíduo lesionado, incluíndo não só os dados e terceiros afetados pela violação de dados, que é semelhante a vulnerabilidade aos consumidores (BIONI, 2020).

Portanto, o consumidor com base na doutrina ocupará uma posição vulnerável em frente aos controladores, e os operadores, muitas vezes manifestados na ordem técnica e econômica, e são essa vulnerabilidade que acaba sendo por procederas responsabilidades da LGPD com os dispostos do CDC.

Além disso, a semelhança estrutural entre LGPD e CDC demonstradas pelos Legisladores, em particular ao comparar as exclusões da responsabilidades da LGPD e do

CDC ,ou seja, artigos 43 da LGPD e 12, §3, e 14, §3º, do CDC, o que sugere que a exclusão da responsabilidade civil da LGPD segue o modelo do CDC. O mesmo acontece quando se compara o art.44 da LGPD e artigo 14 §1 do CDC,quando houver semelhanças relevantes entre tratamento ilícito de dados pessoais e falhas de serviço no mercado consumidor (BRASIL, 2018).

No caso de relações de consumo, a Lei 8.078/90 estipula em caso de evento que cause dano ao consumidor a responsabilidade dos implicados por danos causados por defeito ou vicio no fornecimento do produto conforme artigos 12 e 14 (COTS; OLIVEIRA, 2019, p. 79).

Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.

Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos (BRASIL,1990).

A legislação do CDC pode ser invocada se o dano ao consumidor for causado por: manipulação de dados inadequados, disposto no artigo 45 da LGPD diz:“a hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente” (BRASIL, 2018).

Os titulares dos dados podem invocar o sistema de responsabilização do CDC Dados pessoais quando seus direitos são violados quando você compra um produto ou serviço do receptor final, quando há configuração de relação de consumo (MALDONADO; BLUM, 2020, p. 371).

O encarreagado pelo tratamento e o operador de dados são solidariamente responsáveis, e os fornecedores que intervêm ou obtêm algum benefício do processamento de dados ao titular (MIRAGEM, 2019).

Além disso, a responsabilidade do agente de tratamento pode ser realizada de forma objetiva, quer dizer, que responda com ou sem falhas, mesmo ao reparar danos, é possível inverter o ônus da prova, pressuposto expresso no artigo 43, § 2 da LGPD, mesmo que não

seja uma relação de consumo e a legislação Consumistas (MALDONADO; BLOOM, 2020, p. 371).

Responsabilidade Civil Objetiva Proativa em segurança na RGPD

Ante a referida inércia legislativa ao regime geral estabelecido na legislação de dados, aflorando uma nova espécie de Responsabilidade. A Responsabilidade Civil pela LGPD, consoante os artigos 42 a 45, os quais são apresentados como um sistema muito especial com princípios como a principal inovação legal responsabilização, mencionado no art. 6, inciso X, que aduz o caso de o agente de tratamento provar que foram tomadas medidas eficazes, ademais executar as regras de proteção de dados, porque os legisladores pretendem, juntamente com a indenização fosse resguardada a ocorrência do dano (MORAES;QUEIROZ, 2019, p. 126).

Segundo os autores citados, a legislação de proteção do Brasil, Ao implementar os princípios acima, apoia os regulamentos europeus, levando a uma mudança de paradigma relacionado à prestação de contas, tal como no modelo europeu, entra em jogo o dever de prestação fundamental.

Essa nova responsabilidade é conceituada como a "responsabilidade proativa", para tal mudança de paradigma, exige empresas que utilizam dados em atividades econômicas, com atitude consciente e usar e proteger proativamente esses dados (BIONI, 2020).

Neste caso, será necessário evidência de que “medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, não descumprir a lei, não é mais suficiente” (MORAES; QUEIROZ, 2019, p. 129).

Siga esta linha sobre o regime de responsabilidade especial responsabilidade pela proteção, evidencia-se o posicionamento de Rafael Dresch e Lílian Stein (2020), que, no caso de tratamento de dados pessoais, se esta atividade causar prejuízo ao titular dos dados, então a responsabilidade do agente de tratamento é gerada.

No entanto, nestes termos, a responsabilidade civil não tem sistema de responsabilidade civil subjetiva baseado na culpa, nem do regime de responsabilidade civil objetivo e centrado no risco, visto que é uma forma especial de responsabilidade civil objetiva baseada em garantias de segurança no processamento de Dados pessoais (DRESCH; STEIN, 2020.).

Assim, criou-se um modelo mais maduro de responsabilidade civil que ‘‘possibilita garantir a efetividade do recurso de compensação, adaptando-o às especificidades da atividade de processamento de dados pessoais (MORAES; QUEIROZ, 2019, pp. 133-134).

Portanto, pode-se inferir que as características pertecentes ao sistema a responsabilidade civil especial envolvida se manifesta principalmente em regulamentos detalhados sobre o dever de conduta para agentes de tratamento, com enfoque na gestão de riscos, especialmente com o uso de inovações tecnológicas adaptadas às circunstâncias específicas das atividades de processamento de dados pessoais e as reivindicações de proteção que fazem.

CONSIDERAÇÕES FINAIS

Perante a totalidade de dados pessoais presentes no mundo virtual, e nas consequências dos novos impactos na sociedade, faz-se necessário o desenvolvimento de legislação específica sobre este tema. Nesse contexto, no Brasil foi decretado a Lei Geral de Proteção de Dados nº 13.709/2018.

Desta maneira, apareceram novos desafios, em especial para quem utiliza dados pessoais, como as empresas privadas. Deste ponto de vista, surge a relevância deste estudo, com o objetivo de encontrar soluções eficazes de adaptação à nova legislação tanto para as pessoas singulares como jurídicas de direito privado.

No que toca a instauração do Programa de Integridade, além da obdiência aos princípios que resguardam direitos fundamentais, é essencial ter boa administração corporativa, fazendo a correta gestão dos riscos, conter boa estrutura de tecnologia de segurança da informação e preparar adequadamente as equipes de funcionários.

Muitos desafios aparecem para as empresas privadas que utilizam dados pessoais com entrada em vigor da Lei Geral de Proteção de Dados, ocasião que os primeiros movimentos de proteção já se apresentam nítidas.

Baseado nestas circunstâncias, a conclusão é que essa nova cultura é claramente imposta pela Lei Geral de Proteção de Dados (LGPD), que se propõe a proteger efetivamente a privacidade dos titulares de dados pessoais sob o ângulo material e tem um enorme repercussão nas atividades empresariais, exigindo que a operação no processamento ajuste com clareza dos dados, a compreensão e aceitação das pessoas relevantes, com a finalidade de impedir danos e prejuízos aos usuários e à sociedade como um todo e empresas que demandam os dados pessoais.

REFERÊNCIAS

ANDRADE, Diego de Calasans Melo; MOURA, Plínio Rebouças de. O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço. Revista de Direito, Governança e Novas Tecnologias, Goiânia, v.5, n.1, p.110-133, Jan/Jun de 2019.

BRASIL.Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado, 1988.

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: > http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm< acesso em: 27 marc.2022.

BRASIL. Lei nº 9.296, de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, 24 de julho de 1996. Disponivel em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm> acesso em: 20 marc. 2022.

BRASIL. Lei n. 10.406, 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406compilada.htm>. Acesso em: 20 fev.2022.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011.Lei de Acesso à Informação no Brasil. Brasília, DF, novembro de 2011.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm >. Acesso em: 18 marc. 2022.

BRASIL. Lei 12.965 de 23 de Abril de 2014. Planalto.Disponível em: >http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm <. Acesso em: 14 abr. 2022.

BRASIL. lei nº 12.965, de 23 de abril de 2014. Marco civil da internet. Brasília, 23 de abril de 2014; Disponivel em: <https://www.cgi.br/lei-do-marco-civil-da-internet-no-brasil/ > acesso em: 03 abr.2022.

BRASIL. Medida provisória nº 954, de 17 de abril de 2020. Diário oficial da União: edição extra, Brasília, DF, 17 fev. 2022. Disponível em:>http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm< Acesso em: 12 marc.2022.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BOFF, Salete Oro; et.al. Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação. Lumen Juris: Rio de Janeiro, 2018.

COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Comentada. 3. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

DONEDA , Danilo Cesar Maganhoto. Da privacidade de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São PAulo: Thomson Reuters Brasil, 2020.

DRESCH, Rafael de Freitas Valle. A especial responsabilidade civil na Lei Geral de Proteção de Dados. Migalhas, Ribeirão Preto, 02 jul. 2020. Disponível aqui. Acesso em: 20 marc. 2022.

FORTES, Vinícius Borges. Os direitos de privacidade e a proteção de dados pessoais na internet. Rio de Janeiro: Lumen Juris, 201

FIGUEIREDO, Anna Paula Cavalcante. Vazamento de dados de 220 milhões de pessoas: o que sabemos e quão grave. 2021. Disponivel em: <https://www.ibijus.com/blog/856-vazamento-de-dados-de-223-milhoes-de-brasileiros> acesso em: 20 fev. 2022.

FRAZÃO, Ana. Nova LGPD: principais repercussões para a atividade empresarial, 2018. Disponível em Acesso em: 20 marc. 2022.

GONÇALVES, Carlos Roberto. Responsabilidade civil. 19 Ed. Saraiva Educação SA, 2020.

KRIEGER, Maria Victoria Antunes. A análise do instituto do consentimento frente à lei geral de proteção de dados do brasil (lei nº 13.709/18). Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, 2019. Data da publicação: 05 dez. 2019. Disponível em: >https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y<. Acesso em: 01 de maio 2021.

PURKYT, Paulo. Do que trata Lei de Proteção de Dados Pessoais? 2018. Disponível em: <http://www.purkytveneziani.com.br/do-que-trata-lei-de-protecao-de-dados-pessoais/>. Acesso em: 09 de maio 2021.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). LGPD: Lei Geral de Proteção de Dados comentada. 2. ed. rev. atual. e ampl. São Paulo:Thomson Reuters Brasil, 2020.

MARINELI, Marcelo Romão. Privacidade e redes sociais virtuais. Rio de Janeiro: Lumen Juris, 2017.

MALHEIRO, Luíza Fernandes. O consentimento na proteção de dados pessoais na Internet: uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016. Trabalho de Conclusão de Curso (graduação) – Universidade de Brasília, Faculdade de Direito, 2017.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. IN: Cadernos Adenauer, volume 3, Ano XX, 2019.

MIRAGEM, Bruno. A lei geral de proteção de dados (lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais, v. 1009, 2019. Disponível em: <https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>. Acesso em: 19 marc. 2022.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho. 1995.