PROTEÇÃO DOS DADOS PESSOAIS COMO DIREITO FUNDAMENTAL: A EVOLUÇÃO DA TECNOLOGIA DA INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

Protection of personal data as a fundamental right: the evolution of information technology and the General Data Protection Law in Brazil

Revista de Direito Constitucional e Internacional | vol. 121/2020 | p. 115 - 139 | Set - Out / 2020
DTR\2020\11423

Gianfranco Faggin Mastro Andréa
Doutorando e Mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Bolsista pelo Mackpesquisa. Especialista em Direito Público pela Faculdade de Direito Damásio de Jesus. Graduado em Direito pela Universidade Presbiteriana Mackenzie. Professor Universitário. Analista do Ministério Público da União
professorgianfaggin@gmail.com

Higor Roberto Leite Arquite
Pós-graduando com título de especialista em Direito e Tecnologia da Informação pela Universidade de São Paulo – USP. Graduado em Direito pela Universidade Paulista. Advogado. higorarquite11@gmail.com

Juliana Moreira Camargo
Mestre em Direito da Sociedade da Informação pela FMU. Pós-graduada com título de especialista em Direito Penal e Processo Penal pela Universidade Presbiteriana Mackenzie. Graduada em Direito pela FMU. Professora Universitária do curso de graduação em Direito da UNIP e do curso de pós-graduação em Direito Penal da Universidade Presbiteriana Mackenzie. Advogada Criminalista. Membro efetivo da comissão especial de Direito Digital da OAB/SP. Palestrante.
julianamoreiracamargo@gmail.com

Área do Direito: Constitucional; Digital

Resumo: Com previsão constitucional e em diversas leis esparsas, é de se destacar que o direito à privacidade é debatido em níveis mundiais, em razão de ser um dos mais preciosos direitos resguardados ao ser humano. Com o avanço da tecnologia, houve longas discussões para que se estendesse a tutela jurídica também aos campos digitais, pois os dados pessoais são importantes tanto no universo físico quanto no on-line. O presente trabalho, valendo-se da metodologia de revisão bibliográfica, tem como objetivo demonstrar o panorama geral e a necessidade que se tinha de preencher a lacuna existente quanto a regramento especial acerca da proteção das informações do indivíduo, o que se deu com a Lei Geral de Proteção de Dados no Brasil. Conclui-se que a aprovação de aludida Lei demonstrou um avanço do tratamento do tema no Brasil, coadunando-se com as normas estrangeiras atinentes à espécie.

Palavras-chave: Internet – Proteção dos dados pessoais – Lei Geral de Proteção de Dados

Abstract: With constitutional provision and in various sparse laws, it should be noted that the right to privacy is debated at global levels, due to being one of the most precious rights protected from the human being. With the advancement of technology, there were long discussions to extend legal protection also to digital fields, because personal data are important both in the physical and online universe. The present work, using the methodology of bibliographic review, aims to demonstrate the general panorama and the need to fill the existing gap in terms of the special rule regarding the protection of the individual's information, which the General Data Protection Law in Brazil. It is concluded that the approval of the alluded Law demonstrated an advance in the treatment of the theme in Brazil, consistent with foreign laws related to the species.

Keywords: Internet – Protection of Personal Data – LGPD – GDPR – National Authority for Personal Data Protection and Privacy
Sumário:

1.Introdução

Vive-se em uma era em que a população depende dos meios de comunicação. O poder da informação é absoluto e instantâneo. Em pouco tempo consegue-se ter acesso a notícias de qualquer lugar do mundo, conversar com pessoas do outro lado do continente, assistir filmes, ter acesso a livros e demais documentos sem sair de casa, apenas utilizando o computador ou o celular.

Ainda, de forma automática, os dispositivos tecnológicos fornecem informações adaptadas, apenas baseados nos interesses e na forma como o usuário utiliza determinado aparelho. É o que se chama de algoritmos, no qual esses dispositivos fazem uma leitura automatizada da forma como se manuseia o aparelho e proporciona mecanismos para trazer uma melhor comodidade e um ótimo proveito no mundo digital. Seja recomendando músicas, por meio do Spotify, seja sugerindo séries pelo Netflix ou até mesmo mostrando notícias relevantes sobre time de futebol. Tudo isso involuntariamente.

Para que esse tipo de tecnologia seja aplicado, é necessário que os sistemas façam uma análise dos dados pessoais (compartilhados ou não), incluindo os sensíveis, e utilizem desses para sugerir coisas que mais agradam aos usuários, baseados nos dados também de outras pessoas. O incrível é que as sugestões costumam ser certeiras.

No entanto, sem alguma lei que regule esse tipo de tratamento dos dados, poderá acarretar uma invasão da privacidade alheia, gerando riscos a direitos fundamentais presentes na nossa Constituição Federal. Compra-se um computador ou um tablet com o objetivo de usá-los com conforto, para trabalho, pesquisa e diversão em geral. Sem uma tutela protetiva, o próprio dispositivo poderá utilizar informações não compartilhadas para outros objetivos, e ao final, os produtos/objetos serão os dados pessoais. Não é incomum que ocorram vazamentos de dados bancários, informações pessoais e senhas justamente por algum tipo de falha nos aplicativos ou no próprio sistema, gerando prejuízos de grande monta.

O presente trabalho tem como proposta compreender a necessidade de os direitos fundamentais também serem protegidos no campo da tecnologia, em especial na proteção dos dados pessoais por meio da Lei Geral de Proteção de Dados Pessoais, haja vista que essas informações são um dos mais importantes direitos inerentes à vida humana, pois trata da privacidade do indivíduo e que, se não tutelados, poderão acarretar inúmeros danos.

Para tanto, são trazidos também as normas anteriores e os demais dispositivos normativos, os entendimentos doutrinários e provindos de diversos estudos para melhor compreensão do tema, pois foram os elementos fundamentais do iter percorrido pela LGPD até seu efetivo surgimento.

2.Conceitos basilares: internet, dados, big data, algoritmos e cookies

A fim de se compreender a temática proposta, tem-se que alguns conceitos são pressupostos para o próprio entendimento do avanço da proteção de dados em nosso sistema jurídico. Assim, é preciso entender algumas definições básicas, entre elas a da Internet.

Porém, no que tange à própria legislação atual que regula os dados pessoais, não se encontra qualquer significado sobre o tema. É necessário, então, recorrer a Lei 12.965/2014 (LGL\2014\3339) (Marco Civil na Internet), que em seu artigo 5º, I, define internet como sendo: "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes".[1]

A Internet se resume, portanto, em uma rede no qual inúmeros dispositivos de comunicação são conectados com o objetivo de realizar compartilhamento de dados de forma constante manualmente ou de forma autônoma entre si, por exemplo, a internet das coisas. A internet das coisas nada mais é do que a interconexão entre diversos objetos presentes no nosso cotidiano de forma constante e autônoma, sendo controlada pelo detentor das coisas.

Já os dados, dentro da internet, constituem-se em conjunto de informações que são compartilhadas entre os dispositivos integrantes da rede, representadas através de códigos binários (0 e 1), que são "descriptografados" e "lidos" pelo dispositivo receptor. Os computadores, por processarem qualquer arquivo de forma binária, recebem e armazenam os dados da mesma forma e, que, após o processamento dos dados, transformam no elemento compartilhado. Este, pode ser um documento, uma imagem, um texto, um filme ou praticamente qualquer outra coisa. O conjunto dos referidos dados forma o que é chamado de big data.

Dentro do mundo do Direito, e, em especial no tocante ao observado pela Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018 (LGL\2018\7222)), os dados são classificados em dados pessoais e dados pessoais sensíveis.

O dado pessoal, na forma como preceitua o art. 5º, I, da referida lei, é "informação relacionada a pessoa natural identificada ou identificável". Ou seja, trata-se então de informações comuns correspondentes àquela pessoa, por exemplo, naturalidade, estado civil, idade, documento de identificação pessoal, endereço residencial, entre outros.

Já os dados pessoais sensíveis são aqueles que abrangem a vida pessoal do indivíduo, informações que encampam não apenas requisitos comuns presentes em todas as pessoas, mas aqueles particulares, que, se utilizados, proporcionam uma rápida identificação do indivíduo. Também preceituados pela lei, em seu art. 5º, II, correspondem aos dados subjetivos da pessoa, que envolvem até mesmo convicções políticas e religiosas. Confira-se:

"O 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 (Redação dada pela Lei 13.709/2018 (LGL\2018\7222))."

algoritmos, por usa vez, são basicamente conjuntos de informações efetuadas para que uma máquina execute determinado procedimento. Trata-se de um mero "guia" contendo elementos que, seguidos em uma ordem lógica pelo computador, correspondem a uma ação. Utilizados no campo da programação por empresas e demais instituições, quando possuem um número suficiente de informações sobre um usuário, poderão traçar o perfil e sugerir opções de seu gosto de forma automática, apenas baseando-se em experiências anteriores.[2]

Já cookies correspondem a alguns arquivos encaminhados pelo usuário ao servidor contendo informações a respeito da pessoa. São, de certa forma, considerados dados, mas que servem apenas como "lembretes" de que o usuário já acessou aquele site, como a memorização de usuário e senha. Como bem preceituado por Thiago Pinheiro Vieira de Souza,

"os cookies, por sua vez, compõem a principal tecnologia de rastreamento e monitoramento de usuários na Internet. Permitem a análise de navegação do usuário por um período certo de tempo, funcionando da seguinte forma: em regra, a empresa coloca um cookie de rastreamento (tracking cookie) em um instrumento denominado DTE (data terminal equipment), que ordinariamente converte informações do usuário em sinais quando se acessa algum website que contém tais tecnologias. Essencialmente, os cookies são arquivos de texto simples, armazenados pelo navegador frequentado, contendo informações básicas acerca das preferências dos usuários".[3]

Têm relação direta com os algoritmos e a inteligência artificial, pois são dessas informações compartilhadas entre o usuário e o site ou provedor de internet que o próprio servidor (no sentido amplo do termo) se utiliza para proporcionar um melhor proveito daquele site, e, consequentemente, fazer com que o usuário retorne mais vezes.

3.Arcabouço jurídico antecedente à Lei Geral de Proteção de Dados

Para compreender o estudo da sociedade da informação e o tratamento dos dados pessoais regulamentados pela LGPD, é necessário, antes de tudo, entender como surgiu o poder de comunicação e aproximação entre pessoas de localidades diferentes, de forma instantânea, através de um simples clique.

3.1.Do surgimento da Rede Mundial de Computadores e o General Data Protection Regulation – GDPR

A força comunicacional e horizontal surgiu durante a Guerra Fria (1945 – 1991), período em que as duas maiores superpotências econômicas e militares da época (Estados Unidos da América e União Soviética) conflitavam de forma indireta, com o principal objetivo de transparecer seu poder bélico e tecnológico e, de certa forma, "amedrontar" o seu oponente.[4]

Os computadores já existiam naquela época, mas eram apenas utilizados pelas forças militares com o principal objetivo de captar as ondas de rádio inimigas e coordenar estratégias de ataque e defesa. Eram totalmente diferentes dos modelos atuais, tanto pelo seu tamanho e forma como pela capacidade de processamento de informações, que era infinitamente menor.

A União Soviética, em 1957, lança o seu primeiro satélite artificial, chamado Sputnik, com o objetivo principal de mostrar o seu desenvolvimento tecnológico espacial, algo inovador até o momento. Os norte-americanos, por sua vez, após investimento de grande monta pelo governo, criaram o projeto chamado ARPA ou ARPANET (Advanced Research Projects Agency Network), um sistema de comunicação confiável e eficiente, com o principal objetivo de permitir um trabalho cooperativo entre grupos diferentes, em localidades diferentes, de forma instantânea e constante, sem sofrer interferências externas que afetassem a sua comunicabilidade.[5]

Porém, o que era para ser um simples projeto, acabou ganhando forte relevância, fazendo com que, posteriormente, ultrapassasse os limites acadêmicos ou paramilitares para atingir a população geral e dando início à criação de outras redes análogas, como a Bitnet e a TelNet. Conforme descrito por Túlio Moura:

"[...] na época, apesar da popularidade nos meios científico e universitário, a internet ainda não havia chamado a atenção do grande público. As ferramentas ainda eram rudimentares e o tipo de informação disponível era relevante somente para o campo de pesquisas científicas. Foi quando apareceram ferramentas como o correio eletrônico, o FTP e o TelNet. Ferramentas que permitiam a comunicação e o acesso a bancos de dados. Foram verdadeiros marcos na história da internet".[6]

Esse avanço da tecnologia suscitou uma – de certa forma, tardia – série de debates sobre a privacidade do usuário na rede. Vemos que as primeiras normas de relevância

sobre a proteção de dados surgiram após mais de três décadas de existência da rede mundial de computadores e seu uso por pessoas comuns, sem existir necessariamente um vínculo com o poder público.

A respeito do debate sobre a privacidade no universo digital, surgiu a Convenção 108, de 1980. Essa, teve como objetivo principal garantir a proteção de dados como um direito fundamental a todos, trazendo, então, uma interpretação extensiva sobre cada constituição, abrangendo esse direito à privacidade. Foi uma das pioneiras sobre o tema, tanto que a GDPR utilizou grande parte de seu texto como referência.

Com efeito, a principal legislação (e a utilizada como referência no Brasil) que trata sobre o tema é a GDPR (General Data Protection Regulation), da União Europeia, que entrou em vigor em 25 de maio de 2018, composta por 90 artigos, distribuídos em 9 capítulos.

Trata-se de um regulamento geral no qual todas as empresas que exerçam algum tipo de atividade (remunerada ou não) em algum país da Europa devem possuir um tratamento especial no tocante aos dados dos seus usuários. Essa lei praticamente abrange o mundo inteiro, e, de fato, atinge uma parcela considerável das empresas internacionais, haja vista que a maioria delas presta algum tipo de serviço ou comercializa algum produto em, ao menos, algum lugar da Europa.

Já em suas primeiras considerações, o Parlamento Europeu e o Conselho da União Europeia, através da GDPR, definiram que a proteção dos dados pessoais seria um direito fundamental que está presente não apenas nessa legislação, mas na Carta dos Direitos Fundamentas da União Europeia (art. 8, n. 1) e no Tratado sobre o Funcionamento da União Europeia (art. 16, n. 1).[7]

Já em seu art. 4º, a lei elenca diversas definições que foram adaptadas para a nossa legislação, por exemplo, o conceito dos dados pessoais. Enquanto na GDPR não há exatamente uma distinção entre os dados pessoais e os dados pessoais sensíveis, na nossa legislação, em seu art. 5º, sua distinção é bem apresentada, em seus incisos I e II. Porém, em seu art. 9º, o legislador proibiu expressamente o uso dos dados pessoais de origem racial, ética, convicções políticas, religiosas entre outros, mas com ressalvas.[8]

A GDPR trouxe uma grande influência para o nosso legislador pátrio em muitos dos artigos, como nas hipóteses nas quais os dados pessoais sensíveis poderão ser tratados pelo controlador de forma taxativa, ou seja, apenas dentro daquelas hipóteses descritas em lei é que poderão ser utilizadas. A principal e mais simples delas é mediante a autorização de forma específica e destacada do titular ou responsável legal pelos dados. Outras, também relevantes, poderão ocorrer mesmo sem o consentimento do seu titular, mediante cumprimento de obrigação legal, proteção à vida do titular ou terceiro, exercício regular de direitos, entre outros.

O Chile foi o primeiro país da América do Sul a tratar sobre o tema, em 1999, através da Ley 19.628 (Proyeto de Ley Proteccion de datos de caracter personal),[9] seguido pela Argentina, em 2000, pela Lei de Proteção de Dados Pessoais 25.326[10] (PDPL, na sigla em inglês), com o Decreto regulamentar 1558/2001[11] e outras disposições da Diretoria Nacional de Proteção de Dados Pessoais.

Em 2008 foi a vez do Uruguai criar sua própria legislação sobre o tema pela Ley de Protección de Datos Personales y Acción de "Habeas Data" 18.331,[12] que por muitos é considerada tão complexa e equivalente à da União Europeia, facilitando diretamente os tratados internacionais ou acordos realizados entre os países em relação aos bancos de dados. O Peru apresentou sua legislação sobre o tema apenas em 2011, pela Ley de Protección de Datos Personales 29.733.[13]

O Equador possui referências através da sua Constituição, que são retratadas seguindo a mesma linha das normas anteriores. Já a Bolívia, além de deter previsões constitucionais

a respeito do tema, também é empoderada de normas esparsas, como a Ley 28168, de 2005 (Acceso a la Información del Poder Ejecutivo), Ley 018, de 2010, del Órgano Electoral Plurinacional, a Ley 164 de 2011, General de Telecomunicaciones, Tecnologías de la Información y Comunicación e o Decreto Supremo 1793, de 13 de novembro de 2013, Reglamento de la Ley 164.

Na mesma linha, segue a Venezuela, dotada de previsões constitucionais e leis esparsas, sendo a Ley de registro de antecedentes penales de 1979, Ley sobre Protección a la Privacidad de las Comunicaciones de 1991, Ley Orgánica para la Protección del Niño y del Adolescente de 1998 e Ley Especial contra Delitos Informáticos de 2001[14]. Já a Guiana Francesa e a República Dominicana, apresentam, ao menos, previsões constitucionais. Dos principais países da América do Sul, o Paraguai é o único país dotado de uma legislação genérica, que retrata de forma ampla os tratamentos dos dados pessoais, pela Ley 1682, que regulamenta a informação de caráter privado.

Como precedentes da GDPR, não existiram tantas referências. Como base, existiu a Convenção 108, de 1980 e algumas normas esparsas[15]. Inclusive, não é ousado dizer que os próprios Estados (e isso, em escala mundial) possuem uma certa responsabilidade pelos constantes golpes e exposições de pessoas na internet, pois, por ausência de legislação específica ou de um tipo penal, inexiste crime. Porém, é de reconhecer que o Direito nunca irá conseguir acompanhar o avanço da tecnologia na vida das pessoas.

Ainda, também por ausência de fiscalização ou de uma Autoridade Nacional de Proteção de Dados, não é incomum que uma parcela considerável dos autores desses golpes permaneçam impunes, muitos deles sequer passíveis de localização, pois deslocam seu IP (Endereço de Protocolo Eletrônico, ou seja, a forma de identificação do seu dispositivo no meio virtual) para países diferentes.

Porém, apesar da falha de tutela jurisdicional sobre o tema, é de se entender a importância que essas leis mencionadas (em especial a GDPR) trouxeram para esse novo universo, servindo até mesmo como esboço para outras normas sobre outros temas e de diversos países.

Sua abrangência, ambição legislativa e maturidade conceitual corroboram a ideia de que esse é um autêntico regulamento-modelo, no qual diversas outras iniciativas nacionais, regionais e intracomunitárias também serão espelhadas em busca de padrões normativos uniformes na proteção de dados pessoais. Não seria exagero afirmar que o GDPR nasce como "monstro normativo", um Leviatã a induzir condutas de conformidade (compliance) por parte de agentes nas esferas pública e privada no campo da proteção de dados pessoais e especialmente identificáveis nos ambientes informacional e digital[16].

3.2.Proteção dos dados pessoais no Brasil

É necessário, então, o estudo da proteção dos dados pessoais na nossa legislação, que surgiu derivada de outras e que inclusive possuem diversos princípios em comum.

3.2.1.Código de Defesa do Consumidor

Diante de uma série de normas que regulam o tratamento dos dados pessoais pela América do Sul, o Brasil, de forma tardia, resolveu criar uma legislação que trata especificadamente sobre o tema. Dentro do nosso ordenamento jurídico, os dados pessoais já eram regulados de forma genérica por legislações específicas.

"O Código de Defesa do Consumidor disciplinou, em seu art. 43, os bancos de dados e cadastros de consumidores. Note-se a amplitude do dispositivo em questão, que alcança todo e qualquer dado pessoal do consumidor, indo muito além, portanto, dos bancos de dados de informações negativas para fins de concessão de crédito. A racional do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor."[17]

Os Tribunais superiores já vêm interpretando o art. 43 de forma favorável ao consumidor valendo-se de princípios semelhantes aos adotados pela LGPD, por exemplo, o da inversão do ônus da prova, norma mais favorável ao usuário, bem como uma espécie de in dubio pro usor, que serão expostos posteriormente.

Tal semelhança, após a entrada em vigor dessa nova lei, fará com que as normas de relações de consumo e a LGPD caminhem próximas uma à outra, pois implicitamente possuem preceitos em comum instrumentalizados.

Não é diferente o entendimento de Solano de Camargo: "Na LGPD, o juiz deve levar igualmente em conta o princípio da vulnerabilidade, hipossuficiência da parte para interpretar um conflito"[18].

A necessidade da proteção dos dados pelo nosso ordenamento surge de acordo com o avanço das relações cíveis e consumeristas, no qual o cadastro dos credores e devedores nos contratos celebrados, nas operações de crédito e até mesmo pelo próprio Estado, passaram a depender de uma segurança jurídica que ultrapassa o mero armazenamento ou simples cuidado destes.

A defesa do consumidor e a proteção de dados pessoais visam proteger o cidadão de um desequilíbrio de poderes que possa afetar a tomada de uma decisão livre, autônoma e informada. Enquanto a defesa do consumidor busca reequilibrar a relação entre consumidor e fornecedor no mercado de bens e consumo, a proteção de dados diz respeito ao reequilíbrio entre controlador dos dados pessoais e o titular, que muitas vezes desconhece como se dá o tratamento de dados, suas finalidades ou os seus possíveis riscos.[19]

3.2.2.Lei 12.414/11 (Lei do Cadastro Positivo)

Posteriormente, foi criada e sancionada pela então presidente da república Dilma Rousseff a Lei 12.414/2011 (LGL\2011\1883), denominada Lei do Cadastro Positivo, com relevantes considerações sobre o tratamento dos bancos de dados e a possibilidade de aplicação do Código de Proteção e Defesa do Consumidor ao banco de dados, fonte e consulente (art. 16 e 17 da Lei).

Composta por 18 artigos, tem como objetivo a formação de um banco de dados que facilite a obtenção de crédito à pessoa natural ou jurídica, através da análise de suas informações socioeconômicas.[20]

Um fator interessante nas normas já elencadas é o necessário consentimento do indivíduo nas hipóteses de cessão dos seus dados para terceiros, atribuindo às empresas em geral, de concessão de crédito ou não, a responsabilidade civil no caso de vazamento desses dados.

"Esse arranjo é complementado, ainda, pelo dever de o gestor da base de dados não coletar informações excessivas e sensíveis para fins de análise de crédito, bem como de não as utilizar para outra finalidade que não a creditícia. Com tais limitações, tal quadro normativo limita a coleta e as finalidades de tratamento dos dados pessoais com o intuito de capacitar o consumidor com o controle de suas informações pessoais. Mais uma vez, portanto, a técnica legislativa deita-se sobre o referencial normativo da autodeterminação informacional."[21]

3.2.3.Lei 12.737/2012 (Lei Carolina Dieckmann)

Um dos mais emblemáticos casos envolvendo o furto de dados pessoais foi o sofrido pela atriz Carolina Dieckmann, que, através do seu computador pessoal, teve fotos e conversas íntimas hackeadas e divulgadas na internet. Tamanha foi a repercussão que foi um dos projetos de lei mais rápidos já tramitados pelo Congresso Nacional, sancionada pela então presidente Dilma Rousseff em 30 de novembro de 2012 e acrescentando os arts. 154-A e 154-B, 266 e 298 ao Código Penal.[22]

O fato envolvendo a atriz levantou questões importantes tanto aos juristas quanto para a sociedade, pois se tratou de um acontecimento até então escasso de tutela jurisdicional, e o texto dos artigos apresentados, por falta de cautela, podem não ser condizentes com a realidade ou o futuro, abrindo espaço para mais de uma forma de interpretação sobre o mesmo tema.

É o entendimento de Pedro Berreta sobre um dos artigos acrescidos pela lei, em que:

"[...] o tipo penal do artigo 154-A não fornece a definição exata de "mecanismo de segurança", questão fulcral para cometimento ou não do crime, assim, se o dispositivo invadido não possuir qualquer tipo de proteção (senha, antivírus, firewall etc.), a conduta será atípica, uma vez inexistente a modalidade culposa."[23]

Logo, a tentativa de estabelecer a criminalização da invasão de dispositivos sem autorização torna-se falha, pois também existe a hipótese em que a própria pessoa lesada entrega, por conta própria, sua máquina. Permanece, até aquele momento, a ausência de tutela jurisdicional no que tange ao uso dos dados pessoais por terceiro sem autorização, ou autorização genérica, sem um fim específico. Por exemplo, a autorização para acessar um documento na nuvem mediante a entrega do login e senha pela parte lesada obsta a aplicação da legislação se algum documento indevido for acessado de forma culposa.

3.2.4.Lei 12.965/2014 (Marco Civil da Internet)

O Marco Civil da Internet, sancionado pela então presidente Dilma Rousseff, foi o principal documento legislativo que trata sobre o direito digital e "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil".[24]

Antigamente, o que existiam eram preceitos que traziam direitos e deveres, só que de forma leiga, que não acompanhava a complexidade da rede mundial de computadores. As poucas doutrinas que tratavam sobre o tema também não eram documentos suficientes para retratar de forma absoluta qual a relação entre o Direito e a Tecnologia, bem como os limites do exercício da tutela jurisdicional. A jurisprudência, por sua vez, pouco diversificou, em razão da ausência de material e fundamentação disponível, haja vista a escassez de leis.

Porém, como toda e qualquer área nova do Direito, são através desses "esboços legislativos" que desempenham pesquisas acadêmicas, doutrinárias e legislativas, para então evoluir.

Foi o que aconteceu com as normas anteriores, que, em sua maioria, tinham como objetivo acrescentarem aspectos ao âmbito criminal, sendo contrário ao tamanho que é o mundo eletrônico.[25] O Marco Civil da Internet foi uma verdadeira ruptura que alavancou os estudos jurídicos sobre o tema, pois foi um preceito fundamental para entender a liberdade de expressão dentro desse novo campo jurídico, além de assegurar de forma cautelosa os direitos e garantias fundamentais.

Composta por 32 artigos divididos em 5 capítulos, a Lei tem como base a liberdade de expressão nos meios digitais, mas com princípios que visam garantir o direito à privacidade e a proteção dos dados pessoais.[26]

Observa-se então que o tratamento dos dados pessoais já caminha a passos largos, de forma até bem estruturada, garantindo a partir daqui uma tutela do Estado relevante e já demonstrada uma cultura jurídica sobre o tema pelo legislador, principalmente no cenário pós-Snowden[27], relacionado ao acesso indevido de dados particulares pelo governo norte-americano.[28] Além disso, também traz alguns aspectos técnicos que não foram completamente reproduzidos na prática, tanto pelo Estado como pelas empresas prestadoras de serviços de telecomunicações, como o presente no art. 3º, V, que visa preservar a estabilidade, a segurança e a funcionalidade da rede, e o art. 4º, ao tratar sobre o direito de acesso à internet a todos.

4.Lei Geral de Proteção de Dados: uma breve análise do marco em proteção de dados como direito fundamental

Diversos Projetos de Lei antecederam o Projeto de Lei 53/2018 que se tornou a Lei Geral de Proteção de Dados no Brasil. Todos os projetos anteriores, apesar das boas intenções, apresentaram-se incompletos e não tratavam do tema como se deveria.[29] Assim, o Projeto de Lei da Câmara 53/2018 foi o último dos projetos que trataram da Lei Geral de Proteção de Dados no Brasil. Em razão dos diálogos e da pressão por parte da sociedade, das empresas e dos próprios órgãos públicos, diversas entidades se reuniram para fazer um manifesto requerendo a aprovação do PL.[30]

Até então, se tratava de uma medida de urgência, pois o Brasil continuava escasso de legislação específica sobre o tema.

"[...] A proposta é o resultado possível e maduro de diálogo e negociação intensa entre diversos interessados na consolidação de uma moderna lei geral de proteção de dados pessoais, adequada ao atual contexto tecnológico, compatível com futuros avanços e compromissada com direitos fundamentais. Hoje, o mundo todo repensa a relação entre inovações tecnológicas e riscos coletivos gigantescos. E o Brasil pode dar um passo certo na direção de mais segurança jurídica e de uma economia de dados centrada no respeito a direitos (Coalizão Direitos na Rede, 2018)."[31]

Em julho de 2018, finalmente o projeto de Lei foi aprovado pelo Senado Federal, o qual foi sancionado e publicado em agosto do mesmo ano. Veio à lume, portanto, a Lei 13.709/2018 (LGL\2018\7222), com vigência 24 meses após sua publicação no Diário Oficial da União.[32]

Apesar de ter sido uma vitória a criação da Lei Geral de Proteção de Dados Pessoais, houve alguns vetos pelo ex-presidente Michel Temer[33] e alterações pelo presidente da república Jair Bolsonaro[34]. A LGPD é composta por 65 artigos divididos em 10 capítulos. A Lei:

"dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (art. 1º)".

Sua aplicabilidade recai sobre todas as pessoas físicas ou jurídicas de direito público ou privado que efetuem o tratamento ou a coleta de dados pessoais em território nacional. Nesse aspecto, enquadram-se as também as empresas nacionais ou internacionais que efetuem o tratamento dos dados com o objetivo de fornecer bens ou serviços em indivíduos localizados em território nacional (art. 3º), tanto que o dispositivo normativo não faz qualquer distinção entre pessoas que possuem residência ou domicílio no Brasil ou não.

Uma das exceções é o do tratamento dos dados pessoais para fins particulares e não econômicos (art. 4º, I). De certa forma, trata-se de um preceito que recai sobre os direitos individuais e relativiza o direito à privacidade, pois abre espaço para que exista uma constante invasão às informações alheias entre pessoas naturais para qualquer outro fim, haja vista que o conceito de "fins particulares" é bem amplo, dando espaço para inúmeras interpretações diferentes. A LGPD não deve se pautar apenas em objetivos econômicos ou sociais, mas deve considerar também as relações cíveis entre os indivíduos.

Existem também exceções aos dados tratados com fins exclusivamente jornalísticos, artísticos e acadêmicos em que, como já visto anteriormente, o interesse público é superior ao privado, tanto que o STF já decidiu através da ADI 4.815 sobre o tema. Como últimas exceções, presentes nos incisos III e IV do art. 4º da referida lei, são os que tangem à segurança pública, do Estado e da defesa nacional, inclusive para fins de

repressão de infrações penais. Novamente o interesse público se sobressai sobre o privado, cabendo então uma relativização da vida privada do indivíduo para garantir a segurança da sociedade e dos órgãos públicos.

Também é de se entender a ligação entre a LGPD e o Marco Civil da Internet. Enquanto este possuía breves considerações sobre o tratamento dos dados pessoais, a LGPD tem em todo o seu corpo legislativo essa lacuna que faltava, a profundidade e a cautela sobre o tema. "Estamos falando especificamente sobre tratamento de dados pessoais, seu uso, destino, comercialização etc. – matéria na qual o MCI não conseguiu avançar profundamente. E foi isso que a nova Lei Geral de Proteção de Dados veio regulamentar".[35]

4.1.Fundamentos da LGPD

Os fundamentos presentes na LGPD poderão ser encontrados no art. 2º. Convém trazer a informação de que parte desses fundamentos são encontrados em outras normas, como o Código de Defesa do Consumidor, os projetos de leis anteriores e principalmente na Carta Magna. Pelo fato do direito à informação e tratamento dos dados pessoais serem fundamentais e presentes no art. 5º da CF (LGL\1988\3), é necessário trazer à tona principalmente aqueles de maior importância, justamente por serem partes fundamentais.

O primeiro e principal fundamento presente na LGPD é sobre o respeito à privacidade do indivíduo. Trata-se de um fundamento já cristalizado na forma da Constituição, em seu art. 5º, X, bem como na Declaração Universal dos Direitos Humanos (art. 12). Trata-se do direito da pessoa de excluir do conhecimento de terceiros tudo aquilo que a ela se relaciona.[36]

Outro elemento fundamental é o da autodeterminação informativa, que atribui ao proprietário dos dados pessoais, além da plena ciência sobre o modo com seus dados são utilizados, também a liberdade de requerer sua exclusão, portabilidade, retificação ou acréscimo de informações ao big data.

O direito à autodeterminação informativa possui dois elementos: um de caráter negativo – os princípios que regulam a qualidade de tratamento dos dados – e outro de caráter positivo, ou seja, o direito dos interessados que podem ser assegurados através de instrumentos como o habeas data.[37]

Outros fundamentos importantes são os da liberdade de expressão, informação, comunicação e opinião e a inviolabilidade da intimidade, honra e da imagem. Porém, trata-se de elementos que basicamente repetem previsões constitucionais e que já foram tratados durante esse trabalho.

4.2.Princípios da LGPD

A LGPD é dotada de alguns princípios básicos, elencados no caput do art. 6º e em seus incisos, sendo eles:

4.2.1.Princípios da boa-fé e finalidade

De acordo com Ruy Rosado Aguiar Júnior, a boa-fé é significa que todos devem guardar fidelidade à palavra dada e não frustrar ou abusar da confiança que constitui a base imprescindível das relações humanas, sendo, pois, mister que se proceda tal como se espera que o faça qualquer pessoa que participe honesta e corretamente do tráfego jurídico.[38]

Na Lei Geral de Proteção de Dados, é importante elencar que a cessão dos dados pelo indivíduo a outrem requer transparência e confiança para ambas as partes, sob a pena de nulidade.[39]

Pelo princípio da finalidade, encontrado no primeiro inciso do art. 6º, deve-se entender que o tratamento dos dados pessoais deverá possuir um fim específico, predefinido, e que as partes tenham ciência disso, sob pena de nulidade dos atos e possibilidade de reparação de danos.

4.2.2.Princípios da adequação e necessidade

O segundo inciso do art. 6º define o princípio da adequação como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Ou seja, o tratamento dos dados pessoais será feito de acordo com o fim especificado e convencionado pelas partes. Já o princípio da necessidade pode ser entendido como a utilização dos dados pessoais de maneira limitada, correspondendo apenas ao mínimo necessário para a finalidade específica. Tem como objetivo evitar a coleta de dados pessoais desnecessários, afetando também a privacidade do indivíduo (por exemplo, requerer dados pessoais sensíveis quando não existe necessidade).

4.2.3.Princípios do livre acesso e da qualidade dos dados

Esse princípio foi cristalizado nessa legislação, bem como tratado de forma profunda nos projetos de leis anteriores, pois visa garantir que aquele que cedeu os dados para outrem possa ter acesso a esses dados, podendo a qualquer momento requerer a portabilidade, exclusão, alteração e inclusão de novos dados. Trata-se de um princípio que possui também garantia constitucional e que fora tratado de forma ampla nos tópicos anteriores.

Por sua vez, o princípio da qualidade dos dados é um princípio corolário ao anterior, pois este visa garantir que os dados pessoais sejam transmitidos de forma exata e clara entre o titular e o operador ou responsável pelo tratamento.

4.2.4.Princípios da transparência e da prevenção

O princípio da transparência também é outro princípio já elencado profundamente nos tópicos anteriores, que aduz que os dados pessoais deverão ser tratados de forma clara e transparente entre o operador e o titular que cedeu os dados pessoais. Ele tem como objetivo garantir que o titular dos dados possa ter ciência da forma como seus dados estão sendo utilizados. Há duas flexibilizações no que tange a esse princípio, que é o dos segredos comerciais e industriais.

Por outro lado, o princípio da prevenção tem como objetivo garantir que os operadores e responsáveis pelo tratamento dos dados pessoais adotem medidas e procurem soluções de maneira constante para prevenir algum tipo de dano às informações, como o vazamento de dados pessoais para terceiros.

4.2.5.Princípios da não discriminação, responsabilização e prestação de contas

O princípio da não discriminação encontra-se em conformidade com a Constituição Federal e ao Estado Democrático de Direito, no qual em hipótese alguma deverá existir o tratamento dos dados pessoais com objetivos discriminatórios (religião, raça, opinião política, sexualidade ou qualquer outro tipo). Além disso, aquele que o fizer poderá ser responsável criminalmente pelos atos praticados.

Finalmente, o princípio da responsabilização e prestação de contas tem como objetivo garantir que os dados pessoais sejam tratados de acordo com a finalidade já convencionada entre as partes.

Todos os princípios, além de elencados no art. 6º e seus incisos, possuem expressas previsões nos diversos artigos dos capítulos posteriores, sempre trazendo uma tutela jurisdicional ao indivíduo que cedeu os dados para uso, demonstrando que qualquer ato efetuado pelo operador deverá respeitar os princípios apresentados e que o titular poderá, a qualquer tempo e respeitadas previsões legais, requerer o término do

tratamento desses dados (arts. 15 e 16).

Ainda, há uma tutela especial no que tange aos dados pessoais das crianças e dos adolescentes (art. 14), no qual o consentimento do menor não é levado em consideração se não houver, ao menos, a autorização de um dos pais ou de responsável legal.

4.3.Da Autoridade Nacional de Proteção de Dados Pessoais e Privacidade (ANPD)

Um dos principais projetos relevantes nessa nova lei e que fora muito debatido nos projetos de leis anteriores é sobre a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela tutela dos dados pessoais. Enquanto nos projetos de leis anteriores se falavam apenas da necessidade de o poder estatal criar um órgão que tivesse tais atribuições de maneira vaga, o presidente Michel Temer, através da análise constitucional, resolvendo o vício de iniciativa e os legisladores da LGPD foram inovadores ao especificarem qual será esse órgão e todas as atribuições, elencadas no rol dos arts. 55-A à 55-L da lei.

4.4.Responsabilidade civil

Sobre o tema, é imperioso destacar que a LGPD possui um corpo dotado de alguns preceitos semelhantes ao do Código de Defesa do Consumidor, levando em consideração a proteção do indivíduo acima dos interesses de outrem. Isso ocorre pelo fato de o legislador encarar aquele que cedeu suas informações como parte hipossuficiente da relação, com não tantos recursos jurídicos para delimitar seus atos, bem como pela necessidade que o operador ou o responsável pelo tratamento dos dados possui quanto ao tratamento dos dados pessoais, em razão da importância jurídica que este tem.

Sobre o tema, a responsabilidade civil dos operadores ou responsáveis é objetiva (na mesma forma do art. 186, 187 e 927 do Código Civil (LGL\2002\400)), ou seja, independe da comprovação de culpa ou dolo pelos atos praticados ou que foram deixados de praticar, sendo necessário apenas a comprovação dos danos causados.

Na LGPD, a responsabilidade civil é encontrada a partir do art. 42, atribuindo ao controlador ou ao operador a obrigação de reparar os dados causados no exercício da atividade de tratamento dos dados pessoais. No § 1º do mesmo artigo, aplica-se a responsabilidade solidária, que gera um certo efeito cascata no mercado, atingindo também as empresas responsáveis pela cessão dos dados.[40]

Existem hipóteses em que a responsabilidade civil é afastada, elencadas no rol do art. 43, sendo necessário comprovar que:

"I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros."

4.5.Sanções administrativas

As sanções administrativas são elencadas no Capítulo VIII, Seção I, a partir do art. 52, que vão desde advertências, multas, publicação da infração, bem como bloqueio dos dados pessoais até a regularização ou, em último caso, a eliminação dos dados pessoais (incisos I a VI).

Somente ocorrerão as sanções administrativas após o devido procedimento administrativo e respeitado o contraditório e a ampla defesa, observando a gravidade do ato praticado, o grau de dano, a existência da boa-fé, a reincidência, entre outros. Logo, pode-se garantir que o processo administrativo deverá respeitar os princípios básicos presentes na legislação, como também no direito processual em geral, mesmo que tal procedimento não dependa do trâmite do Processo Civil Brasileiro, no qual existe a figura

do juiz representando o Estado, a parte autora e a defesa, todos dotados de tutela jurisdicional. No entanto, não existe nada que exclui a hipótese dessas sanções serem aplicadas seguindo as normas do CPC (LGL\2015\1656) ou de leis equivalentes, principalmente em hipóteses que geram relevância jurídica ou houver interesse de menor. Também é importante ressaltar que o operador ou responsável pelo tratamento dos dados pessoais nem sempre será a parte passiva da demanda. Nada impede que ele possa instaurar um inquérito administrativo contra terceiro ou contra a própria pessoa que cedeu os dados, bem como requerer através do Judiciário a apreciação do ato administrativo.

Por fim, essas sanções referem-se exclusivamente a fatos que envolvam a LGPD ou no exercício dela. O Marco Civil da Internet ou demais normas não poderão sofrer penalidades previstas nesses artigos.

4.6.O papel do advogado na LGPD

Durante a vigência dessa nova legislação, o advogado possuirá uma função importante para a adequação das empresas a essa forma de tutela dos dados dos indivíduos, sejam eles físicos, sejam on-line. Ele será o Head da equipe, pois requer conhecimentos jurídicos para poder fazer com que não exista qualquer falha ou lacuna procedimental que descumpra algum requisito da norma.

Para tanto, é necessário envolver as áreas de Marketing, Pessoal e TI, de forma a construir uma linguagem aderente às suas necessidades para, finalmente, iniciar a operacionalização dos procedimentos que devem ser implantados para se manter em compliance e assegurar a proteção e cautela no tratamento de dados pessoais.[41] Além disso, esse também será responsável por assessorar e patrocinar a parte nos litígios envolvendo a proteção de dados pessoais judicialmente através do ajuizamento de demandas, como também extrajudicialmente, através de negociações entre as partes.

5.Conclusão

O presente trabalho buscou abordar de forma ampla e crítica a importância do tratamento dos dados pessoais no Brasil e no mundo, capaz de traduzir uma maior compreensão quanto à necessidade de existirem normas bem definidas e em consonâncias com os princípios e regramentos fundamentais entrincheirados na Constituição Federal.

Trata-se de um longo caminho que certamente será dotado de erros e acertos para que o direito à privacidade seja preservado também nesse novo campo que envolve o plano digital.

No entanto, com a ciência da informação e o necessário entendimento tanto por parte dos juristas quanto por parte da sociedade em geral de que os dados pessoais, desde os mais simples até os sensíveis, são extremamente importantes para a nossa vida, existirá uma cautela em cada ato praticado que envolva a cessão ou compartilhamento de alguma informação.

A internet com certeza mudou a forma como a vida das pessoas se relaciona e o século XXI é aquele em que tudo será automatizado, robótico, através de algoritmos e inteligência artificial. Para existir um controle sobre o tema, o Direito é o mecanismo mais importante para garantir que não exista nenhum tipo de dano e este (por muitos entendido como o mais tradicional) será o campo que caminhará mais próximo da tecnologia e das inovações.

Os dados pessoais inseridos e protegidos pelos princípios constitucionais da privacidade e da intimidade, nos termos do disposto no art. 5º da Constituição Federal de 1988, não bastam por si só. É necessário um verdadeiro arcabouço jurídico com as especificidades que o tema exige, notadamente em se tratando de direito digital e proteção de dados sensíveis. Nesse sentido, caminhou o progressivo regramento de aludidas questões,

iniciando-se pelo Código de Defesa do Consumidor que buscou trazer uma tutela relevante, acrescentando dispositivos referentes aos bancos de dados das empresas, em especial as de crédito. Em seguida, a "Lei Carolina Dieckmann" como a maior responsável pelo avanço das discussões sobre a necessidade de uma legislação específica e a cautela necessária no universo digital.

Posteriormente, com a entrada em vigor do Marco Civil, a internet começou a ser tratada de outra forma, como um direito fundamental e inerente ao ser humano. E entendido o Direito à Privacidade como um direito fundamental, a legislação que regula os dados pessoais (LGPD), sejam os físicos, sejam os on-line, transmutou-se em peça-chave para que em especial as empresas não utilizem de forma indevida as informações inerentes ao ser humano como uma forma de obter dividendos, mas sim que os indivíduos detenham o poder de requerer a reanálise, a exclusão, a transferência ou o acréscimo dos dados cedidos.

A vida é um filme e o direito dotado de natureza estática, por certo, sempre estará no encalço buscando regular a dinâmica e célere transformação do mundo fático. A velocidade com que a tecnologia avança, portanto, exige atenção em relação às novas relações que vêm surgindo, e cabe ao legislador estabelecer o regramento necessário, justamente para que os valores fundamentais de nossa Constituição continuem a serem protegidos.

Para Citar este artigo: Andréa, Gianfranco Faggin Mastro; Arquite, Higor Roberto Leite; Camargo, Juliana Moreira. Proteção dos dados pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil. Revista de Direito Constitucional e Internacional. vol. 121. ano 28. p. 115-139. São Paulo: Ed. RT, set.-out. 2020. Disponível em: (http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2020-11423)

6.Referências bibliográficas

AGUIAR JUNIOR, Ruy Rosado. Extinção dos contratos por incumprimento do devedor. 2. ed. Rio de Janeiro: Aide, 2003.

ALVES, Gustavo Furtado de Oliveira. O que é algoritmo? Dicas de Programação, São Paulo, 04 maio 2013. Disponível em: [https://dicasdeprogramacao.com.br/o-que-e-algoritmo]. Acesso em: 26.10.2019.

BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. Proteção de dados pessoais no Brasil: São Paulo: Artigo19, 2016. Disponível em: [https://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%c3%a7%c3%a3o-de-Dados-Pessoa Acesso em: 02.11.2019.

BERETTA, Pedro. Sem meios eficazes, Lei Carolina Dieckmann até atrapalha. Consultor Jurídico, São Paulo, 10 maio 2014. Disponível em: [www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha] . Acesso em: 31.10.2019.

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

CARVALHO, Diógenes Faria de; FERREIRA, Vitor Hugo Amaral. Defesa do consumidor ganha com a nova lei de proteção de dados pessoais. Consultor Jurídico, São Paulo, 15 ago. 2018. Disponível em: [www.conjur.com.br/2018-ago-15/garantias-consumo-defesa-consumidor-ganha-lei-protecao-dados] . Acesso em: 31.10.2019.

COALIZÃO DIREITOS NA REDE. Carta ao Senado pela imediata aprovação do PLC 53/2018. Disponível em: [[https://medium.com/direitos-na-rede/pela-imediata-aprovacao-do-plc53-18-e50072b37713].

Acesso em: 03.11.2019.

DRUMMOND, Marcílio Guedes. Proteção de dados além do óbvio. Migalhas, São Paulo, 28 jan. 2019. Disponível em: [www.migalhas.com.br/dePeso/16,MI294971,31047-Protecao+de+dados+alem+do+obvio]. Acesso em: 03.11.2019.

GUERRA FRIA. Só História. Virtuous Tecnologia da Informação, 2009-2019. Disponível em: [www.sohistoria.com.br/ef2/guerrafria]. Acesso em: 29.10.2019.

JINKINGS, Daniela. Governo vai debater criação de marco legal para proteção de dados pessoais no Brasil. Agência Brasil: Empresa Brasil de Comunicação, Brasília, v. 1, n. 1, p.1-1, 30 nov. 2010. Disponível em: [http://memoria.ebc.com.br/agenciabrasil/noticia/2010-11-30/governo-vai-debater-criacao-de-marco-l
Acesso em: 01.11.2019.

LEI GERAL DE PROTEÇÃO DE DADOS deve ter o mesmo peso do CDC (LGL\1990\40), afirma advogado. Consultor Jurídico, São Paulo, 11 set. 2018. Disponível em: [www.conjur.com.br/2018-set-11/lei-protecao-dados-peso-cdc-advogado]. Acesso em: 31.10.2019.

MOURA, Túlio. Um Breve Histórico da Internet. Dialhost, São Paulo, 17 de maio 2019. Disponível em: [www.dialhost.com.br/blog/um-breve-historico-da-internet]. Acesso em: 29.10.2019.

O QUE É ARPANET. Disponível em: [https://sites.google.com/site/sitesrecord/o-que-e-arpanet]. Acesso em: 29.10.2019.

POLIDO, Fabrício B. Pasquot et al. GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. Disponível em: [http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercussões-no-direito-brasileiro-Prir
. Acesso em: 31.10.2019.

PONTES DE MIRANDA, Francisco Cavalcanti. Tratado de direito privado. Rio de Janeiro: Borsoi, 1971. t. VII.

PRADO, Jean. O que Temer vetou na lei de proteção de dados pessoais: O principal foi a ANPD, mas existem outros vetos no texto aprovado pelo presidente Michel Temer que seriam importantes. Tecnoblog, São Paulo, ago. 2018. Disponível em: [https://tecnoblog.net/255745/vetos-lei-dados-pessoais-temer]. Acesso em: 03.11.2019.

SCARTEZINI, Vanda; WEIKERSHEIMER, Deana. Os dados, o cidadão digital e a LGPD no Brasil. Convergência Digital, São Paulo, 25 out. 2019. Disponível em: [https://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=52082&sid=15]. Acesso em: 04.11.2019.

SCHREINERT, Ricardo Ruiz; RUARO, Regina Linden. O direito à proteção de dados pessoais na sociedade de vigilância: a necessidade de um marco regulatório como dever prestacional do estado democrático de direito. Anais do Seminário Interno de Avaliação da Iniciação Científica. Edição I, 22 a 25 de agosto de 2011. Porto Alegre: Pontifícia Universidade Católica do Rio Grande do Sul. Disponível em: [https://docplayer.com.br/45242426-Ricardo-ruiz-schreinert-regina-linden-ruaro-1-orientador-resumo.

SOUZA, Thiago Pinheiro Vieira de. A proteção de dados pessoais e a [in]civilidade do uso de cookies. Monografia (Conclusão de Curso) – Faculdade de Direito, Universidade Federal de Uberlândia, Uberlândia, 2018. Disponível em: [https://repositorio.ufu.br/bitstream/123456789/23198/3/Prote%C3%A7%C3%A3oDadosPessoais.pdf]
Acesso em: 26.10.2019.

UNIÃO EUROPEIA, Jornal Oficial (2016). Disponível em: [https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL]. Acesso em: 29.10.2019.

VALENTE, Jonas. Bolsonaro sanciona, com vetos, lei sobre proteção de dados. Agência Brasil, Brasília, v. 1, n. 1, p. 1-1, 10 jul. 2019. Disponível em: [http://agenciabrasil.ebc.com.br/geral/noticia/2019-07/bolsonaro-sanciona-com-vetos-lei-sobre-protec . Acesso em: 03.11.2019.

---

1 BRASIL. Lei 12.965 de 23 abril de 2014. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm]. Acesso em: 26.10.2019.

2 Para exemplificar: Tício gosta de Rock. Durante o dia, acessa um site de Streaming para ouvir bandas do seu gênero preferido. O serviço de Streaming, ao reconhecer o estilo musical mais acessado por Tício através da leitura dos seus dados sensíveis (preferência sonora), automaticamente sugere novas músicas para este ouvir, mas do mesmo gênero. Aqui ocorreu uma espécie de "receita" no qual o serviço de Streaming utilizou para proporcionar uma melhor experiência do usuário. Basicamente ele entendeu que se Tício ouve Rock todos os dias, deve gostar de bandas do mesmo estilo. Logo, as melhores sugestões para ele seja apresentar opções do seu seguimento musical preferido (ALVES, Gustavo Furtado de Oliveira. O que é algoritmo? Dicas de Programação, São Paulo, 04 maio 2013. Disponível em: [https://dicasdeprogramacao.com.br/o-que-e-algoritmo]. Acesso em: 26.10.2019).

3 SOUZA, Thiago Pinheiro Vieira de. A proteção de dados pessoais e a [in]civilidade do uso de cookies. Monografia (Conclusão de Curso) – Faculdade de Direito, Universidade Federal de Uberlândia, Uberlândia, 2018. p. 26. Disponível em: [https://repositorio.ufu.br/bitstream/123456789/23198/3/Prote%C3%A7%C3%A3oDadosPessoais.pdf] Acesso em: 26.10.2019.

4 GUERRA Fria. Só História. Virtuous Tecnologia da Informação, 2009-2020. Disponível em: [www.sohistoria.com.br/ef2/guerrafria]. Acesso em: 29.10.2019.

5 O QUE É ARPANET. Disponível em: [https://sites.google.com/site/sitesrecord/o-que-e-arpanet]. Acesso em: 29.10.2019.

6 MOURA, Túlio. Um breve histórico da internet. Dialhost, São Paulo, 17 de maio 2019. Disponível em: [www.dialhost.com.br/blog/um-breve-historico-da-internet]. Acesso em: 29.10.2019.

7 UNIÃO EUROPEIA. Jornal Oficial, 2016. Disponível em: [https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL]. Acesso em: 29.10.2019.

8 Artigo 9º

Tratamento de categorias especiais de dados pessoais

1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. (UNIÃO EUROPEIA. Regulamento (UE) 2016/679. Disponível em: [https://gdpr-info.eu]. Acesso em: 29.10.2019).

9 CHILE. Lei 19.628, de 6 de agosto de 1999. Disponível em: [www.leychile.cl/Navegar?idNorma=141599]. Acesso em: 29.10.2019.

10 ARGENTINA. Ley 25.326, de 4 de outubro de 2000. Disponível em: [http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm]. Acesso em: 29.10.2019.

11 ARGENTINA. Decreto Parlamentar 1558, de 29 de novembro de 2001. Disponível em: [http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm] . Acesso em: 29.10.2019.

12 URUGUAI. Ley 18.331, de 18 de agosto de 2008 Disponível em: [www.oas.org/es/sla/ddi/docs/U4%20Ley%2018.331%20de%20Protecci%C3%B3n%20de%20Datos%2 . Acesso em: 29.10.2019.

13 PERU. Ley 29.733, de 3 de julho de 2011. Disponível em: [www.oas.org/es/sla/ddi/docs/P6%20Ley%2029733%20de%20protecci%C3%B3n%20de%20datos%20 . Acesso em: 29.10.2019.

14 RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. Legislación Venezuela. Disponível em: [www.informatica-juridica.com/legislacion/Venezuela]. Acesso em: 29.10.2019.

15 Vide as leis Hessisches Datenschutzgesetz, de 1970 na Alemanha e Sw. Datalagen, na Suécia. Ambas as normas surgiram também em razão do avanço tecnológico, já prevendo que as informações pessoais serão comumente armazenadas em computadores, podendo ser acessível de forma ampla e geral. Disponível em: [www.scandinavianlaw.se/pdf/47-18.pdf] e [www.ess-koeln.de/dokumente/160/151010084004Hessen.pdf]. Acesso em: 30.10.2019.

16 POLIDO, Fabrício B. Pasquot et al. GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. Disponível em: [http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercussões-no-direito-brasileiro-Prir . Acesso em: 31.10.2019.

17 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 184.

18 Lei de Proteção de Dados deve ter o mesmo peso do CDC, afirma advogado. Consultor Jurídico, São Paulo, 11 set. 2018. Disponível em: [www.conjur.com.br/2018-set-11/lei-protecao-dados-peso-cdc-advogado]. Acesso em: 31 out. 2019.

19 CARVALHO, Diógenes Faria de; FERREIRA, Vitor Hugo Amaral. Defesa do consumidor ganha com a nova lei de proteção de dados pessoais. Consultor Jurídico, São Paulo, 2018. Disponível em: [www.conjur.com.br/2018-ago-15/garantias-consumo-defesa-consumidor-ganha-lei-protecao-dados]. Acesso em: 31.10.2019.

20 BRASIL. Lei 12.414, de 2015. Disponível em: [www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm]. Acesso em: 31.10.2019.

21 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 185.

22 BRASIL. Lei 12.737, de 30 de novembro de 2012. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm]. Acesso em: 31.10.2019.

23 BERETTA, Pedro. Sem meios eficazes, Lei Carolina Dieckmann até atrapalha. Consultor Jurídico, São Paulo, 10 maio 2014. Disponível em: [www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha]. Acesso em: 31.10.2019.

24 BRASIL. Lei 12.965, de 23 de abril de 2014. Disponível em: [www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm]. Acesso em: 01.11.2019.

25 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 186.

26 Confira-se o art.7º da apontada Lei: "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: [...]

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."

27 EDWARD SNOWDEN. In: WIKIPÉDIA, a enciclopédia livre. São Francisco: Wikimedia Foundation, 2020. Acesso em 02 nov. 2019. Disponível em: [https://pt.wikipedia.org/w/index.php?title=Edward_Snowden&oldid=57363368].

28 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 186.

29 Existiram, principalmente, os Projetos de Lei 4060/2012, 330/2013 e 5276/2016. Porém, todos com vícios que não retratavam a necessidade da proteção de dados como direito fundamental. Por certo serviram para avançar no debate da questão da proteção de dados. Para maior aprofundamento das problemáticas constantes dos aludidos projetos ver: BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. Proteção de dados pessoais no Brasil: São Paulo: Artigo19, 2016. Disponível em: [https://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%c3%a7%c3%a3o-de-Dados-Pessoa . Acesso em: 02.11.2019.

30 Manifesto apresentado em 13 de julho de 2018, em defesa da aprovação pelo Senado do Projeto de Lei da Câmara 53 de 2018. Disponível em: [https://brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais] . Acesso em: 03.11.2019.

31 Trata-se de outro manifesto também requerendo a aprovação da PLC 53/2018, dessa vez apresentado pela Coalizão Direitos na Rede. Disponível em: [https://medium.com/direitos-na-rede/pela-imediata-aprovacao-do-plc53-18-e50072b37713] . Acesso em: 03.11.2019.

32 BRASIL. Projeto de Lei da Câmara 53, de 2018. Disponível em: [https://legis.senado.leg.br/sdleg-getter/documento?dm=7738705&ts=1571776630943&disposition=in . Acesso em: 03.11.2019.

33 Os vetos levados a efeito pelo ex-presidente Michel Temer recaíram sobre a Autoridade Nacional de Proteção de Dados (mero vício formal que fora superado pela MP 869/2019) e as sanções administrativas sobre as empresas e organizações que descumprissem a Lei, que suspendia e proibia o acesso a bancos de dados, o que inviabilizaria, por vezes, a própria função essencial das empresas. Outros vetos foram o da publicidade do compartilhamento de dados pessoais entre os entes públicos (art. 28 e inciso II do art. 23) e a transferência com as entidades privadas (art. 26, § 1º) (PRADO, Jean. O que Temer vetou na lei de proteção de dados pessoais: O principal foi a ANPD, mas existem outros vetos no texto aprovado pelo presidente Michel Temer que seriam importantes.Tecnoblog, São Paulo, ago. 2018. Disponível em: [https://tecnoblog.net/255745/vetos-lei-dados-pessoais-temer]. Acesso em: 03.11.2019).

34 O Presidente da República Jair Bolsonaro foi o responsável por sancionar a Lei 13.853/2019, responsável por alterar a LGPD ao criar a Autoridade Nacional de Proteção de Dados Pessoais e da Privacidade. Alterou ponto, outrossim, no sentido de que pessoas jurídicas, além das físicas, poderão fazer revisões automatizadas. Porém, abre espaço para que existam novos softwares para tanto, como um responsável apenas para a revisão dessas decisões (VALENTE, Jonas. Bolsonaro sanciona, com vetos, lei sobre proteção de dados. Agência Brasil, Brasília, v. 1, n. 1, p.1-1, 10 jul. 2019. Disponível em: [http://agenciabrasil.ebc.com.br/geral/noticia/2019-07/bolsonaro-sanciona-com-vetos-lei-sobre-protec Acesso em: 03.11.2019).

35 FORTES ADVOGADOS. Proteção de dados: o que mudou no Marco Civil da Internet?, 21 ago. 2018. Disponível em: [www.fortesadvogados.com.br/blog/protecao-de-dados-o-que-mudou-no-marco-civil-da-internet]

. Acesso em: 03.11.2019.

36 Cf., entre outros, PONTES DE MIRANDA, Francisco Cavalcanti. Tratado de direito privado. Rio de Janeiro: Borsoi, 197. t. VII. p. 124 e ss.

37 SCHREINERT, Ricardo Ruiz; RUARO, Regina Linden. O direito à proteção de dados pessoais na sociedade de vigilância: a necessidade de um marco regulatório como dever prestacional do estado democrático de direito. Anais do Seminário Interno de Avaliação da Iniciação Científica. Edição I, 22 a 25 de agosto de 2011. Porto Alegre: Pontifícia Universidade Católica do Rio Grande do Sul. Disponível em: [https://docplayer.com.br/45242426-Ricardo-ruiz-schreinert-regina-linden-ruaro-1-orientador-resumo.

38 AGUIAR JUNIOR, Ruy Rosado. Extinção dos contratos por incumprimento do devedor. 2. ed. Rio de Janeiro: Aide, 2003. p. 238.

39 AGUIAR JUNIOR, Ruy Rosado. Op. cit., 2003.

40 DRUMMOND, Marcílio Guedes. Proteção de dados além do óbvio: a conclusão que se chega ao analisar a LGDP além do óbvio é de que se trata de uma lei a ser construída no cotidiano das empresas e das pessoas, com uma multa aqui e outra ali para "servir de exemplo", mas que com o tempo provavelmente ganhará força e relevância maior na qualidade reputacional das corporações. Migalhas, São Paulo, 2019. Disponível em: [www.migalhas.com.br/dePeso/16,MI294971,31047-Protecao+de+dados+alem+do+obvio]. Acesso em: 03.11.2019.

41 SCARTEZINI, Vanda; WEIKERSHEIMER, Deana. Os dados, o cidadão digital e a LGPD no Brasil. Convergência Digital, São Paulo, 2019. Disponível em: [https://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=52082&sid=15] . Acesso em: 04.11.2019.