UNIVERSIDADE FEDEREAL DE OURO PRETO
Departamento de Direito

Talita Aguiar Seleiro

CONTROLE DE DADOS PESSOAIS:
a Identidade *Blockchain* como ferramenta de proteção de dados pessoais

Ouro Preto
2020

Talita Aguiar Seleiro

CONTROLE DE DADOS PESSOAIS:

a Identidade *Blockchain* como ferramenta de proteção de dados pessoais

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientadora: Juliana Almeida Evangelista

Ouro Preto

2020

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

S464c Seleiro, Talita Aguiar .
CONTROLE DE DADOS PESSOAIS [manuscrito]: a Identidade Blockchain como ferramenta de proteção de dados pessoais. / Talita Aguiar Seleiro. - 2020.
56 f.

Orientadora: Profa. Dra. Juliana Almeida Evangelista.
Monografia (Bacharelado). Universidade Federal de Ouro Preto. Escola de Direito, Turismo e Museologia. Graduação em Direito .

1. Direito à privacidade. 2. Sigilo (Direito). 3. Sigilo (Direito) - Identidade digital. 4. Proteção da confiança (Direito) - Blockchain. I. Evangelista, Juliana Almeida. II. Universidade Federal de Ouro Preto. III. Título.

CDU 347.51

Bibliotecário(a) Responsável: Maristela Sanches Lima Mesquita - CRB: 1716

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Talita Aguiar Seleiro

CONTROLE DE DADOS PESSOAIS: a Identidade *Blockchain* como ferramenta de proteção de dados pessoais

Membros da banca

Prof. Dra. Juliana Almeida Evangelista (Orientadora)
Prof. Dra. Beatriz Schettini (Banca examinadora)
Felipe Melazzo do Nascimento Santos (Banca examinadora)

Versão final
Aprovado em 16 de Novembro de 2020

De acordo

Prof. Dra. Juliana Almeida Evangelista

Documento assinado eletronicamente por **Juliana Evangelista de Almeida**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 19/11/2020, às 12:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0104349** e o código CRC **78316D9A**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 23109.008783/2020-19 SEI nº 0104349

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: 3135591545 - www.ufop.br

À minha amada e saudosa mãe, minha maior inspiração e fonte de motivação.

RESUMO

Este trabalho busca verificar a possibilidade de utilização da identidade digital baseada na tecnologia *blockchain* como ferramenta de proteção de dados pessoais. Será exposta a evolução do direito à privacidade até o surgimento do direito à proteção de dados pessoais, expondo como os dados pessoais são relevantes para a sociedade atual, denominada sociedade da informação. O direito à proteção de dados pessoais vem ganhando relevância com o desenvolvimento constante e crescente das tecnologias e com a elaboração de legislações de proteção de dados pessoais, como é o caso da LGPD, no Brasil. Diante disso, defende-se que as tecnologias devem ser utilizadas de forma a contribuir com a proteção dos dados pessoais, a partir de ferramentas que garantam ao titular o controle e autonomia sobre os seus dados pessoais. Será utilizada a abordagem jurídico-dogmático como metodologia, haja vista a utilização das normas jurídicas como dogmas prefixados e sua interpretação de acordo com a mutabilidade dos fatos sociais, principalmente aqueles decorrentes do desenvolvimento tecnológico. A pesquisa é qualitativa, com enfoque em pesquisas bibliográficas e documentais e tem como objetivo apontar a potencialidade da tecnologia *blockchain* como instrumento de proteção de dados pessoais, principalmente através da ferramenta identidade digital baseada em *blockchain*, também denominada *self-sovereign identity* (identidade autossoberana).

Palavras-chave: Privacidade. Proteção de dados pessoais. Identidade digital. *Blockchain*.

ABSTRACT

This paper seeks to verify the possibility to use a digital identity based on *blockchain* as a personal data protection tool. It will be exposed the right to privacy and its evolution until the emerging needs to protection of personal data, exposing how personal data are relevant to today's society, also known as information society. The personal data protection as a right has been gaining relevance with the constant and growing development of technologies and the personal data protection laws around the world, such as LGPD in Brazil. Therefore, it is argued that technologies should be used in order to contribute to personal data protection, using tools that guarantee the owner control and autonomy over their personal data.The juridical-dogmatic approach will be used as a methodology, considering the use of legal norms as preset dogmas and their interpretation according to the mutability of social facts, mainly those resulting from technological development. The research is qualitative, with a focus on bibliographic and documentary research and aims to point out the potential of blockchain technology as an instrument of personal data protection, mainly through the blockchain-based digital identity tool, also called self-sovereign identity.

Key-words: Privacy. Personal data protection. Digital identity. Blockchain.

SUMÁRIO

1 INTRODUÇÃO

O direito à privacidade se transformou ao longo dos anos e, principalmente, nos tempos atuais, em que as relações pessoais são permeadas pelas tecnologias. O fluxo de informações é desmedido e impacta diretamente na privacidade dos indivíduos, haja vista que há uma exposição imensa e descontrolada da vida privada e de aspectos íntimos da pessoa. Concomitantemente, devido ao constante desenvolvimento tecnológico, a personalidade da pessoa vem sendo cada vez mais "datificada", isto é, os dados pessoais tornam-se a expressão do indivíduo, já que simbolizam aspectos da personalidade humana.

Dessa forma, os dados pessoais passam a ter alto valor na sociedade da informação, sendo essenciais para o desenvolvimento dos mais diversos negócios e da economia, o que faz com que muitas organizações tenham acesso e tratem os dados pessoais. Assim, frequentemente o acesso e tratamento de dados pessoais podem implicar em violações à privacidade e à liberdade das pessoas, ao passo que interferem diretamente nas escolhas, autonomia e individualidade dos seres humanos. Nota-se que, atualmente, o indivíduo se encontra totalmente vulnerável.

Diante disso, é indispensável que os dados pessoais sejam tutelados, de modo que cada pessoa tenha acesso e controle aos seus dados para que seja protegido o direito à privacidade e garantido o livre desenvolvimento da pessoa humana. É necessário que o indivíduo tenha acesso aos seus dados pessoais, que lhe seja garantido o controle sobre eles e que tenha segurança sobre a finalidade e destinação de seus dados pessoais. Nesse contexto, emerge o direito à proteção de dados pessoais, decorrente do direito à privacidade e com fins de assegurar aspectos fundamentais da liberdade e do livre desenvolvimento da personalidade.

Estudar-se-á como as tecnologias podem colaborar para o efetivo controle e proteção de dados pessoais, de modo que seja assegurado ao titular desses a autonomia sobre as suas informações e a sua identidade, sendo o objetivo principal do trabalho averiguar se a identidade *blockchain* pode ser uma ferramenta para a proteção de dados pessoais. O trabalho perpassa pela evolução do direito à privacidade e o direito à proteção de dados pessoais, como estes direitos se situam no ordenamento jurídico brasileiro até a promulgação de uma legislação geral sobre o assunto no Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018.

Serão indicados alguns mecanismos que já contribuem para a proteção dos dados pessoais no ambiente virtual, como a assinatura digital e a certificação digital. Entretanto, como espera-se que LGPD cause um grande impacto social econômico, é importante que

sejam atualizadas as ferramentas de segurança de dados e melhoria nos procedimentos e fluxos de dados pessoais. Assim, será exposto como a tecnologia *blockchain* pode ser um instrumento de auxílio para garantir a aplicação da LGDP, através da identidade digital baseada em *blockchain.*

Não se pretende com este trabalho esgotar as possibilidades de aplicação da tecnologia *blockchain*, tendo em vista que é uma tecnologia ainda emergente que certamente passará por transformações nos próximos anos, dada a celeridade do desenvolvimento tecnológico atual. A intenção é apresentar a potencialidade desta tecnologia quando aplicada à identidade digital como ferramenta para a proteção de dados pessoais.

A utilização da identidade digital baseada em *blockchain* surge como uma promessa para garantir um sistema de identificação digital seguro e exclusivo. Será verificada a compatibilidade da tecnologia com a legislação de proteção de dados pessoais para que seja utilizada como instrumento aliado à LGPD, de modo a contribuir com o empoderamento das pessoas sobre os seus dados pessoais, garantindo-lhes o direito à autodeterminação informativa e permitindo o livre desenvolvimento da personalidade no ecossistema digital.

2 DA PRIVACIDADE

O crescente e contínuo desenvolvimento das TICs (tecnologias da informação e comunicação), bem como a consolidação de espaços públicos em ambientes virtuais, fez com que as informações pessoais se tornassem a expressão do indivíduo e de sua personalidade. Assim, como forma de se proteger a privacidade do indivíduo, visando o livre desenvolvimento da personalidade, faz-se necessária a proteção de seus dados pessoais.

Dessa forma, nota-se a existência de uma profunda conexão entre a proteção de dados pessoais com a tutela da privacidade, razão pela qual deve ser contextualizado o conceito de privacidade. Como se verá adiante, é um conceito mutável, que se transformou diante da evolução social e do desenvolvimento tecnológico, por isso, será exposto como se deu a sua evolução até o surgimento da necessidade de tutelar especificamente os dados pessoais.

2.1 A evolução do direito à privacidade

O conceito de privacidade é um conceito volátil, que varia no tempo e no espaço. A origem da privacidade se deu com a desagregação da sociedade feudal e a ascensão da burguesia. Com o surgimento das habitações privadas e a nova disposição das cidades, o isolamento torna-se algo propício, revelando uma nova necessidade: a intimidade (RODOTÁ, 2008).

Antigamente a concepção de privacidade era diretamente associada à proteção da propriedade privada, sendo o isolamento considerado um privilégio da classe burguesa, pois era a classe da sociedade que tinha condições materiais de proteger o seu próprio espaço e desfrutar da própria intimidade. Percebe-se que a privacidade não era uma experiência natural de cada indivíduo, mas sim um privilégio de um grupo específico, decorrente do direito da propriedade (RODOTÁ, 2008).

Apenas no final do século XIX a privacidade surgiu como um direito autônomo, desvinculado do direito à propriedade. Tal marco se dá com a publicação do famoso artigo "*The Right to Privacy"*, de Warren e Brandeis, publicado na *Harvard Law Review*, em 1890. Os autores construíram uma concepção a este direito fundamentada na inviolabilidade pessoal da intimidade.

Pautados nas transformações da sociedade, decorrentes do advento das tecnologias e preocupados principalmente com a divulgação de informações íntimas de forma não autorizada, os autores pregaram pela criação e proteção de novos direitos. O artigo apresenta a

concepção do direito à privacidade a partir da expressão inaugurada pelo juiz norte americano Thomas Cooley, em 1873, "*the right to be let alone*" (o direito de estar só), exaltando um individualismo exacerbado e uma índole solitária do indivíduo (NAVARRO, 2011). A privacidade vai sendo identificada como aquilo que a pessoa é, e não aquilo o que ela tem, aludindo à ideia da privacidade como direito da personalidade.

Com o passar do tempo, foi se desenvolvendo cada vez mais a ideia da tutela jurídica da privacidade, com o entendimento de que é essencial para a realização da pessoa humana e do livre desenvolvimento de sua personalidade (DONEDA, 2020).

A Segunda Guerra Mundial foi um elemento catártico para a evolução dos direitos e para a consolidação dos direitos da personalidade, visto que no período subsequente à guerra surgiu a necessidade de proteger o ser humano em sua essência. O ordenamento jurídico passou a assumir responsabilidade pela tutela da pessoa em sentido amplo, reconhecendo o princípio da dignidade humana como fundamento dos direitos da personalidade (BLUM, 2018).

Em 1984, decorrente da recognição da dignidade da pessoa humana, o direito à privacidade foi tutelado em âmbito internacional, com a promulgação da Declaração Universal dos Direitos Humanos (DUDH). O direito à privacidade foi consagrado no artigo 12 da DUDH: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei*"*.

Nota-se que não é possível limitar a privacidade à ideia de espaço privado, haja vista o caráter relacional assumido pela privacidade, que se tornou determinante na construção do indivíduo como ser, no desenvolvimento de sua personalidade e na sua inserção na sociedade (CANCELIER, 2017).

Com as transformações na sociedade e a consequente evolução do conceito de privacidade, a dicotomia entre o público e o privado foi superada e, cada vez mais, o direito à privacidade vem sendo reconhecido como um direito da personalidade, tanto na jurisprudência como na legislação constitucional de diversos países.

No Brasil, a privacidade é reconhecida como direito fundamental, tutelado não só pela Constituição Federal de 1988, mas também pelo Código Civil de 2002 e por artigos esparsos na legislação infraconstitucional. Vale ressaltar que o legislador não tratou o tema se referindo à privacidade propriamente dita, mas optou por fazer uma abordagem mais ampla do direito à privacidade, utilizando as palavras "vida privada" e "intimidade".

Como anteriormente mencionado, o direito à privacidade é não só um direito fundamental, previsto constitucionalmente, mas é também um direito da personalidade. Assim, para melhor compreensão do assunto, faz-se necessário conceituar os direitos da personalidade antes de abordar mais profundamente o direito à privacidade.

A princípio, cumpre ressaltar que os direitos da personalidade são aqueles inerentes à condição da pessoa humana, que por sua vez, deve ser protegida em todos os seus aspectos e manifestações. Santos Cifuentes (1999, p. 54) define os direitos da personalidade como: "direitos subjetivos privados, inatos e vitalícios, que têm por objeto manifestações interiores da pessoa, e que, por serem inerentes, extrapatrimoniais e necessários, não podem ser transmitidos nem disponibilizados de forma absoluta e radical"[1].

Não obstante à definição apresentada, destaca-se que o direito da personalidade não pode ser limitado a uma previsão normativa específica, uma vez que deve estar apto a tutelar a pessoa humana e todas as suas condições e manifestações possíveis, abarcando toda a sua complexidade, a fim de permitir o livre desenvolvimento da personalidade. Nesse sentido, Paulo Mota Pinto (1993, p. 491, *apud* DONEDA, 2020) explica que o direito da personalidade é "aberto, sincrônica e diacronicamente", por isso permite a tutela de novos bens que venham a surgir em decorrência de novas ameaças à pessoa humana, fundamentando-se sempre no respeito pela personalidade, independente da ocorrência de mudanças, ou não, no desenrolar do desenvolvimento da pessoa.

Vê-se que a personalidade não é um direito propriamente dito, mas um atributo imanente à pessoa, em que são apoiados os direitos e deveres a ela inerentes. A personalidade é parte intrínseca da pessoa humana, que permite que o titular exercite, modifique, conduza e defenda os seus interesses. Daí decorre a necessidade de tutelá-la, haja vista que os direitos da personalidade estão atrelados ao desenvolvimento da pessoa humana, como forma de garantir e preservar a sua dignidade (FARIAS, 2015).

Em horizonte equivalente, Bittar (2015, p. 41) expõe que os direitos da personalidade devem ser compreendidos como:

> a) os próprios da pessoa em si (ou originários), existentes por sua natureza, como ente humano, com o nascimento; b) e os referentes às suas projeções para o mundo exterior (a pessoa como ente moral e social), ou seja, em seu relacionamento com a sociedade.

[1] Texto original, em espanhol: "derechos subjetivos privados, innatos y vitalicios, que tienen por objeto manifestaciones inferiores de la persona, y que, por ser inherentes, extrapatrimoniales y necesarios, no pueden transmitirse ni disponerse en forma absoluta y radical*"*.

À vista disso, conclui-se que os direitos da personalidade buscam tutelar a identidade de cada um, visando à proteção da capacidade de a pessoa desenvolver suas particularidades, permitindo que esta expresse e desenvolva pensamentos e sentimentos próprios, construa valores e defenda sua essência e dignidade. Os direitos da personalidade são conferidos à pessoa como forma de proteger as características personalíssimas, respeitando o livre desenvolvimento da pessoa em suas projeções sociais, morais, físicas e intelectuais, de maneira a resguardar a individualidade de cada um.

Isso posto, descomplica-se o entendimento de que o direito à privacidade é um direito da personalidade, pois proteger a vida privada e a intimidade da pessoa é uma forma de resguardar a sua individualidade. Conforme enuncia Farias (2015, p. 215), *ipsis litteris*, "o direito à vida privada, como um bem integrante da personalidade, funda-se no legítimo interesse de salvaguardar do conhecimento alheio tudo o que diz respeito à esfera íntima de uma pessoa".

O direito à privacidade enquadra-se como direito da personalidade ao passo que valoriza a liberdade individual e protege as escolhas pessoais como forma de exercer a cidadania e a liberdade civil de cada um. De acordo com Rodotá (2008, p. 15), o direito à privacidade é "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".

Segundo Doneda (2020), a privacidade deve ser compreendida como um espaço de liberdade com condições de desenvolvimento da própria personalidade, livre de qualquer tipo de controle social. Já que as interferências e influências de terceiros poderiam resultar em perda da individualidade da pessoa, bem como impossibilitariam o uso da autonomia privada e dificultaria o livre desenvolvimento da personalidade. Atribui-se à privacidade uma posição de destaque na proteção da pessoa humana, não apenas no que se refere ao mundo externo, mas também como um elemento que incita a autonomia e a cidadania.

Vianna (2006, p. 73) afirma que o direito à privacidade é composto por três direitos "o direito de não ser monitorado, o direito de não ser registrado e o direito de não ser reconhecido", esse último compreendido como o direito de não ter registros pessoais publicados. Dessa forma, transcende as limitações do direito privado, tornando-se um dos fundamentos do Estado Democrático de Direito, pois favorece a liberdade de manifestação de pensamento e a igualdade jurídica.

Como inicialmente mencionado, o direito à privacidade não é unitário e concreto, é na realidade um conceito dinâmico e maleável, que vai se moldando de acordo com a cultura, com os valores e se transformando conforme vão ocorrendo mudanças na sociedade. Com a

expansão das tecnologias e principalmente a partir das novas técnicas de comunicação, as pessoas têm ficado cada vez mais expostas e têm tido a sua privacidade cada vez mais invadida.

Desta feita, a tutela da privacidade não se limita ao isolamento da pessoa e ao resguardo de sua vida privada, em que são protegidos os bens e os espaços, relaciona-se mais a uma lógica de construção da esfera pessoal a partir de livres escolhas existenciais. Muitos dos interesses que influenciam diretamente nas escolhas e na construção do ser estão envolvidos com a coleta e uso de informações pessoais. Nesse contexto, constata-se que o direito à privacidade muito se aproxima do controle que a pessoa possui sobre os seus dados, sendo que a tutela se volta para o uso de dados pessoais, para a forma de coleta e tratamento das informações pessoais disponibilizadas o tempo todo (BLUM, 2018).

Segundo expõe Paesani (2014, p. 35), surge um "novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações mesmo quando disponíveis em bancos de dados". Nesse sentido, a tutela à privacidade volta-se para as informações pessoais e manifesta-se principalmente, mas não somente, a partir da proteção de dados pessoais.

Com a contínua expansão das técnicas de comunicação e virtualização das relações sociais, as pessoas ficam expostas permanentemente, nos mais diferentes aspectos, profissionais, pessoais e sociais. Assim, esse direito vem assumindo, progressivamente, mais relevo no ordenamento jurídico, principalmente em um contexto de Estado Democrático de Direito.

O crescente uso da internet gera uma circulação de dados informáticos enorme, que possibilita o acúmulo indiscriminado de informações particulares dos indivíduos nas mais diversas condições, possibilitando também a confrontação e comunicação entre as informações obtidas. Logo, surge a necessidade de proteger os dados pessoais e criar institutos jurídicos que permitam o controle sobre as próprias informações, o que leva à ratificação do direito à autodeterminação informativa, decorrente do direito à privacidade (PAESANI, 2014).

Conforme ensina Mendes (2014), a autodeterminação informativa é compreendida como uma vertente do direito à privacidade, que garante que o indivíduo tenha controle sobre as suas informações e dados pessoais, ressaltando a autonomia da pessoa humana. Portanto, revela-se importante explanar os conceitos de dados pessoais e dados pessoais sensíveis preliminarmente, para que seja mais bem abordada a proteção de dados pessoais, bem como o direito à proteção de dados pessoais.

2.2 Dados pessoais e dados pessoais sensíveis

Na sociedade atual, denominada como sociedade da informação[2], as pessoas encontram-se constantemente imersas em um universo de informações, mantêm-se conectadas a dispositivos eletrônicos ininterruptamente para atingir os seus objetivos sociais, profissionais, pessoais, econômicos e políticos. Encontram-se diariamente expostas, pois transmitem, recebem, processam e armazenam dados instantânea e intensamente, às vezes até mesmo sem notarem que estão disponibilizando suas informações pessoais (FERREIRA, 2019).

Nesse contexto, a transmissibilidade de dados ocorre em tempo real, o que avulta a importância da proteção dos dados pessoais e a necessidade de o indivíduo possuir controle sobre as próprias informações. Por mais que os conceitos dados e informações sejam, muitas vezes, considerados sinônimos, deve-se destacar que não são. O dado é o estado primordial da informação. Explica-se a diferenciação através das palavras de Bioni (2020, p. 31): "dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação".

A Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, trouxe expresso o conceito de dados pessoais:

> Artigo 2º: a) 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.

Na linha da definição da Diretiva, Sarmento Castro (2005, *apud* OLIVEIRA 2017) descreve que dado pessoal é aquele relacionado a um indivíduo identificado ou identificável, sendo indiferente a forma como o dado está registrado, seja por imagem, escrita, áudio ou vídeo. O indivíduo identificado é compreendido por aquele que já é conhecido e o identificável é a pessoa que tem a possibilidade de ser conhecida, diretamente pelo titular de seus dados, ou indiretamente por meio de recursos que estejam disponíveis para outrem.

A Lei Geral de Proteção de Dados Pessoais – que será abordada mais profundamente em capítulo posterior – no inciso I, do artigo 5º, conceitua dado pessoal como "informação relacionada à pessoa natural identificada ou identificável". Vê-se que a definição da lei é bem abrangente, de forma que quaisquer informações relacionadas à pessoa podem ser consideradas como dados pessoais.

[2] De acordo com Bioni (2020) "a informação é o (novo) elemento estruturante que (re)organiza a sociedade".

Pinheiro (2020, p. 35) explica que os dados pessoais podem ser os mais diversos e que são sempre relativos à pessoa natural viva. Para a autora, os dados pessoais são:

> toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço profissional ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras número do *Internet Protocol* (IP), dados acadêmicos, histórico de compras, entre outros.

Nota-se, a partir do exposto, que o conceito de dados pessoais é bem amplo e expansivo. Para que um dado seja pessoal, basta que determinada informação possibilite a identificação de um sujeito, direta ou indiretamente. Há que se destacar, porém, que alguns dados pessoais, por estarem relacionados a características da personalidade da pessoa humana, podem possuir potencial discriminatório a depender a forma como forem tratados e a finalidade de uso. Esses dados merecem definição específica, são os dados pessoais sensíveis.

A definição de dado pessoal sensível está disposta na Lei Geral de Proteção de Dados Pessoais, no art. 5º, inciso II:

> 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.

Pinheiro (2020) explica que os dados pessoais sensíveis são aqueles relativos a atributos da personalidade do ser humano e suas escolhas particulares, como crença religiosa, opinião política, origem racial ou étnica, orientação sexual, filiações ideológicas, dados genéticos, de saúde e biométricos.

Segundo Bioni (2020, p. 83), “os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação”. Isto é, no momento de coleta de dados, é possível notar distinções relativas a características da personalidade do indivíduo, são os dados sensíveis, assim denominados porquanto permitem a identificação de individualidades mais significativas das pessoas.

Dessa forma, revela-se a importância não só de tutelar a proteção de dados pessoais, mas também de delimitá-los como sensíveis ou não, para que seja aplicado o princípio da isonomia no tratamento dos dados pessoais e, consequentemente, para que sejam evitadas práticas discriminatórias e abusivas que dele podem surgir.

3 PROTEÇÃO DE DADOS PESSOAIS

Conforme brevemente citado, a sociedade atual é a sociedade da informação. Bioni (2020) destaca o trajeto da sociedade, demonstrando que essa foi inicialmente agrícola, na época em que a riqueza era proveniente da terra. Em seguida, com a revolução industrial, adveio a sociedade industrial, na qual as máquinas e a produção fabril representavam riquezas. Na fase pós-industrial, a prestação de serviços passou a ser o motor do desenvolvimento socioeconômico. E atualmente, a informação é tida como o elemento central para o desenvolvimento da sociedade e da economia.

Com o avanço crescente das tecnologias, mais especificamente a partir da descoberta dos *bits*[3], ocorreu uma evolução de ordem quantitativa e qualitativa no processamento das informações. Quantitativa, pois com a desmaterialização da informação, foi possível um acúmulo inigualável de informações nas mais diversas plataformas (computadores, celulares, *pen drives* etc) e qualitativa, pois a partir da organização das informações, tornou-se mais fácil seu acesso e localização (BIONI, 2020).

Nesse sentido, a informação passou a ocupar um lugar de destaque na geração de riquezas e os dados pessoais tornaram-se um ativo para o desenvolvimento da economia. Em 2006, o matemático londrino especializado em ciência de dados, Clive Humby disse a frase "*data is the new oil*"[4], que foi popularizada internacionalmente e é altamente utilizada no mercado. O cientista explica que os dados por si só não são valiosos, eles precisam ser analisados para que tenham valor, da mesma forma que o petróleo precisa ser refinado. No entanto, diferentemente do petróleo, que é finito, os dados são inesgotáveis e estão à disposição o tempo todo, em volume e variedade. Como o acesso à dados é muito facilitado, seu valor subsiste na forma como são tratados e, se forem usados de forma analítica, possuem valor ainda maior, sendo capazes de transformar realidades e mercados (PALMER, 2006).

Alcalá (2005) salienta que a partir do arranjo das tecnologias tornou-se possível a coleta, registro, processamento, cruzamento e transmissão de informações de maneira intensa e ilimitada. E, através dessa dinâmica, em que a combinação de dados permite a obtenção de novos elementos informativos, viabilizou-se a obtenção de informações e dados pessoais privilegiadas sobre os indivíduos, capazes de conduzir tomadas de decisões políticas, econômicas e sociais, tanto de órgãos públicos como de entidades privadas.

---

[3] *Bit* é a sigla de *binary digit* (dígito binário), é a menor unidade de informação que pode ser armazenada ou transmitida. (MANZANO, 2007).

[4] Tradução: dados são o novo petróleo.

Com os avanços das tecnologias, teve-se a impressão de que a privacidade foi sendo cada vez mais suprimida. No entanto, a tecnologia deve ser utilizada a favor da sociedade e, por isso, é de extrema relevância a criação de soluções jurídicas e econômicas para enfrentar os “problemas” oriundos na era da sociedade informacional. Nesse contexto, o direito à privacidade se transfaz na proteção de dados pessoais, mantendo a tutela da personalidade, buscando dar ao indivíduo autonomia sobre as suas próprias escolhas e garantindo a dignidade da pessoa humana (MENDES, 2014).

Como bem sinaliza Paesani (2014), o Direito não pode ficar alheio à revolução tecnológica. É fato que as evoluções tecnológicas são mais rápidas do que a atividade legislativa ou regulamentar, razão pela qual deve ser dada maior prevalência aos princípios do que às regras positivadas. Assim, é possível equacionar os avanços tecnológicos com a imprescindibilidade de alcançar controle sobre o volume de dados que circulam pelo mundo, fazendo com que o direito fundamental da privacidade seja preservado.

Destarte, como as informações e dados pessoais são intermediários entre as pessoas e a sociedade, tem-se que caso não sejam feitos seu bom uso e tratamento, a personalidade de um indivíduo pode ser violada. Daí a necessidade de se tutelar juridicamente os dados de uma pessoa, para que seja assegurada sua liberdade (DONEDA, 2020).

3.1 A proteção de dados pessoais no ordenamento jurídico brasileiro

A interpretação mais comum é de que o direito à proteção de dados pessoais está abarcado pelo direito à privacidade, sendo o direito à proteção de dados pessoais uma subespécie derivada do direito à privacidade, que, irrefutavelmente, é tutelado constitucionalmente (DONEDA, 2020). A seguir serão expostas as técnicas legislativas do ordenamento jurídico brasileiro que tratam da privacidade e da proteção de dados pessoais, de modo que seja possível identificar que, por mais que a proteção de dados pessoais seja decorrente da privacidade, estes são conceitos e direitos diferentes.

Na Constituição Brasileira de 1988, o direito à privacidade está tutelado no artigo 5º de diferentes formas. O inciso X prevê a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando o direito à indenização por danos morais ou materiais que forem decorrentes de sua violação. Essa previsão segue a trilha das orientações internacionais, que inserem o direito à privacidade nos textos constitucionais (BRASIL, 1988).

Os incisos XI e XII também asseguram a privacidade, já que preveem a inviolabilidade do domicílio e do sigilo das comunicações telegráficas e telefônicas, garantindo que os dados e informações daí decorrentes estejam sob o controle de seu titular. O inciso LXXII, que institui a ação constitucional *habeas data*, também é uma forma de tutelar a proteção de dados pessoais, pois estabelece o direito de acesso e retificação das informações pessoais (BRASIL, 1988).

Bittar (2015) aponta que até mesmo na esfera penal existe proteção à vida privada, tendo em vista que são tipificadas condutas que violem a intimidade e a privacidade da pessoa humana. No Código Penal de 1940 são considerados crimes a violação de domicílio (art. 150), a violação de correspondência (art. 151), a violação de correspondência comercial (art. 152), a divulgação de segredo e violação de sigilo profissional (artigos 153 e 154), bem como a invasão de dispositivos informáticos (art. 154-A). Salienta-se ainda a Lei nº 9.296 de 1996, sobre a interceptação de comunicações telefônicas, que regula o inciso XII do art. 5º da CR/88, anteriormente mencionado.

Na esfera privada, o Código de Defesa do Consumidor, de 11 de setembro de 1990, foi pioneiro na legislação brasileira ao abordar a privacidade e a proteção de dados pessoais em adequação as tecnologias de processamento de dados (MENDES, 2014).

O artigo 43 do CDC regulamenta os bancos de dados e cadastros de consumidores:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá **acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.**
> § 1° Os cadastros e dados de consumidores devem ser **objetivos, claros, verdadeiros e em linguagem de fácil compreensão**, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° **A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor**, quando não solicitada por ele.
> § 3° O **consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção**, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades **de caráter público.**
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> § 6º **Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis**, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (grifos nossos).

Pela leitura do dispositivo, observa-se que o legislador teve o cuidado de proteger as informações pessoais dos consumidores presentes em bancos de dados. É resguardado ao consumidor o direito de acessar todas as informações relativas a ele, bem como de onde vêm

as informações. De acordo com o artigo, deve-se observar o princípio da qualidade de dados, tendo em vista que os dados dos consumidores devem ser objetivos, verdadeiros e de fácil compreensão. A obrigatoriedade de comunicação ao consumidor sobre a abertura de ficha cadastral e registros de dados pessoais denota a aplicação do princípio da transparência. Além disso, o dispositivo garante o direito de retificação e cancelamento de dados cadastrais e sugere o direito ao esquecimento, ao passo que impõe limite temporal para o armazenamento de dados pessoais (MENDES, 2014).

O Código de Defesa do Consumidor foi um marco no ordenamento civil brasileiro, tendo em vista que criou regras protetivas ao consumidor, na medida em que interpôs limites ao uso das informações das pessoas armazenadas em banco de dados de fornecedores. Evidencia-se no Código de Defesa do Consumidor o direito à proteção de dados pessoais. Porém, apesar da possibilidade de interpretação extensiva a outros contextos, deve-se observar que a tutela é limitada, considerando que a aplicação desta legislação é voltada especificamente para as relações consumeristas (DONEDA, 2020).

Outro aspecto relevante do dispositivo supracitado é a caracterização de bancos de dados e cadastros relativos a consumidores como públicos. De acordo com Mendes (2014), como os dados armazenados são relativos à personalidade do consumidor, eles não dizem respeito somente aos fornecedores, mas ao público e, por isso, se submetem ao regime constitucional e legal, podendo-se utilizar inclusive da ação de *habeas data* em face de bancos de dados de consumo.

Nesse sentido, é válido assinalar o *habeas data*, haja vista que é um remédio constitucional previsto no artigo 5º, inciso LXXII da Constituição Federal de 1988, que permite ao indivíduo ter acesso às suas informações armazenadas em banco de dados, além de possibilitar a retificação das informações quando houver necessidade. Destaca-se ainda a Lei nº 9.507, de 12 de novembro de 1997, que regulamenta o rito processual do *habeas data*. Doneda (2020) aponta a relevante função desse instituto no exercício democrático do cidadão, bem como no direito à proteção de dados pessoais.

Antes mesmo da legitimação trazida pelo Código de Defesa do Consumidor de que os bancos de dados possuem caráter público e, por isso, podem ser objeto de *habeas data,* alguns doutrinadores já defendiam sua aplicação para os arquivos de consumo, dentre eles Stürmer (1992, p. 82 *apud* BLUM, 2018), que elucida:

> O *habeas data* é ação mandamental, sumária, especial, destinada à proteção de pessoas frente a bancos de dados de qualquer natureza, público ou privado, com o caráter público, com o fim de permitir o conhecimento do que há de registro sobre

> sua pessoa e de retificá-los, complementá-los ou suprimi-los se inexatos ou inverídicos.

Doneda (2020) destaca que o *habeas data* não simboliza mudança substancial no direito à privacidade propriamente dito, mas que serviu para alertar a sociedade sobre a proteção de dados pessoais no país, direito que vinha sendo negligenciado. O autor, contudo, realça que o *habeas data* possui muitas limitações e é bastante criticado pela doutrina, principalmente em razão de sua estruturação processual, com requisitos formais que dificultam sua efetividade, que acaba sendo ofuscada pela sua função simbólica.

De acordo com Dallari (2002, p. 252), no Brasil o *habeas data* "não se destina a assegurar, genericamente, o direito à informação ou o direito à intimidade", mas possui a finalidade específica de "garantir que uma pessoa tenha acesso aos dados que, a seu respeito, constem de bancos de dados que sejam públicos ou de natureza pública". Assim, a realidade complexa que abarca a proteção de dados pessoais é negligenciada, pois é tratada de forma mínima, demonstrando que o *habeas data* não possui a eficácia que deveria ter por ser uma garantia constitucional.

O Código Civil de 2002 endossa a proteção à privacidade no artigo 21, pois coloca a vida privada da pessoa natural como inviolável e intangível. Tal previsão demonstra a proteção da privacidade para além da violação dos direitos à imagem e à honra da pessoa (FARIAS, 2015).

Consoante Mendes (2014), apesar de ser apenas um artigo do Código Civil voltado para o tema, ressalta-se sua importância, pois ocorre a concretização da tutela à privacidade no âmbito das relações privadas. Além disso, como o artigo está inserido no capítulo de direitos da personalidade, fica evidente a natureza jurídica do direito à privacidade, bem como sua relação intrínseca com a dignidade da pessoa humana e o desenvolvimento da personalidade.

Em 2011, surgem duas leis que tratam dos dados pessoais mais especificamente. A Lei do Cadastro Positivo, Lei nº 12.414, de 9 de junho de 2011, e a Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011. A Lei do Cadastro Positivo "disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito" (BRASIL, 2011).

Conforme explica Blum (2018), a referida lei visa organizar as informações oriundas do histórico de crédito das pessoas cadastradas, de modo a permitir que as pessoas caracterizadas como "boas pagadoras" sejam diferenciadas das que possuem histórico de inadimplência e, assim, possam ser bem avaliadas pelas entidades que concedem crédito,

sendo beneficiadas com melhores condições em novos empréstimos. Destaca-se que a lei protege não somente os dados do consumidor, mas de todos – pessoas naturais ou jurídicas – que tenham informações cadastradas em bancos de dados.

Segundo Mendes (2014), a principal característica da Lei do Cadastro Positivo foi a de ampliar o fluxo de dados no mercado, ao passo que permitiu a formação de bancos de dados com informações relacionadas ao adimplemento das pessoas e, paralelamente, cuidou de estabelecer regras de proteção à privacidade e aos dados das pessoas cadastradas. A autora acentua que a lei consolida o direito à autodeterminação informativa no ordenamento jurídico brasileiro, pois atribui ao titular de dados o poder de decidir sobre o destino de seus dados pessoais.

Seguindo a linha do que preceitua o artigo 43 do CDC, a Lei do Cadastro Positivo também aplica o princípio da qualidade dos dados, tendo em vista o artigo 3º, que em seu §1º dispõe que as informações armazenadas devem ser objetivas, claras, verdadeiras e de fácil compreensão, demonstrando a preocupação com a exatidão dos dados. No §2º do mesmo artigo, há vedação de anotações de informações excessivas e sensíveis, o que denota o alinhamento com os princípios da proporcionalidade e necessidade, que determinam que sejam coletados apenas os dados estritamente necessários, evitando a coleta de dados excessiva e desarrazoada (BLUM, 2018).

Identifica-se também a adoção do princípio da finalidade, já que nos termos do artigo 5º da Lei do Castro Positivo, os dados deverão ser utilizados somente conforme a razão pela qual foram coletados. Além disso, é assegurado aos cadastrados os direitos de acessar, retificar e cancelar seus dados. Percebe-se que este quadro normativo orienta as pessoas a assumirem controle sobre suas informações pessoais, pois permite ao titular dos dados pessoais o direito de gerenciá-los (BIONI, 2020).

Essa lei contribuiu, portanto, para que fossem preenchidas algumas lacunas na legislação brasileira no que tange ao direito à privacidade, possibilitando a aplicação de alguns conceitos em outros contextos de proteção de dados pessoais (BLUM, 2018).

A Lei de Acesso à Informação é decorrente do artigo 5º, inciso XXXIII da Constituição Federal de 1988, dispositivo que garante o direito a todos os cidadãos de receberem dos órgãos públicos informações de seu interesse particular, coletivo ou geral, observados os prazos legais e ressalvadas às exceções. A lei seguiu o contexto internacional de garantir mais transparência à Administração Pública através da concretização do direito fundamental de acesso à informação, acompanhando os exemplos de legislações de outros países (NAZARENO, 2020).

O artigo 31 da Lei nº 12.527 de 2011 demonstra claramente a preocupação do legislador em preservar a privacidade e proteger as informações pessoais: “o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais”.

Dessa forma, vê-se que a própria lei asseverou o cuidado com o tratamento das informações pessoais, o que manifesta a presença do direito de proteção de dados pesssoais, e a depender do contexto e da interpretação, pode significar um entrave ao exercício do acesso à informação.

Mendes (2014) aponta a relação ambivalente existente entre o direito de acesso à informação e a proteção de dados pessoais, que pode ser tanto de complementação como de limitação. Explica-se: ao reiterar o entendimento de que o indivíduo pode acessar as suas informações que se encontram sob a posse da Administração Pública, o direito à proteção de dados pessoais é consolidado. No entanto, esse mesmo direito pode ser reputado como uma contenção ao direito de acesso à informação, haja vista que impõe a regra de que terceiros não tenham acesso aos dados pessoais do titular, salvo quando o titular dos dados der seu consentimento.

A intenção principal da Lei de Acesso à Informação é garantir a transparência da Administração Pública para a população através da disponibilização de atos e dados públicos (BLUM, 2018). No entanto, como apontado, o direito à informação, fundamental para a construção e manutenção de um Estado Democrático de Direito, esbarra no direito à proteção dos dados pessoais. Dessa forma, a Administração Pública deve viabilizar o acesso à informação, mas deve também resguardar os dados pessoais dos indivíduos, para que sua privacidade e a personalidade não sejam violadas.

Nessa perspectiva, a Lei de Acesso à Informação trouxe o conceito de informação pessoal, no artigo 4º, inciso IV, como: “aquela relacionada à pessoa natural identificada ou identificável”, que é inclusive equivalente ao conceito de dado pessoal trazido pela Lei Geral de Proteção de Dados Pessoais. Além disso, o artigo 31 supramencionado estabeleceu limites para o acesso às informações pessoais, que só pode ocorrer por terceiros: *(i)* quando houver consentimento do titular; *(ii)* nas hipóteses previstas legalmente que dispensam o consentimento; e *(iii)* após 100 (cem) anos da data que foram produzidas. Ao impor critérios específicos para que os dados não sejam concedidos a terceiros sem o consentimento do titular, a lei demarcou as divisas entre o direito à informação e o direito à privacidade, de modo que ambos os preceitos constitucionais sejam respeitados (MENDES, 2014).

Em continuidade à linha cronológica da legislação sobre proteção de dados pessoais, é forçoso enfatizar a Lei nº 12.965, de 23 de abril de 2014, popularmente conhecida como o Marco Civil da Internet, responsável por estabelecer os princípios, garantias, direitos e deveres para o uso da internet no Brasil.

O Marco Civil da Internet visa regular as relações firmadas no meio ambiente digital de pessoas que estão interligadas por um sistema de comunicação estruturado em escala mundial, de uso público e irrestrito, que permite a troca de dados de forma eficaz e rápida. Assim, a lei busca assegurar que os direitos e deveres fundamentais da pessoa humana garantidos constitucionalmente sejam aplicados para os internautas no uso da internet, tendo em vista que o usuário da internet é necessariamente uma pessoa humana digna de direitos (FIORILLO, 2015).

No artigo 3º da lei é determinado que o uso da internet no Brasil deve seguir a proteção da privacidade e dos dados pessoais, que são vistos como pilares da lei, ao lado da liberdade de expressão e da neutralidade da rede. Outro dispositivo que cuida da proteção de dados pessoais é o artigo 7º, que prevê a inviolabilidade da intimidade da vida privada do usuário de internet, assegura que os dados pessoais não serão fornecidos a terceiros sem consentimento do titular dos dados, determina a utilização dos dados apenas para o uso a que destina, impõe que as finalidades sejam justificadas, legais e específicas e, ainda, possibilita a exclusão definitiva dos dados pessoais, aludindo a ideia do direito ao esquecimento (BRASIL, 2014).

Outros artigos da lei também tratam diretamente da proteção de dados pessoais, os artigos 10 e 11 disciplinam como devem ser guardados e disponibilizados os registros de dados feitos na internet, garantindo que seja preservada a privacidade do titular dos dados. O artigo 16 limita a utilização dos dados pessoais, pois determina que seu uso deve respeitar os limites do consentimento (BRASIL, 2014).

Consoante pontua Bioni (2020), da leitura do Marco Civil da internet é possível verificar a autodeterminação informacional como parâmetro para a proteção de dados pessoais, na medida em que o usuário deve ser sempre cientificado sobre o fluxo de seus dados pessoais e passa a ter controle sobre ele através do consentimento, que conforme exposto na lei, deve ser livre, expresso e informado.

Diante do exposto, vê-se que a proteção de dados pessoais está presente em diversas leis. No entanto, a legislação citada não consegue abranger toda a esfera de proteção de dados pessoais necessária da sociedade, pois são tratados apenas campos específicos, como as relações consumeristas e as relações no âmbito digital, por exemplo. Existia no Brasil uma

carência por uma norma que versasse sobre um direito geral de proteção de dados pessoais propriamente dito, tendo em vista que esse direito era tratado de maneira difusa e não havia delimitação objetiva sobre os critérios adequados para manuseio e tratamento de dados pessoais alinhados a um padrão mínimo de segurança.

À vista dessa necessidade e tendo como inspiração principal o Regulamento Europeu de Proteção de Dados, também conhecido como GDPR (*General Data Protection Regulation*), no dia 14 de agosto de 2018, foi promulgada no Brasil a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, originária do PLC nº 53/2018. O intuito da lei é o de proteger os direitos fundamentais da privacidade, aplicando a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, de forma a garantir o livre desenvolvimento da personalidade (PINHEIRO, 2020).

3.2 Lei Geral de Proteção de Dados Pessoais (LGPD)

Como mencionado, a Lei Geral de Proteção de Dados Pessoais (LGPD) teve como inspiração o Regulamento Europeu de Proteção de Dados (GDPR). Destaca-se que o regulamento europeu foi mais do que somente uma inspiração, mas uma motivação para que fosse consolidada uma legislação sobre a proteção de dados pessoais de modo geral no Brasil. Segundo Sarlet (2020, p. 48), o GDPR foi o "primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados".

O GDPR foi aprovado em 27 de abril de 2016 e entrou em vigor dia 25 de maio de 2018, a partir daí passou a ser exigido dos países e empresas que se adequassem ao regime de proteção de dados pessoais para a manutenção de relações comerciais com os países da União Europeia, na busca de um equilíbrio nas relações oriundas de negócios digitais no mercado global. Dessa forma, a ausência de legislação específica de proteção de dados pessoais do nível da GDPR passou a ser um impasse para quem quisesse estabelecer negócios com os países da União Europeia (PINHEIRO, 2020).

Assim, visando se adequar às regras estabelecidas pelo GDPR e, principalmente, buscando suprir as lacunas das normas gerais sobre proteção de dados pessoais na legislação brasileira, a LPGD foi promulgada em 2018, com início da vigência em 18 de setembro de 2020. De acordo com Ferreira (2019), as principais expectativas sobre o novo regulamento jurídico são: a demarcação da legitimidade da coleta de dados pessoais e como se dará o tratamento dos dados; a especificação de quais são os direitos dos titulares de dados, principalmente no que tange ao consentimento e à privacidade; a determinação de critérios

que garantam a segurança e confidencialidade na coleta, tratamento e armazenamento dos dados; a definição de quais são as responsabilidades do agente responsável pela coleta, tratamento e armazenamento dos dados pessoais; e a criação de uma autoridade nacional de proteção de dados, para fiscalizar, controlar e proporcionar a execução dos mecanismos jurídicos de proteção de dados pessoais.

Conforme enuncia Bioni (2020), o debate sobre a criação de uma lei de proteção de dados pessoais existe no Brasil desde 2010. O autor ressalta que o consentimento é o vetor principal da lei e sempre esteve presente na discussão sobre proteção de dados pessoais. A lei coloca o indivíduo como o principal responsável pelo fluxo de suas informações pessoais a partir de seu consentimento, que "deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral e, em alguns casos, deve ser, ainda, específico" (BIONI, 2020, p. 127).

Sarlet (2020) argumenta no mesmo sentido, exaltando o valor do consentimento informado como principal elemento para a proteção da pessoa humana, especialmente no ambiente digital, haja vista seu fortalecimento como expressão livre, consciente e informada do sujeito de direito.

O principal desígnio da LGPD é garantir a tutela dos dados pessoais – presentes em meio digital ou não – de todas as pessoas humanas. Garcia (2020) salienta que a lei não tem como objeto os dados de pessoas jurídicas, mas apenas os dados que as organizações em geral, públicas ou privadas, possuem das pessoas. No 1º artigo da lei, é estabelecido de forma cristalina que seu objetivo é a proteção de direitos fundamentais da liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural através do tratamento adequado dos dados pessoais.

O artigo 2º do diploma legal disciplina os fundamentos sob os quais está pautada a proteção de dados pessoais, são eles: *(i)* o respeito à privacidade; *(ii)* a autodeterminação informativa; *(iii)* a liberdade de expressão, de informação, de comunicação e de opinião; *(iv)* a inviolabilidade da intimidade, da honra e da imagem; *(v)* o desenvolvimento econômico e tecnológico e a inovação; *(vi)* a livre iniciativa, a livre concorrência e a defesa do consumidor; e *(vii)* os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Observa-se que há fundamentos de natureza existencial, direcionados para o desenvolvimento da personalidade de cada indivíduo, e de natureza patrimonial, voltados para o desenvolvimento nacional nos âmbitos social e econômico. De acordo com Regis (2020) há

uma intenção de tornar diretamente proporcional a relação entre as pessoas e o mercado. É como explica:

> na medida em que a proteção dos dados seja eficiente, resguardando-se a personalidade e a privacidade em todos os seus matizes, o mercado também será protegido, com foco no desenvolvimento econômico e tecnológico, capaz de fomentar a livre-iniciativa e a livre concorrência, sem embaraços de qualquer espécie. (REGIS, 2020, p. 7-21).

Ressalta-se que os fundamentos previstos no referido artigo são elementos basilares da LGPD e, por isso, devem ser sempre observados e utilizados na interpretação dos demais dispositivos, bem como na aplicação da lei nos casos concretos.

A aplicação da lei é tratada no artigo 3º, que indica as três hipóteses em que o tratamento de dados pessoais deve observar as disposições legais: *(i)* quando ocorrer em território nacional; *(ii)* quando a atividade tiver como objetivo a oferta ou fornecimento de bens ou serviços ou os dados forem de indivíduos localizados em território nacional; e *(iii)* quando a coleta dos dados pessoais objeto de tratamento ocorrer em território nacional. Nota-se então que o alcance da LGPD é extraterritorial, já que não se relaciona à nacionalidade dos dados pessoais ou à residência do titular dos dados. O dever de conformidade extrapola as fronteiras do país (PINHEIRO, 2020).

As exceções de aplicação da lei encontram-se no artigo 4º. Não deverão seguir os preceitos legais o tratamento de dados realizado por pessoa natural para fins exclusivamente particulares e não econômicos; os que tiverem fins exclusivamente jornalísticos, artísticos e acadêmicos; e para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais (BRASIL, 2018).

A LGPD aduz a definição de diversos termos e conceitos relevantes quando se discute tratamento de dados pessoais, o que demonstra o intuito do legislador de evitar equívocos na interpretação da lei. Os conceitos de dados pessoais e dados pessoais sensíveis trazidos pela LGPD foram apresentados no capítulo anterior. Abaixo, expõe-se o conceito de tratamento constante no artigo 5º, inciso X, haja vista as repetidas vezes que fora expresso.

> tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Dentre o rol de conceitos expostos no artigo 5º, destacam-se os principais papéis na dinâmica de proteção de dados pessoais instituídos pela LGPD:

> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

É válido ressaltar que a LGPD possui caráter principiológico, sendo o artigo 6º responsável por elencar os princípios que devem ser atendidos nas atividades de tratamento de dados pessoais, alguns deles, inclusive, identificados também em outros diplomas legais que versam sobre a privacidade e a proteção de dados pessoais. Deve-se sublinhar que o rol do artigo 6º não é taxativo, tendo em vista que pela leitura do artigo 64 da LGPD, fica evidente a possibilidade de aplicação de outros princípios e direitos que estejam previstos em outros dispositivos relacionados à matéria ou em tratados internacionais (FLUMIGNAN, 2020).

O artigo 6º da LGPD prevê o princípio da boa-fé no *caput*, além dos dez princípios enumerados nos incisos, são eles:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Não obstante a permissão de que os princípios sejam complementados, deve-se compreender que os princípios supramencionados, por estarem listados na LGPD, devem obrigatoriamente ser observados por todos os envolvidos no tratamento de dados pessoais. Ressalta-se ainda que deve haver uma interpretação sistemática dos princípios para que seja alcançado o objetivo geral pretendido pela lei (FLUMIGNAN, 2020).

Conforme mencionado, o consentimento do titular dos dados é a linha mestra da proteção de dados pessoais, os princípios têm o condão de empoderar o titular dando-lhe o controle de suas informações para efetivar a sua autonomia da vontade (BIONI, 2020). No entanto, o artigo 7º da lei prevê outras nove hipóteses para a coleta e tratamento de dados, que dispensam a obtenção do consentimento do titular.

Como aponta Garcia (2020), o legítimo interesse do tratamento de dados também é base legal para o tratamento de dados pessoais. Isto é, caso alguma organização ou terceiro necessite de tratar dados pessoais para oferecer produtos ou serviços, ou para melhorar e inovar produtos e serviços, é possível fazê-lo sem necessidade de consentimento, com base nos fundamentos do desenvolvimento econômico e tecnológico, da inovação e da livre iniciativa, previstos no artigo 2º da LGPD.

O artigo 8º da LGPD caracteriza o consentimento para as situações em que for escolhido como base legal para o tratamento de dados pessoais. De acordo com a lei, o consentimento deve ser expresso e específico, de modo que cláusulas genéricas serão nulas. Além disso, a lei impõe ao controlador o ônus de demonstrar que o consentimento é legítimo e garante ao titular de dados o direito de revogar seu consentimento a qualquer momento (BRASIL, 2018).

No artigo 9º, é possível identificar os princípios da transparência e do livre acesso. O preceito legal assegura ao titular de dados o fácil acesso às suas informações, de forma clara e ostensiva. Assegura também que o titular será informado sobre a finalidade do tratamento, sua forma, duração e sobre quem está realizando o tratamento, bem como quais são suas responsabilidades (BRASIL, 2018).

O legítimo interesse do controlador como fundamento para o tratamento de dados pessoais é apontado no artigo 10. São elencadas duas hipóteses que possibilitam tal situação, quais sejam: *(i)* apoio e promoção de atividades do controlador; e *(ii)* proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais (BRASIL, 2018).

De acordo com Bioni (2020), por ser uma base legal bem subjetiva, deve ser feito um teste de proporcionalidade do legítimo interesse para sua aplicação no tratamento de dados pessoais, de modo que sejam balanceados os direitos de quem faz o tratamento de dados e do titular de dados. O teste segue quatro etapas. Na primeira, deve ser verificada a legitimidade do interesse legítimo, através da definição da finalidade e do real interesse do agente de tratamento de dados pessoais. Em seguida, deve-se limitar os dados pessoais a serem coletados, para que sejam reunidos apenas os dados estritamente necessários para atingir a finalidade específica – estabelecida na primeira fase. Dessa forma, a coleta e tratamento de dados será menos invasiva e terá menos impacto para o titular dos dados. Na terceira etapa, deve-se delinear como se dará o impacto na vida do titular de dados, para que o tratamento de dados pessoais não impeça ou dificulte o livre desenvolvimento de sua personalidade. Por fim, o agente de tratamento de dados deve observar o dever de transparência, para que o indivíduo tenha informações sobre o que está sendo feito e possa, inclusive, se opor às atividades de tratamento de dados que considerar avessas às suas legítimas expectativas e, também, ter conduta de mitigação de riscos do titular de dados.

Um dos requisitos de validade trazidos pela LGPD é o limite de tratamento de dados pessoais, relativamente não só à quantidade de informações a serem coletadas, mas também quanto à finitude temporal do procedimento de tratamento de dados. Isto é, o tratamento de dados pessoais não pode ser indeterminado, deve ter um término, que deve ocorrer conforme as disposições dos artigos 15 e 16 da LGPD (PINHEIRO, 2020).

O artigo 15 enumera as hipóteses em que o tratamento de dados pessoais será encerrado e o artigo 16 impõe ao agente de tratamento de dados que apague os dados pessoais após o término de seu tratamento, autorizando algumas exceções. Segundo aponta Pinheiro (2020), como a preservação da informação possui alto valor, é provável que antes que os dados sejam excluídos, as organizações estudem se há alguma justificativa legal que permita a retenção dos dados pessoais.

Como já exposto anteriormente, os direitos dos titulares de dados estão assentes nos direitos fundamentais de liberdade, intimidade e privacidade. Assim, a LGPD ratifica esses direitos em seu capítulo III – artigos 17 a 23 – em que prevê direitos para viabilizarem os direitos fundamentais a partir do tratamento de dados pessoais. Dentre eles, destacam-se: o direito a uma gestão rigorosa dos dados pessoais; o direito a receber uma declaração que contenha a discriminação de seus dados pessoais e seus tratamentos; o direito de revogar seu consentimento, bem como de correção, anonimização, bloqueio ou exclusão daquilo que não concordar ou que não estiver em conformidade; a portabilidade de seus dados a terceiro;

direito de ser informado sobre eventuais compartilhamentos de informações; a vedação de utilização dos dados pessoais em prejuízo do titular (GARCIA, 2020).

O capítulo IV é dedicado ao tratamento de dados pessoais pelo poder público. Possivelmente o poder público é um dos entes que detém a maior quantidade de informações pessoais no país, o que denota a importância de a Administração Pública agir em conformidade com a LGPD. Pela leitura dos princípios que regem a LGPD e dos artigos do capítulo, é possível perceber semelhança com alguns princípios que norteiam a Administração Pública, o que demonstra que a LGPD reitera deveres que já são impostos ao poder público (AMARAL, 2020).

O artigo 23 esclarece que o tratamento de dados pessoais pelo poder público deve atender à sua finalidade pública, de modo que o interesse público seja priorizado, com a devida observância e cumprimento das atribuições legais, e respeitadas a necessidade e adequação do tratamento de dados pessoais. Assim como na iniciativa privada, o poder público deve garantir não só o acesso ao titular de dados, mas também clareza em relação ao objetivo e forma do tratamento de dados pessoais. Sobre os prazos e procedimentos para exercícios dos direitos do titular perante o poder público, o §3º deixa claro que deverão ser observadas as leis específicas, Lei do Habeas Data, Lei Geral do Processo Administrativo e Lei de Acesso à Informação (BRASIL, 2018).

Outro artigo desse capítulo que deve ser destacado é o 25, que prevê a manutenção de dados pessoais em "formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral". Como bem assinala Amaral (2020), este dever vai ao encontro do princípio da eficiência que rege a Administração Pública, ao passo que contribui com a eficiência na execução das políticas públicas e com a segurança no tratamento de dados pessoais. Além disso, a descentralização da atividade pública e o amplo acesso à informação pela população em geral, garantem maior e melhor exercício de cidadania.

A LGPD permite o compartilhamento de dados pessoais. O artigo 26 explicita que só será possível o compartilhamento caso sejam observadas as finalidades específicas para execução das políticas públicas e expõe algumas exceções, no entanto, mesmo os casos excepcionais devem observar os princípios da proteção de dados pessoais. De acordo com a lei, a Autoridade Nacional de Proteção de Dados (ANPD) – que será mais bem abordada em momento oportuno – deve ser comunicada sobre os instrumentos firmados com entidades privadas que autorizem o compartilhamento de dados pessoais pelo poder público. Os demais

artigos desse capítulo dizem sobre a faculdade concedida à ANPD de solicitar informações, disciplinar os assuntos relativos ao tratamento e compartilhamento de dados pessoais por parte do poder público, além de apontar sua responsabilidade pela fiscalização do tratamento de dados pelo poder público, de modo a evitar eventuais abusos e/ou desvios (BRASIL, 2018).

O capítulo seguinte da LGPD aborda a transferência internacional de dados pessoais. Seguindo a lógica do GDPR, a lei brasileira determina que a transferência de dados só poderá ocorrer para países ou organizações que possuam parâmetros de proteção de dados pessoais no mesmo nível da LGPD. Conforme explica Pinheiro (2020), o Brasil segue a padronização internacional do fluxo de dados pessoais e a proteção dessas informações, de modo a assegurar a continuidade do desenvolvimento econômico e tecnológico sem relativizar ou violar direitos fundamentais.

Ressalta-se que não basta que a legislação de proteção de dados pessoais do país de destino esteja em consonância com a LGPD, os direitos do titular de dados também devem ser respeitados e estar previstos nas cláusulas contratuais, sejam elas específicas ou padronizadas. Inclusive as normas corporativas, certificados e códigos de conduta devem estar em conformidade com os preceitos legais e os princípios de proteção de dados pessoais (GARCIA, 2020).

A LGPD, no artigo 33, prevê outras hipóteses em que a transferência internacional de dados pessoais pode ocorrer: quando o controlador comprovar cumprimento e garantia aos direitos do titular; quando for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução; quando for necessária para a proteção da vida ou da incolumidade física; quando a ANPD autorizar; para a execução de política pública ou atribuição legal de serviço público; com o consentimento do titular de dados, sendo destacados a transferência e o caráter internacional da operação; para cumprimento de obrigação legal ou regulatória pelo controlador; quando for necessário para execução de contrato ou procedimentos preliminares; e para exercício regular de direitos em processos judicial, administrativo ou arbitral (BRASIL, 2018).

O capítulo VI da LGPD refere-se aos agentes de tratamento de dados pessoais, quais sejam, o controlador, o operador e o encarregado. São expostas quais são suas funções e responsabilidades. Os conceitos são expressos na lei e foram apresentados em trecho anterior neste capítulo, sendo o controlador a pessoa que decide sobre o tratamento de dados pessoais, o operador aquele que realiza o tratamento de dados conforme orientações do controlador, e o encarregado é a pessoa responsável por fazer a interface da comunicação entre os agentes de

tratamentos de dados, os titulares de dados e a ANPD. Tanto o controlador quanto o operador devem manter registros das operações de tratamento de dados pessoais que realizarem e a lei estabelece que eles possuem responsabilidade solidária em caso de descumprimento das normas legais, cabendo direito de regresso entre eles. Ambos devem seguir os padrões de tratamento de dados a serem fixados pela ANPD (BRASIL, 2018).

O encarregado deverá ser indicado pelo controlador e as suas funções dispostas na lei são a princípio mínimas, como aceitar reclamações e comunicações dos titulares e da ANPD, orientar os contratados sobre as práticas de proteção de dados pessoais, entre outras atividades demandadas pelo controlador. No entanto, ressalva-se que a ANPD pode definir e ampliar atribuições complementares ao encarregado. Pinheiro (2020) destaca que o encarregado pode ser qualquer tipo de pessoa, física ou jurídica, contratada ou terceirizada e que as atividades endereçadas ao encarregado são multidisciplinares, pois demandam conhecimento técnico, jurídico e sobre atendimento e relacionamento.

O capítulo VII da LGPD dedica-se a segurança e boas práticas no tratamento de dados pessoais. Dispõe o *caput* do artigo 46:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

O nível de segurança exigido pelo dispositivo, acima transcrito, não exime as organizações de atenderem às exigências da ANPD sobre os padrões mínimos de tratamento de dados pessoais, sendo inclusive responsabilidade do agente a comunicação à ANPD e ao titular de dados, em prazo razoável, sobre a ocorrência de algum incidente de segurança que possa causar dano relevante ou representar algum risco ao titular. A comunicação deve ser completa, haja vista o dever de observância aos princípios da boa-fé, transparência e responsabilização. Conforme ordena o artigo 48, a comunicação deve mencionar a descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, os riscos relacionados ao incidente, as medidas técnicas e de segurança adotadas no tratamento e também as que tiverem sido tomadas a fim de reverter ou mitigar os efeitos do prejuízo e, quando a comunicação não for imediata, devem ser expostos os motivos da demora. A ANPD deve verificar e analisar a gravidade do incidente, e caso seja necessário, irá determinar ao controlador a adoção de providências (BRASIL, 2018).

O artigo 50 da LGPD diz respeito às regras de boas práticas e de governança que deverão ser formuladas pelos controladores e operadores, individualmente ou por meio de

associações, para o tratamento de dados pessoais. Estas regras devem estabelecer condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

Como explica Filho (2020), a governança de dados pessoais objetiva a consolidação de uma relação de confiança entre os agentes de tratamento de dados e os titulares, através de uma atuação transparente e participativa. A governança de dados pessoais deve estar integrada com a governança das organizações e deve ser continuamente monitorada, atualizada e submetida a avaliações periódicas, para que seja capaz de cumprir as boas práticas de proteção de dados pessoais estabelecidas pela ANPD, que, por sua vez, deve estimular a adoção de padrões técnicos que contribuam para que os titulares tenham controle sobre os seus dados.

O capítulo VIII da LGPD aborda a fiscalização e prevê as sanções administrativas a serem aplicadas pela ANPD. A aplicação das sanções administrativas segue uma escala gradativa: *(i)* advertência; *(ii)* multa simples; *(iii)* multa diária; *(iv)* publicização da infração; *(v)* bloqueio dos dados; *(vi)* eliminação dos dados; *(vii)* suspensão parcial do funcionamento do banco de dados; *(viii)* suspensão do exercício da atividade de tratamento dos dados pessoais; *(ix)* proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. As sanções podem ser aplicadas isolada ou cumulativamente, sem obrigatoriedade de seguir a ordem gradativa (BRASIL, 2018).

Nos termos do §1º do artigo 52, “as sanções somente serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto” (BRASIL, 2018). Serão considerados parâmetros e critérios do caso concreto para a aplicação das sanções, como a boa-fé, cooperação, e condição econômica do infrator, a reincidência, a adoção de políticas de boas práticas e governança, a gravidade da infração e o grau do dano e entre outros. Além disso, serão observados os princípios constitucionais da proporcionalidade e razoabilidade para a aplicação das sanções administrativas, de modo a impedir ou ao menos evitar abusos do poder estatal no exercício de suas funções, bem como para não prejudicar a existência de pequenas empresas e projetos de inovação (PINHEIRO, 2020).

O capítulo IX dispõe sobre a Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Vale ressaltar que a

ANPD inicialmente foi vetada, sendo incluída após a promulgação da Lei nº 13.853, de 8 de julho de 2019, que criou a ANPD e inseriu os artigos 55-A a 55-L e 58-A e 58-B na LGPD.

Segundo afirma Pinheiro (2020), a ANPD foi criada para garantir mais segurança e aplicabilidade da LGPD. Como visto, muitos dispositivos da lei carecem de regulamentação da ANPD, que irá determinar as diretrizes de adequação à LGPD no país, o que demonstra sua responsabilidade de estruturar o sistema jurídico de proteção de dados pessoais no Brasil. Além disso, a ANPD será responsável por fiscalizar e aplicar sanções administrativas.

Sobre a natureza jurídica da ANPD, o diploma legal expõe que é um órgão da Administração Pública federal, integrante da Presidência da República. No entanto, essa é transitória, após dois anos e mediante proposta do Poder Executivo, poderá ser transformada em autarquia, o que pode ser considerado positivo, por proporcionar mais autonomia à ANPD (BRASIL, 2018).

O artigo 55-J determina as competências da ANPD, dentre elas, Pinheiro (2020) destaca: zelo pela proteção de dados pessoais, em consonância com a legislação; elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalização e aplicação de sanções nos casos de tratamento de dados pessoais que estiverem em desconformidade com a lei, assegurados o contraditório e a ampla defesa em âmbito administrativo; apreciação de pedidos dos titulares mediante reclamações ao controlador que não tiverem sido solucionadas no prazo legal; disseminação das normas e políticas públicas sobre proteção de dados pessoais e medidas de segurança para conhecimento da população; solicitação ao poder público de informes detalhados sobre o tratamento de dados; realização de autorias sobre tratamento de dados pessoais realizados por agentes de tratamento; edição de normas e procedimentos simplificados e diferenciados para microempresas e empresas de pequeno porte; garantia de que o tratamento de dados pessoais de idosos ocorra de forma simples, clara, acessível e adequada à compreensão.

É possível dizer que a instituição da ANPD é fundamental para a aplicação da LGPD. Nas palavras de Pinheiro (2020, p. 56), “um regulamento com previsão de sanções sem órgão fiscalizador não tem efetividade nem garantia de funcionamento”.

3.2.1 Aplicação da LGPD

Inicialmente, a LGPD possuía o prazo de *vacatio legis* de dois anos, para que as organizações em geral pudessem se preparar para a adequação à lei e às mudanças dela decorrentes. Assim, a lei entraria em vigor em agosto de 2020. Em razão do contexto

pandêmico do corrente ano, ocorreram diversas tramitações legislativas no Senado Federal que geraram enorme insegurança jurídica sobre o início de sua vigência. Contudo, em 18/09/2020 a LGPD entrou oficialmente em vigor[5], mas em decorrência da alteração trazida pela Lei nº 14.010 de 2020, as sanções administrativas serão aplicadas somente a partir de 01/08/2021.

Apesar do adiamento da aplicação das sanções administrativas, com a vigência da lei, torna-se possível que os titulares de dados e o Ministério Público recorram ao judiciário visando o resguardo dos direitos relativos à proteção de dados pessoais, com fundamento legal da nova legislação. Com efeito, a LGPD tem um potencial de transformar não só o sistema jurídico brasileiro, mas a cultura da população em geral, incluindo as pessoas naturais, instituições públicas e da iniciativa privada. Volta-se a atenção para os procedimentos de coleta e tratamento de dados pessoais, para que estejam em conformidade com a lei e de modo que todos passem a se preocupar ainda mais com a privacidade, com a segurança e a proteção de dados pessoais.

Certo é que a implementação dessa complexa legislação traz grandes desafios para todos os setores socioeconômicos do Brasil. Como visto, a premissa básica da LGPD é regulamentar e dispor de normas para o tratamento de dados pessoais, objetivando a proteção da privacidade, intimidade e liberdade dos cidadãos. Para que esse processo seja aplicado com efetividade, será necessário um conjunto de medidas, pautadas na transparência e amparado com mecanismos de controle (RODRIGUES, VIEIRA, 2020).

Ressalta-se que a LGPD não possui o condão de criar uma cultura proibitiva e limitadora sobre o tratamento de dados pessoais. Afinal, reconhece-se que a sociedade atual vive em uma realidade interconectada, baseada em um alto fluxo de dados, em que há necessidade de produção, coleta e tratamento de dados pessoais a todo o momento. Busca-se apenas a proteção de dados pessoais, a partir de uma gestão clara e transparente, embasada na segurança da informação, de modo que seja garantida a autodeterminação informativa ao titular de dados e que ele tenha resguardado os direitos fundamentais de privacidade, intimidade e liberdade. Dessa forma, o crescente desenvolvimento da tecnologia deve ser ensejo na busca de soluções para os desafios impostos pela nova cultura de proteção de dados pessoais, de modo que as tecnologias se tornem instrumentos facilitadores para a aplicação da LGPD.

[5] https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor

4 SEGURANÇA DA INFORMAÇÃO E MECANISMOS DE CONTROLE DE DADOS PESSOAIS

Como supradito, a sociedade atual é a sociedade da informação, tendo em vista que a informação é um ativo de valor e significa poder, capaz de garantir vantagens competitivas para organizações privadas, de orientar decisões e políticas públicas, e até mesmo de manipular os cidadãos. Jimene (2020, p. 40) explica que como a sociedade está vastamente conectada à internet, as informações tornam-se cada vez mais expostas, já que todos têm acesso a elas sem precedentes. Essa exposição indevida das informações deixa os indivíduos vulneráveis e pode ocasionar prejuízos diversos, como ataques cibernéticos, fraudes digitais, vazamento de informações, concorrência desleal e entre outros, o que pode "acarretar desde perda de competitividade de uma empresa em determinado mercado até a violação da privacidade de um ser humano".

Consoante afirma Bioni (2020), as informações pessoais são a matéria prima da economia e do mercado na sociedade informacional. As informações são fluidas e isso torna o fluxo informacional complexo, deixando os titulares em condição de vulnerabilidade para exercer controle sobre seus dados pessoais. O autor expõe estudos empíricos que concluem pela hiper vulnerabilidade do titular em meio ao mercado informacional, em decorrência principalmente de uma assimetria informacional que dificulta o efetivo controle das informações pessoais por seus titulares.

Assim, sendo a informação um ativo de valor e o titular sujeito vulnerável na sociedade informacional, nota-se a pertinência da segurança da informação. Segundo Jimene (2020), a segurança da informação já existia anteriormente à necessidade de proteção de dados pessoais. Porém, era focada para proteção de informações sigilosas e estratégicas relevantes para os negócios. Atualmente, com a vigência da LGPD e perante a necessidade de proteção de dados pessoais como forma de tutelar a privacidade e os direitos da personalidade, deve-se aplicar a segurança da informação também no tocante aos dados pessoais. Isto é, as organizações possuem a obrigação de adotar medidas de segurança sobre os dados pessoais que custodiam para protegê-los.

De acordo com a norma NBR ISO/IEC 27002:2013 da Associação Brasileira de Normas Técnicas (ABNT), alcança-se a segurança da informação a partir da implementação de um "conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware".*

Machado (2014, p. 23) expõe o conceito de segurança da informação de forma bem simples e didática: “a segurança da informação é uma maneira de proteger os sistemas de informação e a sociedade contra diversos ataques, mantendo documentos e arquivos dentro dos princípios de confidencialidade, integridade e disponibilidade”.

Como visto no capítulo anterior, a segurança é um dos princípios que norteia as atividades de tratamento de dados pessoais. Logo, a segurança da informação deve ser aplicada em todas as organizações que tratam os dados pessoais, de modo a permitir a conformidade com a legislação. De acordo com Jimene (2020), devem ser utilizadas medidas técnicas e administrativas que possibilitem a proteção de dados pessoais de acessos não autorizados e de circunstâncias acidentais ou ilícitas de destruição, perda, alteração, compartilhamento ou divulgação.

Bioni (2020) expõe dois conceitos imprescindíveis que auxiliam na equalização da assimetria informacional que torna o cidadão vulnerável. A expressão *Privacy by Design*, que sugere que a proteção de dados pessoais deve nortear a criação de produtos e serviços que facilitem o controle e a proteção de dados pessoais, e as PETs (*Privacy Enhancing Tecnologies*), compreendidas como tecnologias de facilitação da privacidade, incluídos todos os tipos possíveis de tecnologias que possam reforçar e/ou melhorar a privacidade. Dessa forma, a tecnologia é tida como ferramenta para a proteção de dados pessoais, ao passo que empodera e emancipa o cidadão a assumir, de fato, o controle sobre os seus dados pessoais e efetiva sua autodeterminação informativa.

Vê-se então, que a adequação à LGPD passa obrigatoriamente por procedimentos relacionados à tecnologia da informação, tendo em vista o alto volume de dados armazenados em sistemas informatizados, que devem ser tratados com medidas e técnicas de segurança. A utilização de recursos tecnológicos que possibilitem a segurança da informação no ambiente digital é necessária para que sejam cumpridas as obrigações legais de tratamento de dados pessoais e seja garantida a privacidade dos titulares. São alguns exemplos de mecanismos tecnológicos que contribuem para a segurança da informação e, consequentemente, para a proteção de dados: ferramentas de autenticação de acesso, recursos de criptografia, assinatura digital e certificação digital (JIMENE, 2020).

Bioni (2020) salienta que deve ser estabelecida uma relação de interdependência entre a almejada autodeterminação informativa e a tecnologia, de modo que esta seja instrumento de operacionalização daquela e dê ao cidadão a capacidade genuína de gerenciamento de seus dados pessoais.

4.1 Assinatura digital e certificação digital

A assinatura digital e a certificação digital são mecanismos de proteção de dados pessoais, vez que visam identificar quem é o usuário por trás das informações encontradas no ambiente virtual. Pinheiro (2016) explica que para entender os conceitos de assinatura e certificação digital, é necessário antes compreender o que é a criptografia.

Seguem alguns conceitos de criptografia:

> é um método de transformar os dados originais, chamados de texto simples ou de texto puro, em algo aparentemente aleatório e ilegível, conhecido por texto cifrado. Ela é um dos principais mecanismos de segurança utilizado na proteção contra os riscos associados ao princípio da confidencialidade. (MACHADO, 2014, p. 145).

> é uma ciência que tem importância fundamental para a segurança da informação, ao servir de base para diversas tecnologias e protocolos. [...] Suas propriedades – sigilo, integridade, autenticação e não repúdio – garantem o armazenamento, as comunicações e as transações seguras. (NAKAMURA; GEUS, 2007, p. 287).

A criptografia é um mecanismo de codificação utilizado para o envio de mensagens no ambiente eletrônico de forma segura. O sistema criptográfico transforma a informação em algo ilegível, sendo que nenhum ser humano ou máquina consegue compreendê-la, assim, só é conhecida por pessoa autorizada, quando é descriptografada. Há dois tipos de processos de codificação, a depender da chave criptográfica utilizada: simétrica (de chave privada) ou assimétrica (de chave pública) (MACHADO, 2014).

Na criptografia simétrica, o destinatário da mensagem deve conhecer o algoritmo utilizado para criptografar a mensagem para que consiga decifrá-la. A chave deve ser compartilhada com o destinatário final da mensagem, o que compromete a confidencialidade da informação, pois há possibilidade de interceptação (NOGUEIRA, 2008).

Na criptografia assimétrica ou de chave pública, são utilizados dois tipos de chave, uma para codificar e outra para decodificar a informação. Esse sistema é composto por duas chaves diferentes, uma pública e uma privada, sendo que uma mensagem codificada por uma chave pública só será decodificada por sua chave privada correspondente, e vice-versa (MACHADO, 2014).

O sistema de criptografia assimétrica possibilita a utilização de assinatura e certificação digital. Nakamura e Geus (2007, p. 291) explicam como ocorre o processo da assinatura digital:

> A assinatura digital pode ser obtida com o uso de algoritmos de chave pública, no qual o usuário que deseja assinar digitalmente uma mensagem utiliza sua chave privada. Como somente ele possui acesso à chave privada e como somente a chave pública

> correspondente pode fazer com que a mensagem volte ao seu estado original, utilizar a chave privada significa que o usuário assina digitalmente uma mensagem. O processo [...] é feito também com o uso de um algoritmo de *hash*[6], que é um resumo da mensagem. O algoritmo de assinatura digital é aplicado sobre o resumo gerado, com o usuário usando sua chave privada. O resultado, a assinatura digital, é adicionado à mensagem original, que é enviada ao destinatário. É importante notar que o uso da assinatura digital não garante o sigilo da mensagem, somente prova a origem de determinada mensagem, pois somente o dono da chave privada pode assinar a mensagem.

A assinatura digital permite a comprovação de que a informação é autêntica e de que foi, de fato, gerada por seu dono, já que apenas ele conhece a chave privada que codificou a informação. Como foi codificada por uma chave privada, a verificação da assinatura digital é decodificada por uma chave pública correspondente. Conforme ensina Machado (2014), a assinatura digital é um valor *hash* criptografado.

Pinheiro (2016) destaca que a assinatura digital, por ser verificada em tempo real no sistema de duas chaves criptográficas, é mais segura do que a assinatura tradicional. Afinal, as assinaturas tradicionais nem sempre são verificadas, e quando o são, a verificação não ocorre imediatamente. A assinatura digital permite o reconhecimento de sua origem, identifica o usuário e garante autenticidade e integridade.

Convém ressaltar que a assinatura digital é espécie do gênero assinatura eletrônica. São conceitos distintos, sendo o conceito de assinatura eletrônica mais amplo, que envolve todos os recursos de identificação no meio eletrônico, tais como: senhas, códigos de acesso, assinaturas manuscritas digitalizadas, assinaturas digitais, entre outros (NOGUEIRA, 2008).

O certificado digital, por sua vez, materializa o uso da assinatura digital, ao passo que é utilizado para averiguar se a chave pública que codificou a assinatura é, de fato, de determinado usuário. Existe uma Autoridade de Certificação (*Certificate Authority* - CA), que garante que o certificado com determinada chave pública pertence ao usuário. Assim, quando a comunicação se inicia, é enviado o certificado, não a chave pública (MORAES, 2010).

Moraes (2010, p. 92), ensina o processo de criação do certificado digital:

> O usuário cria as chaves pública e privada randomicamente. A chave pública é então enviada para a CA, que cria o certificado com as informações pertinentes e assina-o com a chave privada da CA. O certificado é enviado de volta para o usuário já assinado. Por segurança, todo certificado leva data de validade.

Pelas palavras de Machado (2014, p. 156), o certificado digital "é um documento eletrônico que contém dados sobre a pessoa ou entidade que o utiliza para comprovação

[6] De acordo com Machado (2014, p. 154), "O *hash* é gerado de tal forma que não é possível realizar o processamento inverso para se obter a informação original. Além disso, qualquer alteração na informação original produzirá um *hash* distinto. Apesar de ser teoricamente possível que informações diferentes gerem *hashes* iguais, a probabilidade de isto ocorrer é significativamente baixa".

mútua de autenticidade". Com ele, o usuário pode utilizar sua assinatura de documentos, sendo-lhe garantidos a autenticação, sigilo e integridade da informação.

Não se pretende aqui aprofundar sobre as tecnologias acima expostas ou mencionar todos os tipos disponíveis, tendo em vista ser assunto técnico da área de informática, e não do direito. A breve explicação apresentada propôs-se a demonstrar como a tecnologia já tem atuado de forma colaborativa com a proteção de dados no ambiente digital, visando à garantia da autenticidade e integridade da informação, além da identificação do emissor das informações no meio virtual.

Ocorre que estes instrumentos são aplicados a nichos específicos e, ainda, de forma muito limitada, sendo que uma parcela mínima da população tem acesso e, quem o tem, utiliza em apenas algumas áreas. Com a vigência da LGPD e a imperatividade de tutelar os dados pessoais de forma geral, seria interessante pensar em uma tecnologia que permitisse o controle dos dados pessoais de forma mais generalizada em todos os âmbitos. À vista disso, será exposto a Identidade Digital baseada em *blockchain* como ferramenta de proteção de dados pessoais e será analisada a sua compatibilidade com a nova legislação.

4.2 Blockchain – conceito e aplicações

Em 2008, uma ou mais pessoas, sob o pseudônimo de Satoshi Nakamoto, desenvolveram um modelo de transações de valores em meio eletrônico. Esse modelo ficou conhecido como o protocolo *bitcoin*, um sistema que propõe a tecnologia ponto a ponto para a transação de criptomoedas (moedas digitais) sem que haja a intermediação de um terceiro confiável.

A tecnologia *blockchain* surgiu inicialmente como uma forma segura de registrar as transferências de *bitcoins*. Mas, ressalta-se que *bitcoin* e *blockchain* não são a mesma coisa, o *bitcoin* é apenas uma das várias possíveis aplicações que o *blockchain* pode viabilizar. O *blockchain* é uma tecnologia bem mais ampla, que permite a transação de qualquer ativo, seja tangível, intangível ou digital, com registro seguro (GUPTA, 2018).

De acordo com Don Tapscott e Alex Tapscott (2016), o *blockchain* é uma plataforma de registros distribuída, tendo em vista que não há uma base de dados central; é pública, haja vista a possibilidade de qualquer pessoa acessá-la a qualquer momento; e criptografada, pois são utilizadas chaves criptográficas públicas e privadas para manutenção da segurança virtual. Os autores conceituam *blockchain* como "um livro-razão distribuído que representa um consenso de cada operação que já ocorreu na rede" (TAPSCOTT; TAPSCOTT, 2016, p.37).

Alves *et al*. (2018) argumentam que o *blockchain* proporciona a proteção de dados de uma forma singular, ao passo que utiliza um controle de forma descentralizada que garante a segurança nas transações. Apresentam a seguinte definição de *blockchain*: "uma tecnologia que faz uso de uma arquitetura distribuída e descentralizada para registrar transações de maneira que um registro não possa ser alterado retroativamente, tornando este registro imutável". (ALVES *et. al*., 2018, p. 2).

O controle descentralizado se dá, pois as transações ocorrem em uma rede *peer-to-peer* (P2P) com participantes mutuamente não confiáveis. Nesse sistema, todos os participantes são iguais e são onerados para manutenção do funcionamento da rede (CHICHARINO *et al*., 2017). Marçula (2019), explica que na rede *peer-to-peer* (P2P) não há um servidor central que detém os dados, mas todos os participantes atuam como servidor em algum momento, se conectando em uma rede sobreposta.

Blockchain em sua tradução literal significa cadeia de blocos. Gupta (2018) explica que esse nome se dá pela forma como as transações são registradas, em blocos ligados uns aos outros, formando uma corrente. Conforme o número de dados aumenta, o *blockchain* também cresce. Cada bloco contém uma informação (*hash)* que é verificada à medida que é registrada à cadeia. O *hash* do bloco anterior tem sua informação ligada ao seguinte, de forma que se algum dos dados for alterado, todos os *hashes* dos blocos anteriores farão a verificação. Dessa forma, a cada novo *hash* adicionado à corrente, ocorre um fortalecimento da rede, atribuindo ao *blockchain* a característica de imutabilidade.

Chicharino *et al*. (2017, p. 15) explicam que o *blockchain* é "uma estrutura de dados que armazena transações de forma ordenada e ligada ao bloco anterior, servindo como um sistema de registros distribuído". De forma semelhante à explicação acima, expõem: "cada bloco possui uma identificação única gerada a partir de um resumo criptográfico de *hash"*. De acordo com os autores, o *blockchain* traz grande impacto para a sociedade, ao passo que altera o modo de fazer negócios, aplicando uma forma descentralizada entre agentes distribuídos e mutuamente não confiáveis, sendo dispensável a presença de uma entidade intermediária confiável.

Deve-se observar que a tecnologia *blockchain* pode e já vem sendo utilizada para criação de soluções inovadoras e disruptivas em diversas áreas. Este livro-razão digital de registros de transações consegue gravar praticamente tudo, como certidões de nascimento, óbito e casamento, diplomas de universidades e instituições de ensino, títulos de propriedades, votos, contas financeiras, procedimentos médicos e tudo o que tiver importância e valor para a sociedade (TAPSCOTT; TAPSCOTT, 2016).

Como brevemente citado, o *blockchain* surgiu no mercado financeiro e se tornou conhecido principalmente através da criptomoeda *bitcoin*. No entanto, ressalta-se que essa tecnologia possui inúmeras aplicações, que vão muito além do setor financeiro.

O Grupo de Estudos sobre Blockchain para aplicações de Interesse Público, conduzido pelo Instituto de Tecnologia e Sociedade do Rio (ITS Rio) elaborou um relatório[7] que expõe variadas formas de possibilidade de uso do *blockchain* voltados para o interesse público. Dentre elas está a identidade digital, objeto do presente estudo, que será abordada no próximo capítulo.

São destacadas pelo relatório outras potenciais aplicações da tecnologia, como o uso do *blockchain* no sistema notarial; aplicação do *blockchain* como forma de certificações, a partir da emissão e registros de certificados de cursos de universidades e demais instituições de ensino; aplicação do *blockchain* no rastreamento da cadeia de suprimentos nos mais diversos setores da economia, para garantir transparência sobre as etapas do processo de manufatura e auxiliar na fiscalização; pode ser utilizada para registro e proteção de propriedade intelectual, visando comprovar a autoria das criações e evitar práticas de plágio e fraude; o *blockchain* pode ser aplicada em auditorias, principalmente de instituições pública, mas também em instituições privadas; pode ser uma ferramenta que auxilie a garantir a transparência da Administração Pública, atuando também em combate à corrupção.

Ressalta-se que, além das aplicações apontadas pelo relatório, ainda há outros possíveis usos para o *blockchain*, como registros de provas, *smart contracts (*contratos inteligentes), economias compartilhadas, programas de fidelidade e compartilhamento de informações, governança corporativa das sociedades anônimas, registros de fornecimento de medicamento, entre outras variadas aplicações.

Destaca-se, por fim, que a tecnologia *blockchain* ainda é emergente, pois apesar de possuir grande potencial para criar conceitos e possibilidades e para transformar a economia e o mercado, ainda não está completamente consolidada e possivelmente irá enfrentar grandes desafios para a sua implementação.

[7]Disponível em: https://itsrio.org/wp-content/uploads/2019/03/Relat%C3%B3rio-ITS-GE-Blockchain-vFinal.pdf

5 IDENTIDADE DIGITAL BASEADA NA TECNOLOGIA BLOCKCHAIN

Uma das possíveis utilidades do *blockchain* é sua utilização como forma de gestão de identidade dos usuários. A identidade digital baseada em *blockchain* mostra-se uma ferramenta para tutelar os direitos da personalidade advindos do direito à privacidade e intimidade, uma vez que facilita o controle e autonomia dos titulares sobre os seus dados pessoais.

Como se sabe, são várias as informações que podem identificar um indivíduo, tais como nome, endereço, profissão, data de nascimento e CPF. Atualmente, na sociedade da informação, em que as pessoas vivem conectadas e realizam inúmeras transações em ambiente virtual, a todo o momento são criadas identidades, por meio de cadastros em lojas on-line, redes sociais, plataformas de *streaming*, processos seletivos, cursos on-line, sistemas operacionais, serviços de governo etc.

A cada interação realizada na internet, informações pessoais são disponibilizadas e, da forma como ocorre hoje, o titular não possui o devido controle sobre o que é feito com suas informações, sobre quem tem acesso a elas ou mesmo não tem conhecimento sobre o local de armazenamento dessas informações. Além disso, em razão do grande número de identidades que um mesmo indivíduo possui na internet, não é possível garantir que as informações fornecidas sempre serão verídicas e que determinada identidade é autêntica. Assim, muitos dados pessoais são roubados e violados, o que compromete a identidade das pessoas, caracterizando uma grande vulnerabilidade da identificação digital. Nesse cenário, surgem diversos problemas como a criação de perfis falsos que permitem, por exemplo, a prática de fraudes virtuais (BATISTA, 2018).

Diante dessa conjuntura, foram pensadas soluções para a identidade digital baseadas na tecnologia *blockchain*. O sistema distribuído do *blockchain* permite que os titulares tenham controle sobre a própria identidade e sobre seu compartilhamento, uma vez que nesse sistema os dados pessoais são compartilhados de forma consentida. Esse tipo de identidade digital foi denominado *self-sovereign identity* (identidade autossoberana) e já existem diferentes tipos em desenvolvimento, todos com base na rede descentralizada do *blockchain.* O sistema de verificação dos usuários que dispensa a necessidade de um servidor central e as "*verifiable credentials*" (credenciais criptograficamente determináveis e interoperáveis) das transações conferem maior confiabilidade e segurança à identidade autossoberana. A utilização do *blockchain* nas identidades digitais permite promoção da dignidade humana através da garantia do direito de autodeterminação informativa (WINDLEY, 2018).

Conforme Nakamura *et al.* (2019), a aplicação da tecnologia *blockchain* nas identidades digitais viabiliza a verificação, autorização e gerenciamento das informações pessoais de forma segura e confiável, garantindo a redução de fraudes de identidades. Os autores conceituam a *self-sovereign identity* (identidade autossoberana) como "uma identidade que pertence e é controlada por seu proprietário sem a necessidade de depender de qualquer autoridade administrativa externa e sem a possibilidade de que essa identidade possa ser removida" (NAKAMURA *et al*., 2019, p. 12).

Segundo Zhu e Badr (2018), as identidades digitais baseadas em *blockchain* geralmente são denominadas identidade autossoberana, o que remete a uma interpretação de que o direito de controle de acesso e gestão dos dados pessoais é apenas do titular, analogamente ao que ocorre com as identidades tradicionais, que conferem poder apenas ao dono da identidade.

De acordo com Jehl (2017), a utilização da identidade digital baseada na tecnologia *blockchain* permite que as pessoas controlem a própria identidade e limitem o acesso aos dados pessoais. A autora explica que a identidade digital deve ser personalíssima; permanente, no sentido de que o indivíduo terá a mesma identidade do início de sua vida até a morte; portátil, isso é, possível de acessar de qualquer lugar; e privada, de modo que apenas o titular pode permitir o acesso e uso dos dados nela constantes. A arquitetura descentralizada e distribuída do *blockchain*, em que os dados ficam espalhados em diversos dispositivos contribui para maior segurança contra ciberataques, violação e corrupção de dados.

Atualmente, é praticamente impossível enumerar exatamente quais as empresas e instituições públicas que armazenam dados pessoais da população e, mais difícil ainda, saber como ocorre o tratamento desses. Logo, as identidades dos indivíduos ficam extremamente expostas e vulneráveis, sendo infactível que se possa verificar a origem, por exemplo, de um vazamento de dados pessoais. A tecnologia *blockchain* aplicada às identidades digitais, em decorrência de sua característica de descentralização intrínseca, permite uma redução considerável na exposição e vulnerabilidade das identidades, haja vista que o ataque a uma rede descentralizada é mais complicado e improvável (ALVES *et al.*, 2018).

Consoante expõem Sullivan e Burguer (2019), a identidade digital baseada na tecnologia *blockchain* já está revolucionando o conceito de identidade digital. Por mais que existam identidades tradicionais como certidão de nascimento, passaportes e registros de identidade que são capazes de identificar uma pessoa, essas informações, concedidas em ambiente virtual, não conseguem comprovar que a pessoa que as disponibiliza é, de fato, a titular daquela identidade específica. A tecnologia *blockchain* aplicada à identidade digital

permite que a segurança, autenticidade e imutabilidade das informações registradas, haja vista que o *blockchain* é um "livro" de registros distribuído em vários dispositivos espalhados, que usa a criptografia para assegurar a segurança e confiabilidade das informações armazenadas.

Com a vigência da LGPD e a imprescindibilidade de garantir que os indivíduos tenham acesso, controle e autonomia sobre os seus dados pessoais, a aplicação da tecnologia *blockchain* nas identidades digitais pode ser uma ferramenta muito útil. Porém, deve-se avaliar se a aplicação do *blockchain* é compatível com as regras e princípios estabelecidos pela legislação de proteção de dados pessoais.

5.1 Caso de aplicação da Identidade Digital baseada na tecnologia *Blockchain*

A aplicação do *blockchain* nas identidades digitais não é novidade, grandes empresas como a IBM, Microsoft e Deloitte e governos de alguns países como Estônia e Índia, por exemplo, já investem e utilizam a identidade digital baseada na tecnologia *blockchain* (BATISTA, 2018). No Brasil, algumas instituições privadas de tecnologia e segurança da informação oferecem esse serviço e já existem discussões sobre a padronização da identidade digital autossoberana no país (NAKAMURA *et al.*, 2019).

Em 2018, a Estônia foi denominada pela Forbes como "*The world's most digital country*"[8]. Desde 2013, o governo da Estônia tem utilizado a tecnologia de livro distribuído aliada às funções *hash* criptografadas para garantir a segurança e a autenticidade de registros de identidade digital. O cartão de identidade estoniano baseado no *blockchain (Estonian Blockchain-Based ID Card)* unifica o acesso do titular a uma série de serviços, como realizar transações bancárias, votar, candidatar-se para recebimento de benefícios do governo, consultar histórico de instituições de ensino, são aproximadamente 3000 tipos de funções que são viabilizadas pelo *ID Card*. As empresas podem utilizar o *ID Card* para registrar os relatórios anuais, emitir documentos e solicitar licenças, por exemplo. O governo estoniano consegue criptografar documentos, revisar e aprovar autorizações, contratos e aplicações através do *ID Card* (THOMPSOM; YU, 2017).

De acordo os dados do governo estoniano[9], 99% dos residentes utilizam *ID Card*, sendo que 70% utilizam de forma regular e 99% dos serviços governamentais são *on-line*. Os únicos serviços que demandam presença física das pessoas são casamento, divórcio e compra

[8]Tradução: o país mais digital do mundo. Disponível em: https://www.forbes.com/sites/michellegreenwald/2018/08/16/business-lessons-from-the-worlds-most-digital-country-estonia-the-happiest-country-finland/#686b5cb01935

[9] Disponível em: https://e-estonia.com/

e venda de imóveis. Além de serem utilizados os *ID Cards* para identificação digital, a Estônia também oferece um modelo que utiliza dispositivos móveis (*Mobile ID*). Na Estônia, todas as pessoas podem assinar digitalmente através do *ID Card* e *Mobile ID* para se identificarem com segurança e para utilizar os serviços governamentais de maneira mais acessível e mais rápida.

Na Estônia, a utilização da identidade digital baseada na tecnologia *blockchain* e a construção de um governo digital foram responsáveis pela construção de um ecossistema digital seguro, eficiente e transparente, possibilitando a redução de burocracias e tornando as transações e acessos à serviços mais rápidos. Com a digitalização dos serviços, foram identificadas significativas melhorias no desenvolvimento da sociedade e da economia do país.

5.2 Viabilidade e efetividade da Identidade Digital *Blockchain*

A identidade digital baseada em *blockchain* trata dados pessoais e dados pessoais sensíveis, logo, para que seja utilizada no Brasil, deve atender às regras de tratamento de dados pessoais e os princípios estabelecidos pela LGPD. É certo que a utilização da identidade digital baseada em *blockchain* contribui consideravelmente no processo de adequação à LGPD, tendo em vista que garante aos titulares o controle de seus dados pessoais. Contudo, algumas previsões da lei podem significar desafios para as tecnologias que utilizam o *blockchain*.

A LGPD busca garantir que o titular tenha acesso aos seus dados pessoais, além de garantir ao titular o direito de corrigir e eliminar os seus dados, mediante requisição feita ao controlador, conforme disposição do artigo 18. Em uma identidade digital baseada na tecnologia *blockchain,* como o titular é o próprio responsável pela gestão e controle de seus dados pessoais, não há necessidade de participação do controlador, o que de certa forma, afasta a identidade digital *blockchain* do texto legal. No entanto, salienta-se que o acesso dos dados é concedido ao titular, inclusive de forma mais ampla.

Quanto à retificação dos dados prevista pela LGPD, pode-se afirmar que é aplicada a mesma lógica. Como na identidade digital baseada em *blockchain* o próprio titular dos dados faz a gestão da identidade, esse requisito também é atendido, haja vista que os dados pessoais propriamente ditos não são necessariamente registrados no livro-razão da rede *blockchain*. De acordo com Nakamura *et al.* (2019), os dados pessoais são inseridos através de identificadores

pseudônimos e descentralizados, o que permite o tratamento dos dados pessoais fora do livro-razão principal.

A questão que possivelmente pode causar mais discussão sobre a compatibilidade da identidade digital baseada em *blockchain* com a legislação de proteção de dados pessoais é a previsão de exclusão e eliminação dos dados, referida por alguns como o direito ao esquecimento, mesmo que a LGPD não faça essa menção expressa. Afinal, a característica de imutabilidade do *blockchain* sugere que depois de registrada na rede, a informação não poderá ser excluída.

Existem duas soluções para dirimir essa possível incompatibilidade. É plausível a inutilização da identidade digital baseada em *blockchain* através da exclusão da chave criptografada privada que dá acesso a ela, o que resultaria no extravio definitivo das informações que estavam registradas. A outra possibilidade reside no emprego das *off chains* e *side chains*. No caso das *off chains*, os dados pessoais são armazenados fora da rede principal, constando no livro-razão distribuído primário apenas informações que indiquem as transações relativas aos dados pessoais, conforme explicado anteriormente. As *side chains* são *blockchains* paralelos ao principal e independentes. Dessa forma, os dados pessoais são desvinculados das informações registradas no *blockchain* principal, que exerce função de indexadora do dado ou transação sem revelá-lo, assegurando a privacidade e segurança dos dados pessoais e viabilizando eventuais alterações e exclusões dos dados (BROTTO; RIBEIRO, 2019).

Assim, apesar de aparentemente existir uma incompatibilidade, há tecnologias que permitem a viabilização da conformidade da identidade digital baseada em *blockchain* com a LGPD, pois os parâmetros legais serão atendidos, mesmo que em tese.

Além dos aspectos legais, devem ser consideradas as questões fáticas para averiguar a viabilidade e efetividade da identidade digital baseada em *blockchain* no Brasil. Se comparado com a Estônia, que, como visto, é referência mundial em desenvolvimento tecnológico e digital, percebe-se que o cenário brasileiro é drasticamente diferente. O Brasil possui proporções continentais, sendo sua população e extensão territorial extremamente maior. Outras questões que também impactam a viabilidade da aplicação da identidade digital baseada em *blockchain* são a cultura da sociedade e o limitado acesso que a população possui à internet. Segundo a Pesquisa Nacional por Amostra de Domicílios Contínua 2017-2018[10], realizada pelo Instituto Brasileiro de Geografia e Estatística, aproximadamente 74,7% das

[10] Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101705_informativo.pdf

pessoas com 10 anos ou mais possuem acesso à internet, o que significa que mais de um quarto da população brasileira ainda não tem acesso à internet.

Apesar das dificuldades e adversidades, o Brasil já vem investindo em serviços digitais e tecnologias como *blockchain* já estão sendo utilizadas em instituições públicas e privadas no país. A "Original My"[11] é um exemplo, empresa fundada em 2015, que oferece soluções confiáveis baseadas em *blockchain* para promover mais acesso à justiça através da redução de burocracias e mais transparência nos serviços públicos, com ferramentas que garantem a confiabilidade e autenticidade de documentos, pessoas e arquivos digitais. Um dos serviços ofertados pela empresa é a "Identidade *Blockchain*", aplicável a pessoas físicas e jurídicas. A ferramenta permite o controle dos dados pessoais sem que o titular tenha que criar inúmeros cadastros e, para as empresas, garante a conformidade com a LGPD, posto que os dados que receber já terão sido validados pelo titular.

[11] Disponível em: https://originalmy.com/

6 CONSIDERAÇÕES FINAIS

Conforme discorrido ao longo deste trabalho, o direito à privacidade é um direito da personalidade que foi se ressignificando no decorrer do tempo. Com a constante evolução tecnológica, que contribui para maior disseminação de informações e maior exposição dos dados pessoais, a privacidade foi sendo cada vez mais invadida e fragilizada. Dessa forma, surgiu a necessidade de tutelar especificamente os dados pessoais, tendo em vista a exposição irrestrita em ambientes virtuais e disponíveis nos mais diversos bancos de dados, tanto de instituições públicas, quanto de instituições privadas.

Os dados pessoais passaram a ser considerados um ativo muito valioso para a economia, além de serem a própria representação do indivíduo na sociedade atual, a sociedade da informação. Assim, os dados pessoais devem ser tutelados para que se assegure o livre desenvolvimento da pessoa humana, sendo, inclusive, considerado por alguns estudiosos do tema como um direito autônomo da personalidade. Diante disso, com inspiração no Regulamento Europeu de Proteção de Dados (GDPR), foi promulgada em 2018, a Lei Geral de Proteção de Dados Pessoais no Brasil, com o objetivo de regulamentar o tratamento de dados pessoais e garantir ao titular de dados que tenha acesso e controle de seus dados pessoais.

Em paralelo à preocupação legislativa de conceder proteção aos dados pessoais para garantir o livre desenvolvimento da personalidade, constantemente surgem inovações tecnológicas que impactam diretamente com as leis e a proteção de dados pessoais em si, dentre elas o *blockchain.* Tecnologia que ficou famosa no mercado financeiro, pelas criptomoedas, mas possui inúmeras aplicações.

Como explicado, o *blockchain* é uma espécie de livro-razão distribuído que, através da criptografia, registra informações em uma rede descentralizada, sem necessidade de um intermediário ou uma autoridade central, de modo que todos os envolvidos tenham acesso às informações registradas e possam realizar transações com segurança, com garantia de integridade e autenticidade das informações. Os dados são adicionados e validados em forma de blocos, que são compostos por um conjunto de informações que geram um código *hash*, esse, por sua vez, é único e imutável e associa-se à corrente de blocos.

Conforme Tapscott e Tapscott (2016), essa tecnologia surgiu para revolucionar a maneira como as informações são registradas, armazenadas e como ocorrem as transações, haja vista a segurança, confiabilidade, velocidade e redução de custos que o *blockchain* pode proporcionar. Dentre as possíveis aplicações do *blockchain*, existe a identidade digital

baseada nesta tecnologia, que pode mitigar os danos causados pela diversidade de identidades digitais que uma pessoa possui atualmente, que dificulta sua gestão e deixa os indivíduos vulneráveis a ciberataques, furto e violação de dados pessoais.

A identidade digital baseada na tecnologia *blockchain* possibilita que os registros de identidade digital sejam imutáveis, além de garantir que a vinculação de identidade a transações ou outros dados seja feita apenas após autorização explícita do usuário, o que garante o controle e autonomia sobre os dados pessoais. Através dessa tecnologia, o titular tem seus registros validados de maneira adequada, o que proporciona maior confiabilidade dos dados, tanto no sentido de serem autênticos, impedindo que os dados pessoais sejam violados ou corrompidos por terceiros, quanto no sentido de garantir segurança nas transações realizadas, de forma mais célere e inviolável (BATISTA, 2018).

Assim, a identidade digital baseada na tecnologia *blockchain* pode ser uma ferramenta para tutelar os direitos da personalidade advindos do direito à privacidade e intimidade e, principalmente, para garantir o direito à proteção de dados pessoais, uma vez que facilita o controle e autonomia do usuário sobre os seus dados pessoais.

Deve-se ressaltar, no entanto, que quando as normas legais de proteção de dados pessoais começaram a ser pensadas – tanto o GDPR quanto a LGPD –, a tecnologia *blockchain* ainda estava surgindo e tinha aplicação mais voltada para as criptomoedas, então as leis não foram pensadas em consonância com a tecnologia *blockchain* e suas possíveis aplicações. Por conseguinte, alguns aspectos do *blockchain* são compreendidos como impactos, levando-se a crer que existe uma incompatibilidade com a LGPD.

Pôde-se concluir com este trabalho que há sim aspectos a serem considerados, mas que a tecnologia *blockchain* pode ser adaptada para que haja conformidade com as leis de proteção de dados pessoais. A tecnologia *blockchain* ainda é emergente e pode ser adequada para solucionar os desafios da identidade digital e para conferir ao titular controle e autonomia sobre os seus dados pessoais, sendo instrumento útil para viabilizar a LGPD na prática.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013**. Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

ALCALÁ, Humberno Nogueira. **Autodeterminacíon informatia y habeas data em Chile e información comparativa.** Anuário de Derecho Constitucional Latinoamericano. Chile, 2005. Disponível em: https://revistas-colaboracion.juridicas.unam.mx/index.php/anuario-derecho-constitucional/article/download/30267/27321. Acesso em: 20 set. 2020.

ALVES, Pedro Henrique. *et al*. Desmistificando Blockchain: Conceitos e Aplicações. *In*: MACIEL, Cristiano; VITERBO, José (Orgs). **"Computação e Sociedade"**, Sociedade Brasileira de Computação. 2018. Disponível em: http://www-di.inf.puc-rio.br/~kalinowski//publications/AlvesLNRLK20.pdf. Acesso em: 20 set. 2020.

AMARAL, Luiz Fernando de Camargo Prudente. Desafios da LGPD em relação à implementação pelo poder público. *In*: BLUM Renato Opice (Org) **Proteção de dados**: desafios e soluções na adequação à lei. – Rio de Janeiro: Forense, 2020.

BATISTA, Alex Oliveira Abreu. **Identificação digital baseada em blockchain**: um conceito disruptivo no ciberespaço. Goiânia: Media Lab / UFG, 2018.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2ª edição – Rio de Janeiro: Forense, 2020.

BITTAR, Carlos Alberto. **Os direitos da personalidade** 8. ed. São Paulo: Saraiva, 2015.

BLUM, Rita Peixoto Ferreira. **O Direito à privacidade e à proteção dos dados do consumidor**. 2ª edição. São Paulo: Almedina, 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 set. 2020.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 14 set. 2020.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Brasília, 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14 set. 2020.

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

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 set. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 set. 2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 14 set. 2020.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Brasília, 1997. Disponível em: http://www.planalto.gov.br/CCIVIL_03/LEIS/L9507.htm. Acesso em: 14 set. 2020.

BROTTO, Natália; RIBEIRO, Aleff. **A LGPD e a tecnologia blockchain são compatíveis?** Jota: 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-lgpd-e-a-tecnologia-blockchain-sao-compativeis-05112019. Acesso em: 16 set. 2020.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje:** perspectiva histórica e o cenário brasileiro. Florianópolis: Revista Sequência, v. 38, n. 76, p. 213-240, 2017. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213/34870. Acesso em: 14 set. 2020.

CASTRO, Catarina. Sarmento. **Direito da informática, privacidade e dados pessoais.** Coimbra: Almedina, 2005.

CHICHARINO, Vanessa R. *et al*. Uso de blockchain para privacidade e segurança em internet das coisas. VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília. **Anais**. SBC, 2017.

DALLARI, Dalmo de Abreu. O *habeas data* no sistema jurídico brasileiro. *In*: **Revista Da Faculdade De Direito**, Universidade De São Paulo, 97, 239-253. São Paulo, 2002. Disponível em: http://www.revistas.usp.br/rfdusp/article/download/67544/70154/. Acesso em: 14 set. 2020.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais:** elemento da formação da Lei Geral de Proteção de Dados. 2ª edição, São Paulo, 2020.

FARIAS, Cristiano Chaves de. **Curso de direito civil:** parte geral e LINDB 13. ed. São Paulo: Atlas, 2015.

FERREIRA, Rafael Freire. **Autodeterminação informativa e a privacidade na sociedade da informação.** 3ª edição, Rio de Janeiro: Lumen Juris, 2019.

FILHO, Adalberto Simão. A Governança Corporativa aplicada às boas práticas e *compliance* na segurança de dados. *In*: PEREIRA, Cíntia Rosa (Coord.). **Comentários à lei geral de proteção de dados:** Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019.São Paulo: Almadina, 2020.

FIORILLO, Celso Antonio Pacheco. **O Marco Civil da Internet e o meio ambiente digital na sociedade da informação:** comentários à Lei nº 12.965/2014. São Paulo: Saraiva, 2015.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wéverton Gabriel Gomes. Princípios que regem o tratamento de dados no Brasil. *In*: PEREIRA, Cíntia Rosa (Coord.). **Comentários à lei geral de proteção de dados:** Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almadina, 2020.

GARCIA, Lara Rocha. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: guia de implantação. São Paulo: Blucher, 2020.

GUPTA, Manav. **Blockchain For Dummies®, 2nd IBM Limited Edition**. United States of America: John Wiley & Sons, Inc., 2018.

JEHL, Laura E. Blockchain – **The future of digital identity?** Bloomberg Law, 2017. Disponível em: https://bakerlaw.com/webfiles/Privacy/2017/Articles/12-13-2017-Jehl-BNA-Blockchain.pdf. Acesso em: 3 ago. 2020.

JIMENE, Camilla do Vale. Da importância da segurança da informação para adequação à LGPD. *In*: BLUM, Renato Opice (Org.). **Proteção de dados:** desafios e soluções na adequação à lei.Rio de Janeiro: Forense, 2020.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação**: princípios e controle de ameaças. 1ª edição. São Paulo: Érica, 2014.

MANZANO, André Luiz N. G. **Estudo dirigido de informática básica**. São Paulo: Érica, 2007.

MARÇULA, Marcelo. **Informática:** conceitos e aplicações. 5ª edição. São Paulo: Érica, 2019.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MORAES, Alexandre Fernandes. **Segurança em Redes** - Fundamentos. 1ª edição – São Pualo: Editora Saraiva, 2010.

NAKAMOTO, Satoshi. Bitcoin: **A peer-to-peer electronic cash system**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 3 ago. 2020.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec, 2007.

NAKAMURA, Emilio Tissato; MARINO, Fernando Cezar Herédia; FILHO, José Reynaldo Formigoni; RIBEIRO, Sérgio Luís; OLIVEIRA, Vítor Padilha de. Identidade Digital Descentralizada: Conceitos, aplicações, iniciativas, plataforma de desenvolvimento e implementação de caso de uso. XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. **Anais.** Campinas, 2019. Disponível em: https://www.ic.unicamp.br/~bit/mo809/seminarios/07-out/Identidade%20Digital%20Descentralizada.pdf. Acesso em: 3 ago. 2020.

NAVARRO, Ana Maria Neves de Paiva. **Privacidade Informacional**: origem e Fundamentos no Direito Norte-Americano. Rio de Janeiro, 2011. Disponível em: http://www.publicadireito.com.br/artigos/?cod=34f9a343f945196b. Acesso em: 3 ago. 2020.

NAZARENO, Claudio; PINHEIRO, Guilherme Pereira. **Legislação sobre acesso à informação, proteção de dados pessoais e internet [recurso eletrônico]**, 1. Ed. Câmara dos Deputados, Edições Câmara, Brasília: 2020.

NOGUEIRA, Roberto Henrique Porto. **Documento eletrônico.** Teoria geral dos contratos e os títulos de crédito virtuais. Belo Horizonte: RHJ, 2008.

OLIVEIRA, Rafael Santos de. O direito à privacidade na internet: desafios para a proteção da vida privada e o direito ao esquecimento. *In:* **Rev. Fac. Direito UFMG**, Belo Horizonte, n. 70, pp. 561 - 594, jan./jun. 2017. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/download/1863/1765. Acesso em: 8 ago. 2020.

ONU. **The Universal Declaration of Human Rights**. Paris, 1948. Disponível em: https://www.un.org/en/universal-declaration-human-rights/. Acesso em: 8 ago. 2020.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil.7. ed. São Paulo: Atlas, 2014.

PALMER, Michael. **Data is the new oil**. CMO News, Reinventing Marketing, Technology's Impact, The Customer. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html. Acesso em: 8 ago. 2020.

PINHEIRO, Patrícia Peck. **Direito digital.**6ª ed. São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais** - comentários à Lei n. 13.709/2018 LGPD. 2ª edição. São Paulo: Saraiva Educação: 2020. Disponível em: https://www.mccarthy.ca/en/insights/blogs/snipits/estonian-blockchain-based-id-card-security-flaw-raises-issues-about-identity. Acesso em: 8 ago. 2020.

REGIS, Erick da Silva. Linhas gerais sobre a Lei 13.709/2018 (LGPD): objetivos, fundamentos e axiologia da Lei Geral de Proteção de Dados brasileira e a tutela de personalidade/privacidade. **Revista de Direito Privado.** vol. 103/2020 – p. 63 – 100. Jan – Fev/2020.

RODOTÁ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Paula Marques; VIEIRA, Alessandra Borelli. Educação como um dos pilares para a conformidade. *In*: PEREIRA, Cíntia Rosa (Org.). **Comentários à lei geral de proteção de dados:** Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almadina, 2020.

SANTOS, Cifuentes. **Elementos de derecho civil**. Parte general. 4ª edición. Buenos Aires: Astrea, 1999.

SARLET, Gabrielle Bezerra Sales. Notas sobre a proteção dos dados pessoais na sociedade informacional na perspectiva do atual sistema normativo brasileiro. *In*: PEREIRA, Cíntia Rosa (Org.). **Comentários à lei geral de proteção de dados:** Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almadina, 2020.

SULLIVAN, Clare; BURGUER, Eric. Blockchain, Digital Identity, E-government. *In:* **Business Transformation through Blockchain.** Vol. II. Alemanha: Palgrave Macmillan, 2019. Disponível em: https://doi.org/10.1007/978-3-319-99058-3. Acesso em: 26 ago. 2020.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution:** como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: SENAI-SEP Editora, 2016.

THOMPSOM, Kirsten; YU, Eric. **Estonian Blockchain-Based ID Card Security Flaw Raises Issues About Identity.** CyberLex, 2017.

UNIÃO EUROPEIA. **Parlamento Europeu e do Conselho**. Directiva 95/46/CE, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML. Acesso em: 26 ago. 2020.

VIANNA, Túlio. **Transparência pública, opacidade privada:** o direito como instrumento de limitação do poder na sociedade de controle. Tese de doutorado - Universidade Federal do Paraná, Setor de Ciências Jurídicas, Programa de Pós-graduação em Direito. Defesa: Curitiba, 2006. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/5281/VIANNA%2c%20T%c3%balio%20Lima%20-%20Tese%20doutorado%20em%20Direito%20UFPR.pdf?sequence=1&isAllowed=y. Acesso em: 26 ago. 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, vol. 4, n. 5, p. 193-220, 1890. Disponível em: http://links.jstor.org/sici?s.ici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C. Acesso em: 26 ago. 2020.

WINDLEY, Phillip. **How blockchain makes self-sovereing identities possible.** Computer World, 2018. Disponível em: https://www.computerworld.com/article/3244128/how-blockchain-makes-self-sovereign-identities-possible.html. Acesso em: 26 ago. 2020.

ZHU, Xiaoyang; BADR, Youakim. **Identity Management Systems for the Internet of Things:** A Survey Towards Blockchain Solutions. MDPI, 2018. Disponível em: https://www.mdpi.com/1424-8220/18/12/4215. Acesso em: 16 ago. 2020.