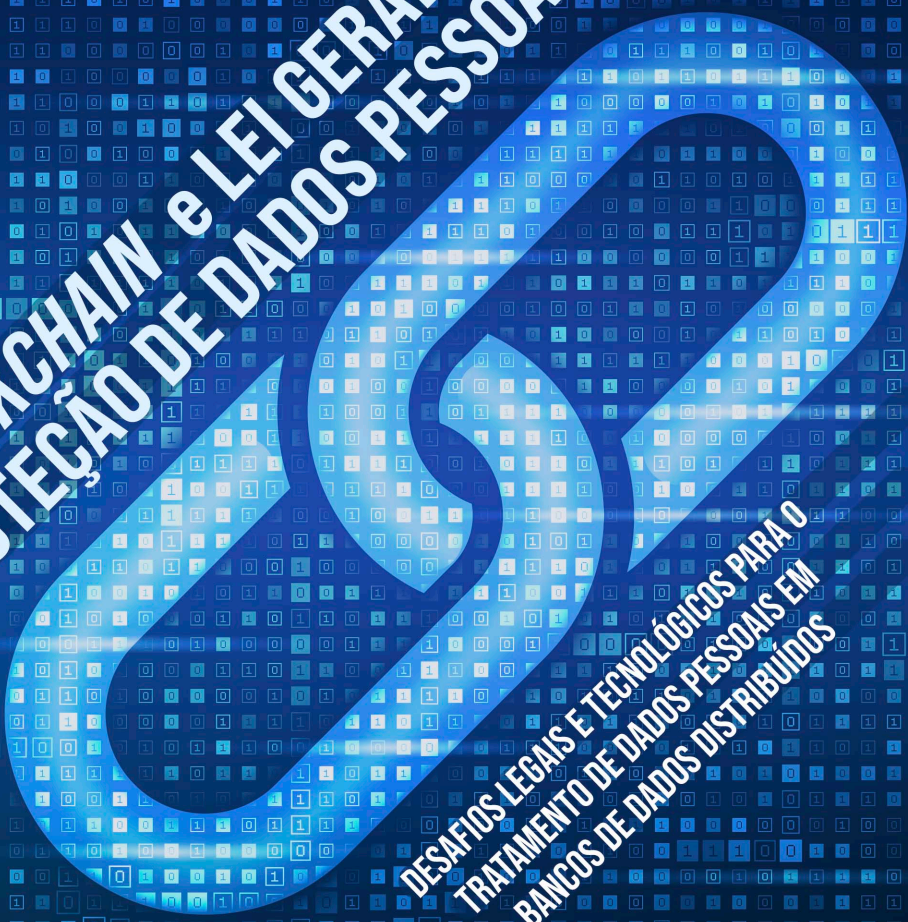
FERNANDO BOTTEGA PERTILE

BLOCKCHAIN e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS



DESAFIOS LEGAIS E TECNOLÓGICOS PARA O TRATAMENTO DE DADOS PESSOAIS EM BANCOS DE DADOS DISTRIBUÍDOS

Blockchains e a LGPD possuem pelo menos dois objetivos em comum: segurança e transparência na utilização de dados. Contudo, como blockchains são uma tecnologia recente, é possível que sua utilização não tenha sido abordada na nova Lei Geral de Proteção de Dados Pessoais. Diante desse cenário, a presente pesquisa constituiu-se de um estudo sobre a Lei nº 13.709, de 14 de agosto de 2018, a partir de previsões também presentes no Regulamento Geral sobre Proteção de Dados europeu, do ponto de vista das tecnologias descentralizadas de armazenamento de dados, especificamente baseadas em blockchain, a fim de verificar se a legislação brasileira se encontra preparada para tais inovações ou alterações técnicas e legislativas precisam ser realizadas.

9 786559 171934

editora fi.org

Blockchain e Lei Geral de Proteção de Dados Pessoais

Blockchain e Lei Geral de Proteção de Dados Pessoais

Desafios legais e tecnológicos para o tratamento de dados pessoais em bancos de dados distribuídos

Fernando Bottega Pertile

Diagramação: Marcelo A. S. Alves
Capa: Carole Kümmecke - https://www.conceptualeditora.com/

O padrão ortográfico e o sistema de citações e referências bibliográficas são prerrogativas de cada autor. Da mesma forma, o conteúdo de cada capítulo é de inteira e exclusiva responsabilidade de seu respectivo autor.

Dados Internacionais de Catalogação na Publicação (CIP)

PERTILE, Fernando Bottega

Blockchain e Lei Geral de Proteção de Dados Pessoais: Desafios legais e tecnológicos para o tratamento de dados pessoais em bancos de dados distribuídos [recurso eletrônico] / Fernando Bottega Pertile -- Porto Alegre, RS: Editora Fi, 2021.

87 p.

ISBN - 978-65-5917-193-4
DOI - 10.22350/9786559171934

Disponível em: http://www.editorafi.org

1. Blockchain; 2. Lei Geral de Proteção de Dados Pessoais; I. Título.

CDD: 340

Índices para catálogo sistemático:
1. Direito 340

Sumário

Introdução

Blockchain pode ser definida como uma tecnologia de banco de dados descentralizada, cujos dados ficam armazenados de forma distribuída e criptografada, não dependendo de um gestor central. O nome, "corrente de blocos", em tradução livre, decorre da forma como as informações são registradas em blocos criptografados sequenciais. Por não depender de um controlador, todos os participantes da rede podem auditar as transações. Os registros em uma *blockchain* não podem, em tese, ser alterados ou excluídos, gerando certeza e confiabilidade aos utilizadores.

Esse último aspecto, especificamente, tido como um dos principais pontos positivos da *blockchain*, por garantir segurança às transações e negócios realizados, pode enfrentar dificuldades frente à legislação em vigor, especialmente a Lei Geral de Proteção de Dados Pessoais. Isso porque referida lei busca *regular* o mundo centralizado de dados, exigindo maior responsabilidade e transparência, bem como estabelecendo responsáveis legais para alterar ou remover dados pessoais. A *blockchain*, por outro lado, visa *desafiá-lo*, trazendo segurança e transparência aos próprios bancos de dados, criando uma categoria "imutável" e compartilhada baseada em criptografia. Em determinados tipos de *blockchain* é impossível determinar uma pessoa como responsável pela gestão dos dados, que ficam armazenados de forma distribuída.

Diante desse cenário, a presente pesquisa constituiu-se de um estudo sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), a partir de previsões também presentes no Regulamento Geral de Proteção de Dados europeu, do ponto de vista das tecnologias descentralizadas de armazenamento de dados, especificamente baseadas

em *blockchain*, a fim de verificar se a legislação brasileira se encontra preparada para tais inovações ou alterações técnicas e legislativas precisam ser realizadas. Isso porque, ao regular as entidades centralizadoras que dominam o mercado de dados atualmente, há a possibilidade de a legislação ter desconsiderado a existência de alternativas *descentralizadas*.

Nesse contexto, buscou-se verificar se a Lei Geral de Proteção de Dados Pessoais permite que tecnologias baseadas em *blockchain* para armazenar dados pessoais operem de acordo com ela. Para tanto, fez-se uso de três hipóteses. A primeira, é que a Lei Geral de Proteção de Dados brasileira se encontra preparada para permitir o correto funcionamento de tecnologias descentralizadas de armazenamento de dados. A segunda, que há total incompatibilidade, caso em que novas soluções técnicas ou jurídicas precisarão ser tomadas. A terceira, que há parcial recepção, e já existem tecnologias que conseguem agir com total *compliance*.

Para analisar as hipóteses, explorou-se, no primeiro capítulo, o aspecto histórico internacional das legislações que visam proteger, inicialmente, a privacidade, e, posteriormente, dados pessoais. Em seguida, examinou-se os fundamentos, princípios e objetivos gerais das leis brasileira e europeia de proteção de dados pessoais, bem como as exigências que as legislações impõem àqueles que armazenam dados pessoais.

No segundo capítulo, buscou-se a origem e detalhamentos técnicos do funcionamento de uma *blockchain*, bem como suas divisões e aplicações práticas. Por fim, analisou-se o grau de adaptabilidade da tecnologia às exigências legais, a fim de verificar se a Lei Geral de Proteção de Dados previu possibilidade de *compliance* para o armazenamento de dados em registros distribuídos em bloco.

A realização desta pesquisa contou com embasamento jurídico e doutrinário, tendo em vista que foram analisadas legislações e proposições teóricas e práticas existentes sobre os tipos de *blockchain*, visando definir

a (in)existência de incompatibilidade entre ambos. Para tanto, foi utilizado o método hipotético-dedutivo, que conduziu a pesquisa por meio da testagem das hipóteses apresentadas.

1

Aspectos legais de proteção de dados

Conforme definição legal, trazida pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), considera-se dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável"[1]. As regulamentações de proteção de dados pessoais se consolidaram a partir da década de 1990, e decorrem do surgimento e desenvolvimentos de negócios e empreendimentos fundados na economia digital, "viabilizados pelos avanços tecnológicos e pela globalização"[2]. Com um novo mundo de interações ocorrendo na via digital, dados passaram a ser gerados, compartilhados, armazenados, vendidos e até mesmo roubados a todo instante.

De acordo com pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC), cerca de 126,9 milhões de brasileiros (equivalente a 70% da população) acessaram à Internet regularmente em 2018[3]. Ainda que um pouco inferior à média dos países desenvolvidos, de 80%, o acesso dos brasileiros está acima de outros países em desenvolvimento árabes e do leste europeu, que fica em torno de 50% a 60%[4].

---

[1] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

[2] PINHEIRO, Patrícia Peck. **Proteção de dados pessoais** - comentários à Lei n. 13.709/2018 LGPD - São Paulo: Saraiva Educação, 2018. p. 15. Disponível em: Minha Biblioteca.

[3] LAVADO, Thiago. **Uso da internet no Brasil cresce, e 70% da população está conectada**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml. Acesso em: 14 out. 2019.

[4] *Ibidem.*

Dos usuários brasileiros, 43,7 milhões (34% do total de usuários) fizeram compras pela Internet, enquanto 19% divulgaram ou venderam algum produto online[5]. Também 32% (equivalente a 40,8 milhões de usuários) pediram táxi ou carro por aplicativo, 28% contrataram serviços de streaming de vídeo, 8% contrataram streaming de música, 12% pediram comida e 3% utilizaram a Internet para contratar algum tipo de serviço financeiro[6].

Para realizar cada uma dessas interações, foi necessária a inserção de dados pessoais, como e-mail, telefone, nome, CPF, cartão de crédito, dentre outros, que ficam na posse de algum controlador. Tratando-se de informações importantes, relativas à privacidade de cada um, é importante a existência de legislações que forneçam algum tipo de proteção. Assim, convém analisar a historicidade das legislações que visam proteger dados pessoas tanto no Brasil quanto no direito comparado, com especial atenção ao direito europeu, pioneiro nesse aspecto, bem como as exigências legais impostas aos agentes de tratamento.

1.1 Histórico das legislações de proteção de dados

Tratando-se de um direito aparentemente recente, é importante compreender o histórico das legislações sobre proteção de dados. Para o presente estudo, a abordagem inicia pela compreensão de como ocorreu a proteção do direito à privacidade (2.1.1) até se chegar à bifurcação que concedeu aos dados e informações pessoais proteção própria (2.1.2). Considerando que o tema de proteção de dados está emergindo concomitantemente em todo o globo, é necessária uma perspectiva global sobre o tema, com especial ênfase no continente europeu, dada a

[5] *Ibidem*

[6] *Ibidem*

similaridade entre a recente Lei Geral de Proteção de Dados Pessoais Brasileira e o Regulamento Geral de Proteção de Dados europeu (GDPR).

1.1.1 Histórico da proteção do direito à privacidade

Ainda que atualmente a proteção de dados pessoais seja distinguida da privacidade, nem sempre foi assim. Convém, portanto, estudar brevemente sobre a proteção da privacidade a fim de se ter uma completa visão sobre o histórico da proteção de dados. Apesar de não possuir definição clara na legislação brasileira, referências à privacidade passam por diversos termos: "vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e até mesmo 'privatividade' e 'privaticidade', entre outros"[7]. Na doutrina e na jurisprudência, reconhecendo-se a dificuldade de defini-la, já foram produzidos diversos conceitos de privacidade, os quais podem ser resumidos em quatro categorias: "a) o direito a ser deixado só (*the right to be let alone*); b) o resguardo contra interferências alheias; c) segredo ou sigilo; d) controle sobre informações e dados pessoais"[8].

A necessidade de proteção da privacidade, ao longo da história, expressou-se de diferentes formas, de acordo com o que a sociedade queria ou precisava proteger dos olhos, ou do conhecimento, alheios. Conforme expõe Doneda, cuja análise histórica do tema é bastante íntegra, a preocupação *jurídica* com a privacidade, contudo, manifestou-se somente no final do século XIX[9]. Anteriormente, os próprios mecanismos sociais cumpriam esse papel.

De acordo com o doutrinador, a doutrina moderna do direito à privacidade tem como marco fundador o artigo "The right to privacy", de

[7] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 101.

[8] LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011. p. 52.

[9] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 8.

Samuel Warren e Louis Brandeis, escrito em 1890 e publicado na revista Harvard Law Review[10]. No texto, os autores preocupavam-se com as ameaças à privacidade que poderiam decorrer dos desenvolvimentos tecnológicos – na época, a invenção das fotografias e a indústria dos jornais[11].

O direito à privacidade foi inicialmente marcado pelo foco no indivíduo "consigo mesmo" (visando isolamento ou tranquilidade), decorrente da individualidade que marcava a época. Aos poucos, foi sendo aprimorado pela consciência de que "a privacidade é um aspecto fundamental da realização da pessoa do desenvolvimento de sua personalidade"[12]. Saindo da concepção individualista para se alinhar à teoria dos direitos da personalidade, a proteção da privacidade se transformou, atualmente, em "um elemento que, antes de garantir o isolamento ou a tranquilidade, [proporciona] ao indivíduo os meios necessários para a construção e consolidação de uma esfera privada própria", auxiliando, assim, na "comunicação e relacionamento com os demais"[13].

Antes disso, contudo, nos primórdios da proteção legal da privacidade, os casos judiciais de proteção à privacidade estavam relacionados a pessoas de grande renome e destaque social, como atores, músicos e políticos[14]. A defesa da privacidade nos tribunais, portanto, estava reservada a pessoas de projeção social, que possuíam demanda para tanto.

A possibilidade de ascensão social, entretanto, acompanhante da economia de mercado e da proteção à propriedade privada, gerou (e gera, cada vez mais) uma multidão de pessoas que passaram a estar sujeitas a

---

[10] *Ibidem*.

[11] LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011. p. 52.

[12] DONEDA, Danilo. *op. cit*.

[13] *Ibidem*. p. 24.

[14] *Ibidem*. p. 11.

ter "sua privacidade ofendida"[15], visto que não estavam mais fixas à esfera social em que nasceram. Conforme lecionou Mises em uma série de palestras feitas na Argentina, em 1958, transformadas, por sua esposa, em um livro:

> Duzentos anos atrás, antes do advento do capitalismo, o status social de um homem permanecia inalterado do princípio ao fim de sua existência: era herdado dos seus ancestrais e nunca mudava. Se nascesse pobre, pobre seria para sempre; se rico – lorde ou duque –, manteria seu ducado, e a propriedade que o acompanhava, pelo resto dos seus dias.
> [...]
> Quem viajasse de um país para outro em 1750 constataria que as classes mais elevadas, os aristocratas, se vestiam em geral de maneira idêntica em toda a Europa; e que as classes baixas usavam roupas diferentes. Vendo alguém na rua, era possível perceber de imediato – pelo modo como se vestia – a sua classe, o seu *status*.
> É difícil avaliar o quanto essa situação era diversa da atual. Se venho dos Estados Unidos para a Argentina e vejo um homem na rua, não posso dizer qual é seu status. Concluo apenas que é um cidadão argentino, não pertencente a nenhum grupo sujeito a restrições legais. Isto é algo que o capitalismo nos trouxe. Sem dúvida há também diferenças entre as pessoas no capitalismo. Há diferenças em relação à riqueza; diferenças estas que os marxistas, equivocadamente, consideram equivalentes àquelas antigas que separavam os homens na sociedade de *status*.[16]

Mises complementa, ainda, que, enquanto na idade média o que distinguia um homem da classe média e baixa era o primeiro ter sapatos e o segundo, não, hoje a diferença entre um rico e um pobre se reduz, muitas vezes, à diferença entre um "Cadillac e um Chevrolet. O Chevrolet pode ser de segunda mão, mas presta a seu dono basicamente os mesmos

[15] *Ibidem*. p. 13.

[16] MISES, Ludwig von. **As seis lições**. 7 ed. São Paulo: Instituto Ludwig von Mises Brasil, 2009. Disponível em: https://mises.org.br/Ebook.aspx?id=113. p. 13 e 33. Acesso em: 10 nov. 2019.

serviços que o Cadillac poderia prestar, uma vez que também está apto a se deslocar de um local a outro"[17]. Assim, não somente políticos ou atores, mas boa parte da população também passou a ser detentora de informações relevantes, inclusive economicamente, o que aprofundou a necessidade de proteção da privacidade.

Após a segunda metade do século XX, com o crescimento do desenvolvimento tecnológico e do fluxo de informações, fruto do complexo crescimento das relações de mercado, a importância dessas informações passou a aumentar, especialmente pelo surgimento de novas técnicas para recolhê-las, processá-las e utilizá-las[18]. Esse aumento no fluxo de informações foi, inicialmente, utilizado somente pelo Estado, que, segundo Doneda, possui duas importantes justificativas para utilizar informações pessoais: controle e eficiência[19]. Ter um conhecimento profundo e preciso sobre a população auxilia no exercício de uma Administração Pública eficiente.

Hely Lopes Meirelles, ao definir a eficiência como um dos princípios e deveres da Administração Pública, conceitua-a como:

> o que se impõe a todo agente público de realizar suas atribuições com presteza, perfeição e rendimento funcional. É o mais moderno princípio da função administrativa, que já não se contenta em ser desempenhada apenas com legalidade, exigindo resultados positivos para o serviço público e satisfatório atendimento das necessidades da comunidade e de seus membros[20].

Maria Di Pietro, complementando, separa esse princípio em dois aspectos:

---

[17] *Ibidem*.

[18] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 12.

[19] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 13.

[20] MEIRELLES, Hely Lopes. **Direito administrativo brasileiro**. 28 ed. São Paulo: Malheiros, 2003. p. 102.

> pode ser considerado em relação **ao modo de atuação do agente público**, do qual se espera o melhor desempenho possível de suas atribuições, para lograr os melhores resultados; e em relação ao **modo de organizar, estruturar, disciplinar a Administração Pública**, também com o mesmo objetivo de alcançar os melhores resultados na prestação do serviço público[21].

Dispor de informações sobre as pessoas, portanto, é fundamental para o exercício eficiente da Administração Pública. Isso implica, por exemplo, na realização de censos e pesquisas, além de regras que tornem obrigatória a comunicação de determinadas informações ao poder público[22]. Deter informações pessoais sobre os indivíduos, por outro lado, também possibilita o exercício de controle sobre eles, muitas vezes sob a justificativa de prevenção ou repressão de crimes. No setor privado, por sua vez, em razão do alto custo para coleta e processamento de dados, as informações pessoais não haviam sido exploradas senão com o desenvolvimento e avanço das tecnologias de informação das últimas décadas[23], assunto que será posteriormente abordado.

Após a Segunda Guerra Mundial acontece, também, a evolução do tratamento da privacidade pelo ordenamento jurídico, que passou a caracterizá-lo como direito fundamental em várias declarações internacionais. Sua primeira menção foi em 1948, na Declaração Americana dos Direitos e Deveres do Homem[24]; no mesmo ano, estava também presente na Declaração Universal dos Direitos do Homem, aprovada pela Assembleia

---

[21] DI PIETRO, Maria Zanella. **Direito Administrativo**. 30 ed. Rio de Janeiro: Forense, 2017. Disponível em: Minha Biblioteca.

[22] DONEDA, Danilo. *op. cit.* p. 14.

[23] *Ibidem*.

[24] "Artigo V. Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar". IX CONFERÊNCIA INTERNACIONAL AMERICANA. **Declaração Americana dos Direitos e Deveres do Homem**. Bogotá, 1948. Disponível em: https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm. Acesso em: 13 nov. 2019.

Geral da Organização das Nações Unidas[25]. Dois anos depois, constou na Convenção Europeia dos Direitos do Homem[26], e, em 1969, na Convenção Americana dos Direitos do Homem (Carta de San José)[27].

No Brasil, a Constituição Federal de 1988, em seu consagrado artigo 5º, inciso X, assegurou a inviolabilidade da intimidade e da vida privada, assegurando o direito de reparação em caso de violação[28]. O Código Civil de 2002, logo em seu início, dedica um capítulo inteiro sobre os direitos da personalidade, garantindo sua intransmissibilidade, irrenunciabilidade e impossibilidade de sofrer limitação voluntária[29], bem como a tutela de quaisquer direitos da personalidade, ao estipular a possibilidade de "exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei"[30].

A análise do histórico de legislações sobre privacidade pertinentes a este trabalho culmina no reconhecimento da proteção de dados pessoais

---

[25] "Artigo 12°. 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". ASSEMBLEIA GERAL DA ONU. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 13 nov. 2019.

[26] "Artigo 8º. Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros". CONSELHO DA EUROPA. Convenção Europeia dos Direitos do Homem. Roma, 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 13 nov. 2019.

[27] "Artigo 11. Proteção da honra e da dignidade. 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas". ESTADOS SIGNATÁRIOS. **Convenção Americana sobre Direitos Humanos**. San José, 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 13 nov. 2019.

[28] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 out. 2019.

[29] "Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária". BRASIL. **Lei nº 10.406, de 10 de janeiro de 2000**. Institui o Código Civil. Brasília: Presidência da República. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 13 nov. 2019.

[30] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2000**. Institui o Código Civil. Brasília: Presidência da República. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 13 nov. 2019.

de forma apartada da privacidade, oficializado na Carta dos Direitos Fundamentais da União Europeia (2000)[31]. Nela há uma interessante diferenciação: a proteção de dados pessoais está prevista expressamente em um artigo posterior ao que protege a privacidade relativa à vida privada, reconhecendo a importância que os dados pessoais passaram a ter, merecendo proteção própria. Nas palavras de Doneda, o primeiro artigo se destina a tutelar "o momento individualista de intromissões exteriores", enquanto o segundo tutela a "dinâmica dos dados pessoais em suas várias modalidades"[32]:

> *Artigo 7º*.
> **Respeito pela vida privada e familiar**.
> Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.
>
> *Artigo 8º*.
> **Proteção de dados pessoais**.
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente[33].

Com essa nova bifurcação, desprendendo a proteção de dados da proteção à privacidade, adentra-se na análise específica das legislações sobre

---

[31] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 27.

[32] *Ibidem*.

[33] UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia, de 07 de dezembro de 2000**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN. Acesso em: 21 out. 2019.

o primeiro tipo, que, por outros meios e com suas próprias características, visam proteger uma parte específica da privacidade humana.

1.1.2 Legislações de proteção de dados pessoais no Brasil e no direito comparado

No contexto legislativo de proteção de dados, convém verificar, inicialmente, como o assunto foi tratado nos ambientes britânico, norte-americano e europeu, à luz de um levantamento feito por Vinicius Borges Fortes. Posteriormente, será dado início à análise do RGPD europeu e das legislações de proteção de dados brasileiras. A exposição, conforme feita pelo autor, não é cronológica, e segue o histórico de cada região.

No contexto britânico, em 1978 o Comitê de Proteção de Dados do Parlamento apresentou um Relatório aprofundado sobre a implantação de uma autoridade de proteção de dados, no qual concluiu que "a função do direito de proteção de dados deveria ser diferente do direito à privacidade", visto que "determinados aspectos da proteção de dados [...] não possuem qualquer relação com a garantia de privacidade"[34]. No próprio estudo, as duas áreas foram nomeadas como "privacidade dos dados" e "privacidade das informações", sendo aquela o poder do indivíduo controlar a circulação dos dados sobre si próprio[35]. Posterior ao Relatório, três instrumentos normativos foram elaborados no contexto britânico (antes do Regulamento Geral de Proteção de Dados Europeu [RGPD/GDPR])[36]: *Data*

[34] FORTES, Vinícius Borges. **O Direito Fundamental à Privacidade**: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil. Tese (Doutorado) - Curso de Doutorado em Direito, Programa de Pós-graduação em Direito, Universidade Estácio de Sá, Rio de Janeiro, 2015. p. 124. Disponível em: https://portal.estacio.br/media/922618/ok-vinicius-borges-fortes.pdf. Acesso em 06 out. 2019.

[35] *Ibidem*.

[36] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em 11 jun. 2019.

Protection Act[37] (DPA), de 1998; *Freedom of Information Act*[38], de 2000; *Privacy and Electronic Communications (EC Directive) Regulations*[39].

Nos Estados Unidos da América, Fortes aponta para oito instrumentos normativos que tratam de proteção de dados. Merecem menção, contudo, para o propósito do presente estudo, três: o *Freedom of Information Act of 1966* (FOIA), que permite "a divulgação total ou parcial das informações inéditas e de documentos controlados pelo governo dos Estados Unidos"[40]; o *Privacy Act 1974*, que consiste em um "código [...] regulamenta a coleta, manutenção, utilização e divulgação de informações sobre indivíduos, mantidas em sistemas de registros por agências federais", podendo, por esse último, cidadãos norte-americanos e estrangeiros residentes permanentes requerer acesso a seus registros e sua alteração[41]; o *Electronic Communications Privacy Act* (ECPA), de 1986, que protege comunicações realizadas por e-mails ou conversas telefônicas, bem como dados armazenados eletronicamente[42].

Na Europa, antes mesmo das legislações mencionadas no contexto anglo-saxão, o Estado de Hesse, na Alemanha, criou, em 1970, a primeira lei de proteção de dados pessoais do mundo, que levou à composição de um projeto de lei que resultou, em 1979, à entrada em vigor da primeira

---

[37] "O primeiro diploma legal britânico, o DPA, consiste em uma norma emitida pelo parlamento do Reino Unido e da Irlanda do Norte com o objetivo de processar os dados dos cidadãos, simbolizando a legislação mais representativa em termos de proteção dos dados pessoais no Reino Unido". FORTES, Vinícius Borges. *op. cit.* p. 127.

[38] "O *Freedom of Information Act 2000* é uma norma oriunda do Parlamento do Reino Unido, que cria um 'direito de acesso' às informações detidas pelas autoridades públicas". *Ibidem*.

[39] "Esse diploma legal cumpre função complementar ao *Data Protection Act 1998*, instituindo regras para a confidencialidade das comunicações eletrônicas, para a restrição no tratamento de determinados dados de tráfego, conferindo especial atenção ao processo de identificação de chamadas telefônicas realizadas e recebidas. Além disso, aponta mecanismos de proteção de dados nas comunicações realizadas por meio de fax e correio eletrônico". *Ibidem*. p. 128.

[40] *Ibidem*. p. 129.

[41] FORTES, Vinícius Borges. **O Direito Fundamental à Privacidade**: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil. Tese (Doutorado) - Curso de Doutorado em Direito, Programa de Pós-graduação em Direito, Universidade Estácio de Sá, Rio de Janeiro, 2015. p. 130. Disponível em: https://portal.estacio.br/media/922618/ok-vinicius-borges-fortes.pdf. Acesso em 06 out. 2019.

[42] *Ibidem*. p. 131.

Lei Federal de Proteção de Dados Pessoais[43]. Fortes faz menção, igualmente, a um julgamento histórico no Tribunal Constitucional Federal alemão envolvendo a Lei do Censo, em 1983, em que houve "o reconhecimento do direito fundamental à autodeterminação informativa sobre os dados de caráter pessoal", momento em que os indivíduos passaram a ter o direito "de decidir quando e em que medida a informação pessoal pode ser publicada", que deu base às normativas continentais europeias[44].

Na Constituição Europeia, de 2004, previu-se, no artigo I – 51º, o direito à "proteção dos dados de caráter pessoal que lhes digam respeito"[45]. Mais à frente, no artigo II – 68º, foi estabelecido que esses dados

> devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação[46].

Referida Constituição remete-se à Diretiva 95/46/CE, de 1995, que instituiu regras de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação no continente[47]. Nessa diretiva tem-se as principais definições de termos referentes a dados pessoais e seu tratamento, em parte reaproveitadas pela GDPR. Como apontado por Fortes, há a imprescindibilidade de que qualquer tratamento de dados seja feito de forma explícita, "lícita e leal com a pessoa da qual se

---

[43] *Ibidem*. p. 133.

[44] *Ibidem*. p. 133-134.

[45] UNIÃO EUROPEIA. **Tratado que estabelece uma Constituição para a Europa. Roma, 2004**. Disponível em: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_pt.pdf. Acesso em: 19 nov. 2019.

[46] *Ibidem*.

[47] UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 19 nov. 2019.

originam os dados, os quais devem, necessariamente, incidir sobre dados adequados, pertinentes e não excessivos em relação às finalidades outorgadas pelo sujeito em questão"[48].

Em 18 de dezembro de 2000, o Parlamento Europeu e do Conselho publicou o Regulamento nº 45/2001, que assegura

> a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais, e não limitam nem proíbem a livre circulação de dados pessoais entre eles ou entre eles e destinatários abrangidos pela legislação nacional dos Estados-Membros que transponha a Diretiva 95/46/CE[49].

O principal avanço desse Regulamento, conforme Fortes, foi a criação de uma autoridade independente de controle, denominada Autoridade Europeia para a Proteção de Dados (EDPS – *European Data Protection Supervisor*), com o objetivo de "controlar a aplicação do regulamento e das diretivas em todas as operações de tratamento de dados [...] no âmbito da União Europeia"[50]. Ademais, outras decisões em setores técnicos e normativos da União Europeia, como a Decisão 2012/C 308/07 e a Decisão 2013/504/EU, aprimoraram e definiram o escopo prático da aplicação das normas supracitadas[51].

Na breve Carta dos Direitos Fundamentais da União Europeia, proclamada pelo Parlamento Europeu, pelo Conselho da União Europeia e

---

[48] FORTES, Vinícius Borges. **O Direito Fundamental à Privacidade**: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil. Tese (Doutorado) - Curso de Doutorado em Direito, Programa de Pós-graduação em Direito, Universidade Estácio de Sá, Rio de Janeiro, 2015. p. 138. Disponível em: https://portal.estacio.br/media/922618/ok-vinicius-borges-fortes.pdf. Acesso em 06 out. 2019.

[49] UNIÃO EUROPEIA. **Regulamento (CE) nº 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000.** Bruxelas. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32001R0045&from=PT. Acesso em: 19 nov. 2019.

[50] FORTES, Vinícius Borges. *op. cit.* p. 138.

[51] *Ibidem*. p. 140.

pela Comissão Europeia em 7 de dezembro de 2000[52], novamente há a expressa proteção de dados pessoais. No Artigo 8º, estabeleceu-se que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" e o "direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação"[53]. Especifica, ainda, que tais dados "devem ser objeto de um tratamento legal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei"[54].

Mais recentemente, promulgou-se o Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679 (GDPR - *General Data Protection Regulation*), aprovado no dia 27 de abril de 2016, com prazo para adequação até 25 de maio de 2018, quando a aplicação das penalidades foi iniciada[55]. Devido à Lei Geral de Proteção de Dados Pessoais brasileira ser profundamente baseada no Regulamento, serão analisados mais detalhadamente em tópico dedicado. Convém destacar que, em comparação com o GDPR, o regulamento anterior era mais "leniente com as empresas e com o que elas faziam com os dados pessoais em seu poder"[56]. Conforme estabelecido em seu preâmbulo, o GDPR tem como objetivos:

> (2) [...] contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a

[52] UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia, de 07 de dezembro de 2000**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN. Acesso em: 21 out. 2019.

[53] UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia, de 07 de dezembro de 2000**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN. Acesso em: 21 out. 2019.

[54] *Ibidem.*

[55] PINHEIRO, Patrícia Peck. **Proteção de dados pessoais** - comentários à Lei n. 13.709/2018 LGPD - São Paulo: Saraiva Educação, 2018. p. 18. Disponível em: Minha Biblioteca.

[56] "Prior to the GDPR, European data was regulated by the Data Protection Directive (the Directive), which was generally more lenient with businesses and what they did with data subjects' data". MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

> consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.
> [...]
> (13) [...] assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno. [...] [Garantir] a segurança jurídica e a transparência nos operadores econômicos, [...] que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento, [...] que assegure um controlo coerente do tratamento de dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades.[57]

No Brasil, além das menções de proteção à privacidade já citadas no tópico anterior, presentes na Constituição Federal e no Código Civil, há, também, previsões específicas de proteção e acesso às informações pessoais. Cita-se, nesse sentido, novamente a Constituição Federal:

> Art. 5º. [...] XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado[58];

No mesmo Diploma, previu-se, também, o remédio constitucional do *habeas data*, que visa assegurar o acesso a informações pessoais que estejam em posse do Estado ou de entidades privadas que tenham informações

---

[57] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em 11 jun. 2019.

[58] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 nov. 2019.

de caráter público[59], bem como sua alteração[60]. Em seu regulamento, acrescentou-se a possibilidade de anotação, nos assentamentos do interessado, de "contestação ou explicação sobre dado verdadeiro, mas justificável, e que esteja sob pendência judicial ou amigável"[61].

Ademais, o Código de Defesa do Consumidor, no art. 43, garante ao consumidor o acesso a informações pessoais suas arquivadas em banco de dados. Além de firmar a impossibilidade de que bancos de dados mantenham "informações negativas referentes a período superior a cinco anos", o artigo exige que os cadastros e dados sejam "objetivos, claros, verdadeiros e em linguagem de fácil compreensão"[62].

A primeira preocupação com dados pessoais virtuais de forma explícita, contudo, apareceu pela primeira vez na legislação brasileira somente com a Lei nº 12.965, de 23 abril de 2014, conhecida como Marco Civil da Internet, que previu, em seu artigo terceiro, como um dos princípios da disciplina do uso da Internet no Brasil, a "proteção dos dados pessoais", ao lado do princípio da proteção da privacidade[63]. No artigo 7º, que assegura

---

[59] O Código de Defesa do Consumidor, no art. 43, §4º, afirma que "[os] bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público". BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 20 nov. 2019.

[60] "Art. 5º. [...] LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo". BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 nov. 2019.

[61] 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: Presidência da República. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 20 nov. 2019.

[62] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 20 nov. 2019.

[63] 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: Presidência da República. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 out. 2019.

os direitos dos usuários da Internet, é frisada a inviolabilidade da intimidade e da vida privada, bem como o sigilo do fluxo de suas comunicações pela Internet. No mesmo dispositivo foi, igualmente, garantida a necessidade de consentimento expresso sobre "coleta, uso, armazenamento e tratamento de dados pessoais"[64]. Nos artigos 10 a 12, é feita uma tímida tutela do processo de tratamento desses dados[65].

Contudo, inexistiam critérios mais objetivos e detalhados para o gerenciamento e tratamento de tais dados dentro de um contexto de proteção legal. Assim, normas mais específicas, que melhor estabeleçam regras para proteção de dados pessoais, bem como que delimitem responsabilidades e instruções para os controladores de dados, se faziam necessárias. Para suprir essas lacunas, promulgou-se no Brasil, em 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), cujos fundamentos, princípios e objetivos gerais serão tratados em seguida.

1.2 Fundamentos, princípios e objetivos gerais da Lei Geral de Proteção de Dados Pessoais (LGPD) e exigências legais aos agentes de tratamento

A Lei nº 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 14 de agosto de 2018, estabelece as disciplinas básicas para o tratamento de dados pessoais no Brasil. De acordo com seu artigo primeiro, o objetivo da lei é "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[66]. Nesse sentido, ela traz "princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da

[64] *Ibidem*.

[65] BARRETO JUNIOR, Irineu Francisco; FAUSTINO, André. **Aplicativos de serviços para saúde e proteção dos dados pessoais de usuários**. p. 298. Revista Jurídica. vol. 01, nº. 54, Curitiba, 2019. DOI: 10.6084/m9.figshare.7841105.

[66] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

sociedade digital, que são as bases de dados relacionados às pessoas"[67]. Além de disposições gerais, a LGPD estabelece regras de controles técnicos para o manuseio dos dados pessoais, visando gerar segurança ao seu titular, que serão abordadas no próximo subcapítulo.

Para esta pesquisa foram utilizadas as definições trazidas pela própria lei, em seu artigo 5º. Assim, conforme ela, dado pessoal significa toda "informação relacionada a pessoa natural identificada ou identificável", sendo chamado de "titular" a pessoa a quem os dados pessoais se referem[68]. Dados anonimizados, relativos a titular "que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento"[69], não são considerados dados pessoais para os fins da LGPD, "salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido"[70].

Migrando para os responsáveis pelo processamento e armazenamento dos dados pessoais do titular, existem as figuras do "controlador" e do "operador", recapitulando os conceitos de controlador e processador utilizados no Regulamento Geral de Proteção de Dados europeu (GDPR)[71]. Controlador é a pessoa "a quem competem as decisões referentes ao tratamento de dados pessoais", enquanto operador é a pessoa que "que

---

[67] PINHEIRO, Patrícia Peck. **Proteção de dados pessoais** - comentários à Lei n. 13.709/2018 LGPD - São Paulo: Saraiva Educação, 2018. p. 15. Disponível em: Minha Biblioteca.

[68] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

[69] *Ibidem*.

[70] *Ibidem*.

[71] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Acesso em 11 jun. 2019.

realiza o tratamento de dados pessoais em nome do controlador"[72]. Ambas podem ser pessoa natural ou jurídica, de direito público ou privado, e podem ser genericamente chamadas de "agente de tratamento". O "encarregado", por fim, é a "pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados"[73].

As operações realizadas com dados pessoais pelos agentes são chamadas de "tratamento", e incluem

> 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 [dos dados pessoais][74].

Os fundamentos da disciplina de proteção de dados pessoais se encontram elencados no artigo 2º, e retomam termos importantes já estudados anteriormente, especialmente o respeito à privacidade e à autodeterminação informativa:

> 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

---

[72] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

[73] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

[74] *Ibidem.*

> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. [75]

Trata-se, portanto, de uma lei bastante completa, em grande parte inspirada no Regulamento europeu, que se propõe a trazer maior segurança jurídica ao tema, assegurando a proteção de direitos dos titulares dos dados pessoais e estabelecendo regras e diretrizes bastante específicas a serem cumpridas pelos agentes de tratamento. Tais exigências legais são direcionadas aos agentes de tratamento, gênero pelo qual são chamados o controlador e o operador, conforme definição já transcrita acima. Eles são os principais alvos das normas codificadas na LGPD, e a eles foram impostas diversas responsabilidades, que serão estudadas no presente subcapítulo.

As atividades de tratamento são sujeitas à boa-fé e a princípios específicos, com conceituação também trazida pela LGPD, em seu artigo 6º. Considerando que todas as disposições da Lei são baseadas nestes princípios, convém estuda-los de maneira específica, bem como de maneira comparada com o Regulamento europeu. São estes os princípios de tratamento de dados previstos na LGPD: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas[76].

O primeiro princípio na lei brasileira, "finalidade", estabelece que os dados não podem ser usados para outros fins que não aqueles informados ao titular antes ou no momento da coleta. Em outras palavras, mesmo de posse dos dados do titular, o agente de tratamento não pode utilizá-los

---

[75] *Ibidem.*

[76] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

como bem entender, estando vinculado aos propósitos informados. No GDPR, referido princípio encontra-se destacado da seguinte forma:

> 1. Os dados pessoais são: [...] b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º, nº 1 («limitação das finalidades»)[77].

Além da previsão semelhante à brasileira, há menção à possibilidade de tratamento posterior para fins de interesse público, científico ou estatístico. Para esses fins, o artigo 89 assegura que, caso os dados sejam utilizados, estarão sujeitos a "garantias adequadas", que asseguram "o respeito do princípio da minimização dos dados", incluindo a "pseudonimização"[78]. No caso brasileiro, o artigo 16 informa sobre essas possibilidades.

O segundo e o terceiro princípios, da "adequação" e da "necessidade", se encontram unidos em um só no GDPR, o da "minimização dos dados"[79]. Em resumo, os dados tratados devem ser limitados à necessidade, sem captação superior à efetivamente necessária à finalidade para a qual consentiu o titular.

O quarto e o sexto princípios, "livre acesso" e "transparência", garantem a consulta dos titulares a seus dados e ao tratamento a ser realizado,

---

[77] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Artigo 5º. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Acesso em 11 jun. 2019.

[78] *Ibidem*. Artigo 89º.

[79] "Os dados pessoais são: [...] c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»)". *Ibidem*. Artigo 5º.

de forma clara, precisa e gratuita. O quinto, "qualidade dos dados", por sua vez, visa assegurar que os dados coletados são verdadeiros, correspondentes à realidade, sendo garantido ao titular a possibilidade de atualização, de acordo com a necessidade e a finalidade[80].

O princípio da "segurança" visa garantir que os dados não serão acessados por pessoas não autorizadas, tampouco perdidos, destruídos ou alterados de forma ilícita ou acidental[81]. O oitavo e o novo princípios, "prevenção" e "não discriminação", protegem os titulares de eventuais danos que possam ser causados em razão do tratamento dos dados pessoais, bem como de que os dados sejam usados "para fins discriminatórios ilícitos ou abusivos". Por fim, o décimo princípio, "responsabilização e prestação de contas", exige do agente de tratamento a demonstração de adoção de medidas que comprovem a "observância e o cumprimento das normas de proteção de dados pessoais".

No GDPR, outros dois princípios (que, de certa forma, se mesclam com os da lei brasileira) são mencionados de maneira individualizada: o da "limitação da conservação" e o da "licitude, lealdade e transparência". Enquanto o segundo garante que os dados pessoas são "objeto de um tratamento lícito, leal e transparente em relação ao titular", o primeiro é explicado da seguinte forma:

> 1. Os dados pessoais são: [...] e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para

[80] No Regulamento europeu: "Os dados pessoais são: [...] d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»)". *Ibidem*. Artigo 89º.

[81] No Regulamento europeu: "Os dados pessoais são: [...] f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»)". UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Artigo 89º. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Acesso em 11 jun. 2019.

> as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, nº 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»)[82].

A LGPD estabelece, em seu artigo 7º, uma lista exaustiva de dez situações em que o tratamento de dados pessoais pode ocorrer. A primeira delas é quanto o titular consente com o tratamento. Conforme especificado no artigo subsequente, esse consentimento deve ser fornecido por escrito ou por "outro meio que demonstre a manifestação de vontade do titular". O ônus da prova incumbe ao agente de tratamento, que deve comprovar que o consentimento foi obtido em conformidade com a lei[83].

Mais importante do que o mero consentimento generalista para captação de dados, a LGPD estabelece que o consentimento deverá se referir a finalidades determinadas, e as "autorizações genéricas [...] serão nulas"[84]. Isso significa que o titular dos dados pessoais a serem coletados deve consentir com cada uma das destinações que o agente de tratamento pretender dar a eles. Aplicam-se, nesse sentido, todas as normas referentes aos vícios de consentimento. Ademais, o consentimento pode ser revogado a qualquer momento mediante manifestação do titular.

As outras hipóteses seguem abaixo transcritas, porém, para o propósito da presente pesquisa não há necessidade de sua explanação, que não aquela constante na lei:

---

[82] *Ibidem*. Artigo 5º.

[83] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

[84] *Ibidem*.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente[85].

Convém frisar, a fim de dar início ao estudo de um eventual conflito com as tecnologias *blockchain*, a seguir estudadas, que o consentimento pode ser revogado a qualquer momento, mediante manifestação do titular, ratificando-se os tratamentos realizados "sob amparo do consentimento

[85] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Art. 8º, §5º. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei"[86] (grifou-se). Há previsão, portanto, do direito ao titular dos dados de que esses sejam eliminados completamente, mesmo tendo sido consensualmente cedidos. O artigo 18 estabelece, dentre outros direitos, que o titular, mediante requisição, tem o direito a obter do controlador a "eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei"[87]. Por sua vez, o artigo 16 autoriza a conservação dos dados após o término de seu tratamento para quatro finalidades:

> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Não sendo nenhuma das hipóteses acima, o agente de tratamento deverá realizar a eliminação completa dos dados, caso solicitado pelo titular. O § 4º possibilita ao agente que, "[em] caso de impossibilidade de adoção imediata da providência" solicitada, o controlador enviará resposta ao titular dos dados, na qual poderá informar que não é agente de tratamento de dados, indicando, se possível, quem o é, ou "indicar as razões de fato ou de direito que impedem a adoção imediata da providência"[88]. Contudo, os dados devem ser retirados, ainda que não seja de imediato. Tem-se, aqui, uma hipótese de incompatibilidade com registros em *blockchain*, visto que

[86] *Ibidem.*

[87] *Ibidem.*

[88] *Ibidem.*

informações criptografadas em bloco são impossíveis de alteração ou exclusão, em tese, sem comprometer todo o restante da *blockchain*, tema que será posteriormente analisado.

Conclusivamente, a LGPD considera um cenário em que uma única pessoa física ou jurídica (o controlador) é responsável pela coleta e gestão dos dados pessoais. Ao regular as entidades centralizadoras que dominam o mercado hoje, tornando-as responsáveis, é possível que a legislação tenha desconsiderado a possibilidade de alternativas *descentralizadas* e criptografadas, nas quais a alteração das informações gravadas é impossível, gerando conflitos. Por essa razão, convém abordar o tema dessas tecnologias e, ao final, verificar a (in)existência de incompatibilidades.

2

Blockchain: aplicações práticas e tipos de bancos de dados

A tecnologia *blockchain*, ainda que um pouco distante da realidade prática da população, pelo menos até o presente momento, está trazendo um grande impacto ao mundo da tecnologia, por permitir novos produtos e serviços que antes eram inimagináveis, como moedas e contratos virtuais confiáveis e registros transparentes e "imutáveis"[1]. Estima-se, portanto, que a *blockchain* possa revolucionar muitas instituições e formas de interação entre indivíduos, especialmente os tradicionais registros públicos, bancos, e até mesmo a forma de se fazer contratos, por serem auto executáveis e imutáveis, dada sua base criptográfica.

A *blockchain*, além disso, garante segurança e imunidade à censura, pois decisões arbitrais, inclusive estatais, podem ser fisicamente inaplicáveis, conforme se verá adiante. Por outro lado, tal dificuldade de efetivar alterações nas informações registradas pode dificultar o *compliance* com legislações de proteção de dados, especialmente se não considerada a existência de registros descentralizados, em que é difícil estabelecer um responsável pelos dados ou até mesmo modifica-los.

Convém, em razão disso, estudar as raízes dessa tecnologia, suas especificidades, seus desdobramentos e aplicabilidades (a fim de se ter noção da extensão do impacto aqui estudado), bem como as classificações de *blockchain* existentes, com o fim posterior de analisar as variações das (in)compatibilidades.

---

[1] Ver: ULRICH, Fernando. **Bitcoin – A Moeda na Era Digital**. – São Paulo: Instituto Ludwig von Mises Brasil, 2014. Disponível em: https://mises.org.br/Ebook.aspx?id=99. Acesso em: 16 nov. 2019.

2.1 Conceito, origem e especificações técnicas da tecnologia *blockchain*

A *blockchain* tem origem bastante recente, sendo apresentada ao mundo em uma publicação[2] em 2008, por Satoshi Nakamoto[3], na qual aplica a tecnologia a uma moeda: surgia, assim, o Bitcoin. O contexto da época, em meio à crise do mercado financeiro, originada do excesso de intervenção estatal tanto no mercado imobiliário quanto na manipulação de juros[4], incentivava a busca por soluções que blindassem as pessoas das consequências de novas aventuras estatais em conluio com grandes corporações. "Sakamoto pretendia criar nada menos que uma nova moeda, que fosse imune a políticas monetárias imprevisíveis dos Estados e Governos, bem como à manipulação de mercado"[5]. Nesse sentido, o próprio autor, no resumo de seu artigo, explica que o Bitcoin é uma versão "ponto-a-ponto" de uma moeda eletrônica, "que pode ser enviada de uma pessoa a outra sem a necessidade de uma instituição financeira intermediando a relação"[6], em tradução livre. Em outras palavras, você é dono de sua própria agência bancária dessa moeda, e está automaticamente conectado a todas as outras.

O Bitcoin, primeira aplicação da *blockchain*, provou-se capaz de obter confiança em todo o mundo. Uma unidade dessa moeda, ao tempo em que esta pesquisa foi escrita, valia mais de US$ 7.000,00[7]. Ademais, a

---

[2] NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 23 nov. 2019.

[3] Não se sabe se Satoshi Nakamoto é um indivíduo e esse é seu nome ou seu pseudônimo, ou se, por trás dessa figura, existe um grupo de pessoas.

[4] ROQUE, Leandro. **Como ocorreu a crise financeira americana**. 2018. Disponível em: https://mises.org.br/Article.aspx?id=1696. Acesso em: 23 nov. 2019.

[5] TEIXEIRA, Tarcisio; RODRIGUES, Carlos Alexandre. **Blockchain e Criptomoedas**. Salvador: Editora JusPodivm, 2019. p. 15.

[6] NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 23 nov. 2019.

[7] ECONOMIA UOL. **Cotações**. Disponível em: https://economia.uol.com.br/cotacoes/. 2019. Acesso em: 23 nov. 2019.

desnecessidade de um intermediador ou controlador central, possibilitando transações diretas entre pessoas, abre infinitas possibilidades e soluções para problemas existentes. Cite-se, como exemplo, que o Bitcoin está sendo o único caminho que o povo venezuelano possui para fugir dos efeitos da inflação que destruiu a moeda do país[8] [9] - a inflação do bolívar soberano, de acordo com o Fundo Monetário Internacional, é de cerca de 200.000% em 2019[10].

O sucesso do Bitcoin e suas inúmeras consequências, ainda que revolucionários, não abrem tantas portas quanto a sua tecnologia de base, a *blockchain*. Isso porque o que garante o correto funcionamento do Bitcoin são os registros das transações, que impedem que a moeda seja gasta duas vezes, garantindo, assim, segurança. Antes da invenção da *blockchain*, moedas virtuais eram impossíveis em razão do problema do gasto duplo, abaixo explicado:

> Até a invenção do Bitcoin, em 2008, pelo programador não identificado conhecido apenas pelo nome Satoshi Nakamoto, transações online sempre requereram um terceiro intermediário de confiança. Por exemplo, se Maria quisesse enviar 100 u.m. (unidade monetária) ao João por meio da internet, ela teria que depender de serviços de terceiros como PayPal ou Mastercard. Intermediários como o PayPal mantêm um registro dos saldos em conta dos clientes. Quando Maria envia 100 u.m ao João, o PayPal debita a quantia de sua conta, creditando-a na de João. Sem tais intermediários, um dinheiro digital poderia ser gasto duas vezes. Imagine que não haja intermediários com registros históricos, e que o dinheiro digital seja simplesmente um arquivo de computador, da mesma forma que documentos digitais são arquivos de

[8] PEÑA, Carlos. **O Bitcoin foi o que impediu minha família de morrer de fome na Venezuela**. 2017. Disponível em: https://www.mises.org.br/Article.aspx?id=2771. Acesso em: 23 nov. 2019.

[9] RANDS, Kevin. **Why Venezuela's Currency Crisis Is A Case Study For Bitcoin**. 2017. Disponível em: https://www.forbes.com/sites/realspin/2017/02/03/why-venezuelas-currency-crisis-is-a-case-study-for-bitcoin/. Acesso em: 23 nov. 2019.

[10] IMF. International Monetary Fund. **Inflation rate, average consumer prices**. 2019. Disponível em: https://www.imf.org/external/datamapper/PCPIPCH@WEO/WEOWORLD/VEN. Acesso em: 23 nov. 2019.

> computador. Maria poderia enviar ao João 100 u.m. simplesmente anexando o arquivo de dinheiro em uma mensagem. Mas assim como ocorre com um e-mail, enviar um arquivo como anexo não o remove do computador originador da mensagem eletrônica. Maria reteria a cópia do arquivo após tê-lo enviado anexado à mensagem. Dessa forma, ela poderia facilmente enviar as mesmas 100 u.m. ao Marcos. Em ciência da computação, isso é conhecido como o problema do "gasto duplo", e, até o advento do Bitcoin, essa questão só poderia ser solucionada por meio de um terceiro de confiança que empregasse um registro histórico de transações.[11]

A *blockchain* (cadeia de blocos, em tradução livre) soluciona esse problema mantendo um registro cronológico das transações distribuído entre todos os participantes da rede[12]. Cada transação é verificada pelos chamados mineradores (ou *nodes*), computadores que fornecem poder de processamento em troca de recompensas na própria moeda[13]. Os mineradores analisam as informações inseridas e as confirmam, se verdadeiras. Após determinado número de informações ou transações registradas, consolida-se um "bloco" de informações, que recebe uma numeração criptográfica própria (através do processo de *hashing*), a qual é acrescentada no início do bloco seguinte, e assim por diante, criando uma cadeia de blocos criptografados que, em tese, não podem ser alterados[14].

Assim, todos os participantes da rede conseguem visualizar o estado das coisas, e verificar a validade das transações. Todas essas informações são armazenadas de forma descentralizada e passíveis de conferência em todos os computadores participantes. Essa, inclusive, era a intenção do

---

[11] ULRICH, Fernando. **Bitcoin – A Moeda na Era Digital**. – São Paulo: Instituto Ludwig von Mises Brasil, 2014. p. 17. Disponível em: https://mises.org.br/Ebook.aspx?id=99. Acesso em: 16 mar. 2019.

[12] *Ibidem*. p. 20.

[13] *Ibidem*.

[14] CHRISTIDIS, Konstantinos; DEVETSIKIOTIS, Michael. *Blockchains* and Smart Contracts for the Internet of Things. *in* **IEEE Access**, vol. 4, p. 2292-2303, 2016. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408. Acesso em: 20 nov. 2019.

inventor, que pretendeu criar um sistema eletrônico de pagamento "baseado em prova criptográfica em vez de confiança", possibilitando que duas pessoas transacionem sem a necessidade de confiar em um terceiro[15].

Em suma, uma *blockchain* é um livro-razão público e descentralizado, cuja confiança se dá na tecnologia em que é construída[16]. Normalmente, é descrito como tendo as seguintes características: consenso, proveniência, imutabilidade, finalidade e descentralização. A primeira, porque, em uma blockchain, a validade de um bloco é definida através de consenso entre os nós (computadores habilitados a validar um bloco, processo que será explicado adiante); a segunda, porque toda a cadeia de informações registradas é passível de verificação e conferência; a terceira, porque a edição das informações em um bloco consolidado é impossível; finalidade, porque todos os dados e histórico de transações e registros se encontram em uma única fonte confiável; descentralização, porque todos os registros são compartilhados/distribuídos entre todos os nós ou usuários da *blockchain*, então, caso um dos nós falhe, a rede continua funcionando, e os registros permanecem salvos em todos os computadores conectados[17].

---

[15] Tradução livre de: "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party". NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 23 nov. 2019.

[16] Uma analogia interessante de entender como uma *blockchain* funciona é compará-la ao Google Docs. Imagine-se a diferença entre escrever em conjunto um arquivo no Microsoft Word e escrevê-lo no Google Docs. Enquanto no primeiro seria necessário que cada um, individualmente, fizesse as alterações necessárias em seu computador, e depois enviasse o arquivo a outra pessoa, que estava aguardando, visto que duas pessoas não poderiam alterar o documento ao mesmo tempo, no Google Docs todos podem realizar alterações no mesmo arquivo de maneira pública e registrada concomitantemente. De: MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

[17] MCKINNEY, Scott; LANDY, Rachel; WILKA, Rachel. Smart Contracts, Blockchain, and the Next Frontier of Transactional Law. **Washington Journal of Law, Technology & Arts**, v. 13, Issue 3, 2018. Disponível em: http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1818/13WJLTA313.pdf?sequence=4&isAllowed=y. Acesso em: 01 dez. 2019.

A *blockchain* torna desnecessário, por exemplo, que seja necessário confiar nas outras pessoas com quem se está negociando, porque o que fideliza as transações é o próprio método. Contorna-se, aí, a necessidade de confiança em um armazenador (*keeper*) das informações[18], isso é, um computador que irá centralizar e processar todas as transações realizadas, o que evita diversos possíveis problemas que podem comprometer o objetivo:

> 1. [Um armazenador é] um ponto único que, se falhar, isto é, se ele se desconectar, ninguém conseguirá realizar nenhuma transação.
> 2. Armazenadores comumente cobram por seus serviços. Como pontos únicos capazes de possibilitar as transações, eles estão em uma posição de poder para aumentar suas cobranças ameaçando impedir os usuários de utilizarem seu serviço.
> 3. Como se certificar de que o armazenador não manipula o registro ou a aplicação para beneficiar certos membros de uma comunidade ou a si próprio? E se ele modificar as regras de validação?
> 4. Para determinados usos, pode ser impossível entrar em acordo sobre quem seria o armazenador[19].

A confiança na impossibilidade de alteração das informações decorre, majoritariamente, da gravação sequencial em bloco, aliada à criptografia. Para entender como isso ocorre, é preciso, inicialmente, compreender alguns conceitos e a forma técnica como uma *blockchain* se dá. Através dessa análise, compreender-se-á porque uma *blockchain* não é completamente imutável, apesar de, *na prática*, algumas acabarem sendo.

---

[18] IBANEZ, Luis-Daniel; O'HARA, Kieron; SIMPERL, Elena. **On *Blockchains* and the General Data Protection Regulation**. p. 2. 2018. Disponível em: https://eprints.soton.ac.uk/422879/. Acesso em 06 jun. 2019.

[19] Tradução livre do original em inglês: "1. Introduces a single point of failure, that is, if the keeper goes offline, then no one can do any transaction. 2. Keepers commonly charge for their services. As single points of failure, they are in a position of power to increase their charges by threatening to block users from the service. 3. How to be sure that the keeper does not manipulate the ledger or application to benefit certain members of the community or itself? What if it changes the validation rules? 4. For some use cases, it might be impossible to reach an agreement on who name as keeper". IBANEZ, Luis-Daniel; O'HARA, Kieron; SIMPERL, Elena. **On *Blockchains* and the General Data Protection Regulation**. p. 2. 2018. Disponível em: https://eprints.soton.ac.uk/422879/. Acesso em 06 jun. 2019.

Inicialmente, convém estudar a criptografia. Trata-se de uma ciência que "estuda meios de, com a utilização de 'segredos', manter dados seguros"; "a ciência da criptoanálise, por outro lado, é a ciência que estuda meios de decifrar os sistemas criptográficos"[20]. Juntas, formam a criptologia, que tem por escopo o estudo de códigos, com sua escrita e resolução. Seu objetivo é proteger determinada informação e "prover segurança aos dados armazenados e transmitidos nos diversos tipos de relações que se utilizam de dados digitais"[21]. Em outras palavras, visa ocultar dados através de códigos que podem, ou não, ser resolvidos.

Na prática, o processo de encriptação consiste em converter informações claras em uma versão não legível ou não acessível, visando prevenir que pessoas não autorizadas as acessem[22]. Isso é bastante útil para proteger dados pessoais, visto que, sem a chave de descriptação correta, uma pessoa não autorizada não poderá acessá-los.

Existem três classificações clássicas de criptografia: simétrica, assimétrica e por *hashing*. Outros autores, especialmente no contexto da *blockchain*[23], categorizam somente as duas primeiras como criptografia, inserindo a terceira como um procedimento autônomo, dada sua particular irreversibilidade. Enquanto o *hashing* é essencial em uma *blockchain*, não necessariamente os outros tipos de criptografia precisam estar presentes, embora normalmente estejam.

Em uma criptografia por chave simétrica, uma mensagem é criptografada e descriptografada utilizando a mesma chave. Assim, ao enviar

---

[20] TEIXEIRA, Tarcisio; RODRIGUES, Carlos Alexandre. **Blockchain e Criptomoedas**. Salvador: Editora JusPodivm, 2019. p. 37.

[21] *Ibidem.*

[22] BINANCE ACADEMY. **Encryption**. Disponível em: https://www.binance.vision/glossary/encryption. Acesso em: 30 nov. 2019.

[23] Como Andries Van Humbeeck, em: HUMBEECK, Andries Van. The Blockchain-GDPR paradox. **Journal of Data Protection & Privacy**, v. 2, nº 3, p. 208–212. Disponível em: https://www.henrystewartpublications.com/jdpp/v2. Aceso em: 28 nov. 2019.

uma mensagem criptografada a outra pessoa, será necessário enviar a chave também, ainda que por outro meio, a fim de permitir que a outra pessoa possa lê-la[24]. Contudo, ao ser transmitida, a chave pode ser vista e copiada por terceiros não autorizados. Esse problema levou à criação da criptografia por chave assimétrica.

Nessa segunda forma de criptografia cada usuário possui duas chaves: uma pública e outra privada. A chave pública é utilizada para criptografar, enquanto a privada é utilizada para descriptografar[25]. Quando alguém pretende enviar uma mensagem a outra pessoa, ele realiza a criptografia utilizando a chave pública do destinatário, e então realiza o envio. Estando a mensagem criptografada com a chave pública do destinatário, essa mensagem somente poderá ser descriptografada com a chave privada dele. Quaisquer terceiros que interceptem a mensagem não poderão acessá-la, visto que somente a chave privada do destinatário será capaz de fazê-lo. Nem mesmo o remetente, que realizou a criptografia, conseguirá desfazê-la[26]. Cumpre, portanto, a cada usuário guardar sua chave privada da maneira mais segura.

Contudo, apesar da insegurança na transmissão da chave, a criptografia simétrica é mais rápida e requer menos poder computacional. Por outro lado, a criptografia assimétrica é muito mais lenta e requer mais poder de processamento, especialmente porque as chaves são maiores e mais complexas[27].

Sobre o procedimento *hashing*, trata-se de um processo unilateral feito através de um algoritmo complexo, que transforma uma quantidade

---

[24] BINANCE ACADEMY. **Symmetric vs. Asymmetric Encryption**. Disponível em: https://www.binance.vision/security/symmetric-vs-asymmetric-encryption. Acesso em: 30 nov. 2019.

[25] *Ibidem*.

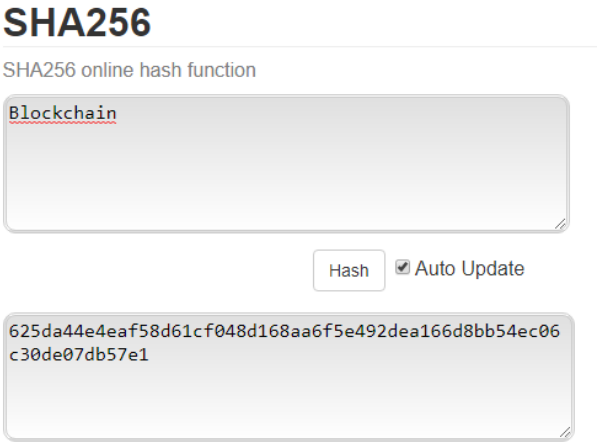
[26] *Ibidem*.

[27] *Ibidem*.

de dados em uma sequência de números (ou números e letras), que sempre terá o mesmo número de caracteres[28]. Exemplificativamente, se eu inserir 1.000 caracteres de informação, ou 50, o número *hash* terá sempre a mesma quantidade, de, suponhamos, 100 caracteres. Além disso, cada informação inserida (*input*) possuirá um código *hash* diferente e específico (*output*), como uma assinatura digital. Dessa forma, a cada caractere inserido, retirado ou modificado, seja um espaço, uma letra, um número ou um símbolo, o código mudará completamente.

Existem ferramentas que simulam algoritmos de *hashing*, como o SHA-256, que é utilizado no Bitcoin[29]. Nas figuras abaixo, utilizando uma dessas ferramentas, é possível verificar como o processo funciona. Na primeira, é inserida a palavra "Blockchain", com a letra inicial maiúscula.

Figura 1 - Exemplo de *hash* através do algoritmo SHA256.



Fonte: elaborada pelo próprio autor através do site Online Tools[30].

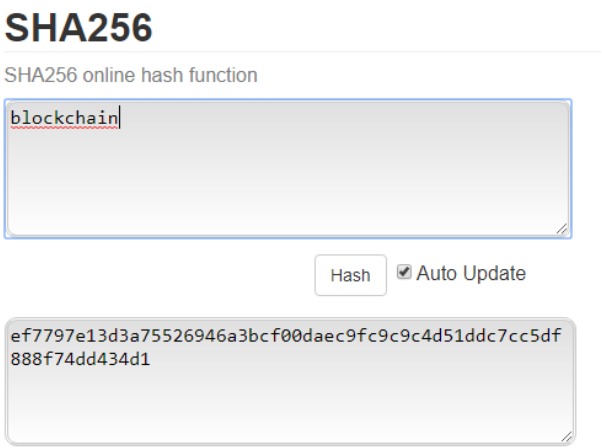
[28] O número de caracteres do *hash*, bem como se ele possuirá números ou letras é definido na elaboração do algoritmo. BINANCE ACADEMY. **O que é hashing?**. Disponível em: https://www.binance.vision/pt/security/what-is-hashing. Acesso em: 26 nov. 2019.

[29] O SHA-256 possui *output* de 256 bits, ou 64 caracteres. BINANCE ACADEMY. **O que é hashing?**. Disponível em: https://www.binance.vision/pt/security/what-is-hashing. Acesso em: 26 nov. 2019.

[30] ONLINE TOOLS. **SHA256**. Disponível em: https://emn178.github.io/online-tools/sha256.html. Acesso em: 26 nov. 2019.

Na segunda figura, a mesma palavra é inserida com o caractere inicial minúsculo:

Figura 2 - Exemplo de *hash* através do algoritmo SHA256.

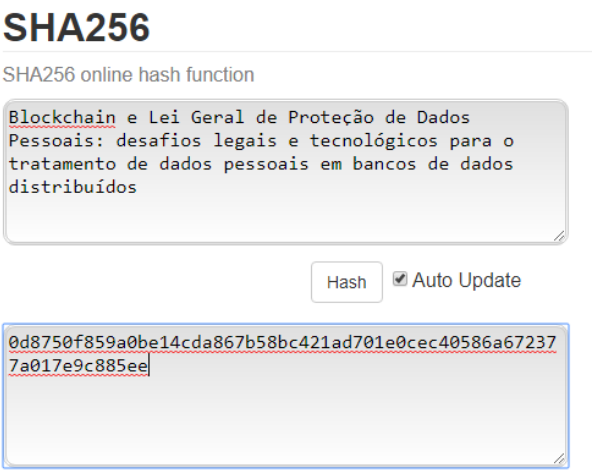


Fonte: elaborada pelo próprio autor através do site Online Tools[31].

Nota-se como os códigos *hash* são bastante distintos, e mantém o mesmo número de caracteres. Mesmo alterando um único caractere, toda a sequência é completamente alterada. Ainda, na terceira figura, insere-se o título completo da presente pesquisa, a fim de demonstrar a manutenção do número de caracteres:

[31] ONLINE TOOLS. **SHA256**. Disponível em: https://emn178.github.io/online-tools/sha256.html. Acesso em: 26 nov. 2019.

Figura 3 - Exemplo de *hash* através do algoritmo SHA256.



Fonte: elaborada pelo próprio autor através do site Online Tools[32].

Nesse caso, o processo de *hash* é feito de forma a não ser possível realizar a sua reversão e descobrir as informações que o geraram[33]. É uma transformação unilateral. Contudo, sempre que a mesma informação for inserida, o *output* (*hash*) será o mesmo[34]. O propósito do processo de *hashing* é, portanto, verificar a precisão e a integridade dos dados. Sempre que o código gerado for o mesmo, garante-se que as informações permanecem as mesmas. Ademais, é possível comprovar a autenticidade de uma mensagem apenas mostrando o *hash* gerado por ela, não sendo necessário divulgar as informações nela contidas (isso é o que ocorre, normalmente, quando sites armazenam senhas pessoais dos usuários)[35].

Para fins exemplificativos, imagine-se que a primeira caixa das figuras acima seja um bloco onde estão sendo inseridas as informações da

[32] *Ibidem*.

[33] HUMBEECK, Andries Van. The Blockchain-GDPR paradox. **Journal of Data Protection & Privacy**, v. 2, nº 3, p. 208–212. Disponível em: https://www.henrystewartpublications.com/jdpp/v2. Aceso em: 28 nov. 2019.

[34] BINANCE ACADEMY. **O que é hashing?**. Disponível em: https://www.binance.vision/pt/security/what-is-hashing. Acesso em: 26 nov. 2019.

[35] *Ibidem*.

blockchain (por exemplo, os registros de propriedade imobiliária de uma cidade). Quando determinado número de registros for inserido, o bloco será finalizado, e um *hash* específico àquelas informações inseridas (incluindo datas, horas, descrições, etc.) será gerado.

Aqui ocorre o processo que dá nome à *blockchain*: a chamada *hash chain*. Ao iniciar o próximo bloco, a primeira informação inserida é o *hash* do bloco anterior. Portanto, parte das informações que gerarão o *hash* do bloco seguinte é o próprio *hash* do bloco anterior. Dessa forma, todos os blocos ficam interligados sucessivamente, o que garante que todas as informações que foram inseridas nos blocos de informação anteriores permanecem as mesmas. Caso se tente alterar uma informação contida em um bloco anterior, o *hash* dele também será modificado, e, consequentemente, todos os *hashes* dos blocos posteriores serão modificados. Evidentemente, essa situação será constatada pelos nós (*nodes*, ou mineradores), que não validarão a modificação. Em uma *blockchain* real, o *hashing* é feito de forma mais frequente, mas, para o exemplo, basta ter em mente a situação mencionada no presente parágrafo.

Convém ressaltar que, uma vez que a possibilidade de informações a serem inseridas (*input*) são infinitas, mas os *outputs* são finitos, é possível que dois *inputs* diferentes resultem no mesmo *hash* (fenômeno chamado de "colisão"). Contudo, a probabilidade é extremamente baixa, e os algoritmos de *hash* considerados seguros à colisão, como o SHA-256, exigem "milhões de anos de cálculos computacionais" para que uma falha seja encontrada[36]. Ademais, apesar de não ser possível a reversão do *hash* para obter as informações inseridas, é possível, através de tentativa e erro, inserir dados até que se encontre o mesmo *output*, descobrindo-se a

[36] BINANCE ACADEMY. **O que é hashing?**. Disponível em: https://www.binance.vision/pt/security/what-is-hashing. Acesso em: 26 nov. 2019.

informação original. Contudo, os algoritmos de *hashing* também visam ser seguros quanto ao problema, chamado de "resistência à pré-imagem"[37].

Entendido o processo de *hashing*, passa-se a estudar a forma como se dá a validação e o consenso que permitem a continuidade e a segurança de uma *blockchain*. Nesse ponto, relembra-se que uma *blockchain* é *distribuída*, *pública* e *criptografada*. Não há uma base de dados, ou uma autoridade, central, mas os registros são "criados e carregados por cada nó de forma independente"[38]. As informações são compartilhadas entre todos os nós da rede, e dependem do consenso entre eles para sua validação.

Uma vez que as *blockchains* públicas não dependem de uma autoridade central, os computadores da rede "precisam concordar na validação das transações" [39]. Essa validação se dá através de "algoritmos de consenso", que "garantem que as regras do protocolo estão sendo seguidas e que todas as transações ocorrem de forma confiável"[40]. Existem diferentes tipos de algoritmos de consenso, sendo os principais o "*Proof of Work*" (PoW, "prova-de-trabalho") e o "*Proof of Stake*" (PoS, "prova de participação"). Importa mencionar que isso faz parte de uma ciência chamada "criptoeconomia", que, através de incentivos econômicos e criptografia, pretende regular o comportamento dos participantes[41].

O primeiro (prova-de-trabalho, em tradução livre), utilizado no Bitcoin, valida os blocos em que mais for exercido trabalho computacional:

---

[37] *Ibidem.*

[38] TEIXEIRA, Tarcisio; RODRIGUES, Carlos Alexandre. **Blockchain e Criptomoedas**. Salvador: Editora JusPodivm, 2019. p. 15.

[39] BINANCE ACADEMY. **O Que São os Algoritmos de Consenso das Blockchains?**. Disponível em: https://www.binance.vision/pt/blockchain/what-is-a-blockchain-consensus-algorithm. Acesso em: 28 nov. 2019.

[40] *Ibidem.*

[41] *Idem.* **A Beginner's Introduction to Cryptoeconomics**. Disponível em: https://www.binance.vision/economics/a-beginners-introduction-to-cryptoeconomics. Acesso em: 28 nov. 2019.

há um custo de energia despendido para formar o bloco, o que evita a geração de blocos desnecessários ou incorretos. Os mineradores (assim chamados, no caso do Bitcoin, pelo fato de serem recompensados pelo serviço com novas unidades da moeda) empenham poder computacional para, de uma lista de transações ainda não confirmadas (chamada de "*mining pool*" – aqui ficam as transações e informações que acabaram de ser enviadas para a rede, e aqui permanecem até sua validação), juntá-las em pares, formando um *hash* de cada par; os *outputs* são novamente juntados em pares em novos *hashes* até que somente um *hash* final seja produzido[42]. Esse processo se chama "Árvore de Merkle", que é uma forma de organizar grandes quantidades de dados. O número/*hash* final se chama "raiz de Merkle"[43]. Esse *hash* é, então, juntado com o *hash* do bloco anterior e com um número pseudoaleatório chamado "*nonce*", bem como com outras variáveis[44]. Um novo *hash* é feito dessa combinação, formando um bloco "candidato".

Entretanto, o minerador só terá sucesso, e o bloco somente será confirmado, se o *hash* do bloco candidato iniciar com um certo número de zeros, definido pelo protocolo[45]. Trata-se de um processo baseado em tentativa e erro, e vários processos de *hash* precisam ser feitos com diferentes *nonces* gerados pelo minerador, até que se encontre um resultado válido. A figura abaixo demonstra o processo de hashing das transações até a raiz de Markle, que, em conjunto com a hash do bloco anterior e o *nonce*, forma o *hash* final do bloco candidato.

---

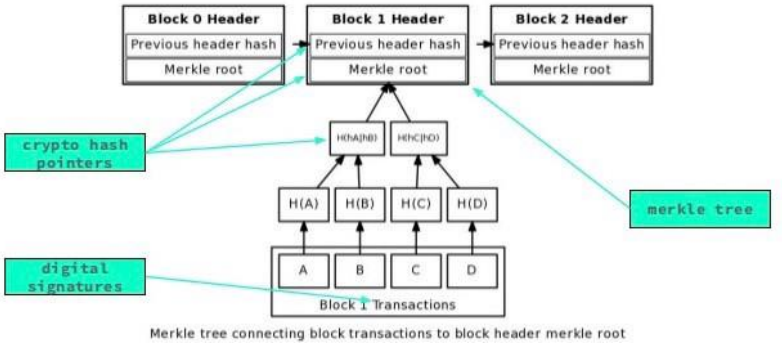
[42] BINANCE ACADEMY. **Mining**. Disponível em: https://www.binance.vision/glossary/mining. Acesso em: 28 nov. 2019.

[43] *Idem*. **Merkle Tree**. Disponível em: https://www.binance.vision/glossary/merkle-tree. Acesso em: 02 dez. 2019.

[44] Para mais detalhes, ver: *Idem*. **Nonce**. Disponível em: https://www.binance.vision/glossary/nonce. Acesso em: 28 nov. 2019.

[45] BINANCE ACADEMY. **Mining**. Disponível em: https://www.binance.vision/glossary/mining. Acesso em: 28 nov. 2019.

Figura 4 - Ilustração de formação de um bloco em uma blockchain.



Fonte: KOZLINER, Evan. Merkle Tree Introduction[46].

Frise-se que, no Bitcoin, a probabilidade é aumentada ou diminuída pelo protocolo (aumentando ou diminuindo a quantidade de zeros), conforme o poder computacional no momento em toda a rede, de forma a manter o tempo médio de mineração de cada bloco em dez minutos[47]. A título exemplificativo, no Bitcoin cada bloco tem no máximo 1 megabyte de informação, e as validações variaram de 1.425 a 2.763 transações por bloco até o presente momento[48].

Quando um bloco é validado (isso é, um minerador encontra um bloco cujo *hash* é menor do que o número determinado pelo protocolo), o *hash* correto funciona como uma "prova" do trabalho realizado: foi exercido tanto poder de processamento, e despendida tanta energia elétrica, que o *hash* correto foi encontrado. Assim, os outros nós da rede, confirmando o valor gerado pelo bloco, validam-no, e passam a trabalhar no bloco seguinte, utilizando o bloco validado como antecessor. Caso o bloco validado contenha informações diferentes das constantes nas cópias

[46] KOZLINER, Evan. **Merkle Tree Introduction**. Disponível em: https://medium.com/hackernoon/merkle-tree-introduction-4c44250e2da7. Acesso em: 01 dez. 2019.

[47] BINANCE ACADEMY. **Mining**. Disponível em: https://www.binance.vision/glossary/mining. Acesso em: 28 nov. 2019.

[48] BLOCKCHAIN. **Average Number Of Transactions Per Block**. Disponível em: https://www.blockchain.com/en/charts/n-transactions-per-block. Acesso em: 01 dez. 2019.

da *blockchain* dos outros mineradores, o *hash* será diferente, e o bloco não será confirmado, continuando-se os cálculos até que um bloco candidato seja validado pela rede.

Como visto, trata-se de um procedimento que demanda bastante recursos, e, para fraudar uma *blockchain* baseada nesse algoritmo de consenso, seria necessário um imenso poder computacional a fim de alterar as informações e validar cada bloco com as novas informações. Consequentemente, quanto mais antigo o bloco for, mais novos blocos precisam ser novamente validados até chegar ao bloco presente, demandando ainda maiores recursos. Em tese, seria necessário ter 51% do poder de processamento da rede para alterá-la (o que, por sua vez, demonstraria que mais "trabalho" estava sendo investido no bloco com informações adulteradas). Na prática, isso significa que, quanto maior o número de *nodes*, mais difícil é fraudar a rede[49]. Para se ter noção do quão difícil seria fraudar o Bitcoin, menciona-se que "a rede Bitcoin conta com força computacional de cerca de 2.000 PH/s (um *petahash* significa um quatrilhão de tentativas de cálculo da prova-de-trabalho por segundo)"[50].

O segundo algoritmo de consenso, normalmente traduzido para "prova de participação", não se baseia no maior poder computacional para validar as transações, mas em uma seleção parcialmente aleatória de quem será o validador[51]. Para se candidatar, o nó deverá "consignar" parte de suas moedas, as quais serão perdidas caso o usuário tente comprometer

[49] Convém mencionar a possibilidade de diferentes blocos válidos surgirem ao mesmo tempo, com informações distintas. É por isso que se deve aguardar a formação de novos blocos a fim de assegurar que a transação ou o registro foi realizado e confirmado com sucesso. Como visto, quanto mais blocos posteriores, mais segura está a informação inserida.

[50] ULRICH, Fernando. **Entendendo os riscos e a segurança do bitcoin**. Disponível em: https://www.infomoney.com.br/colunistas/moeda-na-era-digital/entendendo-os-riscos-e-a-seguranca-do-bitcoin/. Acesso em: 28 nov. 2019.

[51] BINANCE ACADEMY. **Proof of Stake**. Disponível em: https://www.binance.vision/pt/blockchain/proof-of-stake-explained. Acesso em: 28 nov. 2019.

ou alterar o bloco. Cada algoritmo estabelece critérios objetivos para a escolha do nó validador, como maior quantia armazenada, maior antiguidade da moeda consignada, etc. Por não depender de energia elétrica igual o método anterior, é tido como mais sustentável[52].

Diante da exposição técnica do funcionamento de uma *blockchain*, nota-se a razão pela qual as informações inseridas são, em tese, impossíveis de serem modificadas, visto que, caso haja alguma alteração nos dados inseridos, o *hash* também seria modificado, e todos os blocos posteriores teriam de ser revalidados com a nova informação – o que, como visto, seria um processo extremamente custoso. Assim, pelo menos em uma *blockchain* pública, tem-se que os dados inseridos permanecerão registrados enquanto ela existir. Contudo, na *blockchain* pública Ethereum, já foram realizados raros *forks*, isso é, modificações de blocos anteriores para reverter transações realizadas. Tais mudanças foram extremamente controladas, e nenhuma fraude ocorreu[53]. Assim, conclui-se que uma *blockchain* não é imutável no sentido pleno da palavra, mas que modificar as informações registradas demanda muitos recursos, o que, na prática, dependendo do tipo de *blockchain*, significa que modificações não serão feitas.

---

[52] CRUZ, Eduardo. **Formas de Mineração e Diferença entre: PoW, PoS, PoC**. Disponível em: https://medium.com/@eduardo.domc/formas-de-minera%C3%A7%C3%A3o-e-diferen%C3%A7a-entre-pow-pos-poc-22a3881195b5. Acesso em: 28 nov. 2019.

[53] DE LEON, Daniel Conte; SHELDON, Frederick.; JILLEPALLI, Ananth. **Blockchain: properties and misconceptions**. Disponível em: https://www.researchgate.net/publication/321811785_Blockchain_properties_and_misconceptions. Acesso em: 02 dez. 2019.

2.2 Tipos de blockchain e suas aplicações

Os conceitos acima debatidos se referem, especialmente, às "*blockchains* públicas" (ou sem necessidade permissão, "*permissionless blockchains*"), como o Bitcoin, em que qualquer pessoa pode acessar as informações da *blockchain*, realizar uma transação ou se tornar um nó validador de novos blocos. Podem ser feitas, contudo, *blockchains* baseadas em permissão (*permissioned blockchains*), que possuem uma camada a mais de controle: é possível restringir seu acesso ou quem serão os nós verificadores[54]. Nelas é possível determinar se todos, ou selecionados, podem visualizar os registros, bem como limitar os mineradores ou nós que realizam as verificações. Em palavras mais simples, a segunda se refere a um tipo de registro que está sob controle de um grupo limitado de pessoas, enquanto a primeira se traduz em uma *blockchain* que não está sob controle de ninguém, como a do Bitcoin e de outras moedas virtuais[55]. É também possível criar uma "*blockchain* privada", completamente restrita e limitada a uma organização central que exerce o controle e as validações, podendo seu conteúdo ser visto, ou não, por terceiros[56] - não há, aqui, algoritmos de consenso, visto que a autoridade central toma todas as decisões.

Em uma *permissioned blockchain*, em que o processo de consenso (a validação dos blocos) é controlado por um número pré-selecionado de nós, a leitura da *blockchain* pode ser pública ou restrita aos participantes, com variações a serem definidas conforme a necessidade de cada caso[57]. Ela

---

[54] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

[55] Retomando a analogia com o Google Docs, uma *blockchain* baseada em permissão poderia ser um documento que todos teriam a possibilidade de ler, porém somente pessoas selecionadas poderiam editá-lo. *Ibidem*.

[56] *Ibidem*.

[57] BUTERIN, Vitalik. **On Public and Private Blockchains**. Disponível em: https://ethereum.github.io/blog/2015/08/07/on-public-and-private-blockchains/. Acesso em: 30 nov. 2019.

também pode ser feita de forma a autorizar pessoas a entrarem após uma identificação ou autorização[58].

A título exemplificativo, um desenvolvedor de uma *permissioned blockchain* pode optar por deixar determinadas informações abertas ao público, como o nome de um produto e a quantidade envolvida na transação, mas limitar aos participantes a visualização dos preços ou valores[59]. Em uma *blockchain* baseada em consórcio (*consortium blockchain*), formada, digamos, por quinze instituições financeiras (que seriam os nós validadores), pode-se requerer que dez, de cada vez, validem cada bloco, e permitir aos consumidores que visualizem o histórico de transações[60]. Tudo isso controlado por essa camada a mais de controle. Assim, uma *permissioned blockchain* se torna um meio fácil e seguro de compartilhar informações confiáveis, assegurando a confiabilidade (utilizando as criptografias explicadas acima) que negócios necessitam para operar efetivamente[61]. Além dos dois algoritmos de consenso já explicados anteriormente, existem diversos outros que também podem ser utilizados (visto que os incentivos da criptoeconomia podem não ser necessários dependendo da confiança entre os nós), multiplicando as possibilidades de governança de uma *permissioned blockchain*, bem como diminuindo os custos de validação[62].

---

[58] FRANKENFIELD, Jake. **Permissioned Blockchains**. Disponível em: https://www.investopedia.com/terms/p/permissioned-blockchains.asp. Acesso em: 30 nov. 2019.

[59] *Ibidem*.

[60] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

[61] KADIYALA, Anant. **Nuances Between Permissionless and Permissioned Blockchains**. Disponível em: https://medium.com/@akadiyala/nuances-between-permissionless-and-permissioned-blockchains-f5b566f5d483. Acesso em: 01 dez. 2019.

[62] *Ibidem*.

Uma *permissioned blockchain* acaba conciliando as vantagens de uma *blockchain* pública e diminuindo outros riscos, visto que não existe risco de vazamento de dados ou de alterações em caso de um "ataque de 51%"[63], posto que os nós validadores são limitados e escolhidos previamente. Elas são utilizadas por empresas para facilitar o *compliance* e eventual auditoria, dado o registro confiável de todo o histórico, sem alterações[64]. Da mesma forma, bancos e hospitais, instituições cuja guarda do que ocorre é necessária, também podem se proteger de ataques a bancos de dados centrais ao salvar as informações em *blockchains* com acesso restrito. Por outro lado, *permissioned blockchains* não dispõem de um dos maiores trunfos da blockchain pública: sua descentralidade. Quanto menor o número de nós, menos difícil é adulterar os dados. Esse risco, contudo, é diminuído das formas expostas acima, bem como em *blockchains* de consórcio[65].

Um exemplo prático de uma *permissioned blockchain* em que várias entidades participam é o Medicalchain. Conforme disposto em seu *white-paper*[66], o Medicalchain é uma organização focada em armazenar, em um só local, todos os dados médicos referentes a uma pessoa. Ela permite aos pacientes acesso aos seus dados médicos de forma criptografada, os quais podem conceder permissões de escrita e leitura a médicos e a instituições de pesquisa ou de saúde de sua escolha.

Nesse mesmo sentido, *permissioned blockchains* também são consideradas como método para registros de propriedades, substituindo bancos

---

[63] BINANCE ACADEMY. **O que é um Ataque de 51%?**. Disponível em: https://www.binance.vision/pt/security/what-is-a-51-percent-attack. Acesso em: 01 dez. 2019.

[64] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

[65] *Ibidem*.

[66] MEDICALCHAIN. **Whitepaper 2.1**. Disponível em: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf. Acesso em: 01 dez. 2019.

de dados centralizados[67]. Nesse último caso, *blockchains* privadas são utilizadas para armazenar dados pessoais do proprietário, enquanto uma *blockchain* pública faz o registro dos títulos das propriedades[68], diminuindo a possibilidade de fraudes, os custos e permitindo que transferências ocorram em até dez minutos, como no caso da Geórgia[69].

Tratando-se de um registro seguro e descentralizado de informações, pessoas ao redor do globo têm procurado aplicar a *blockchain* em outros ramos. Cite-se um dos mais visionados atualmente, os chamados *smart contracts*, contratos inteiros que podem ser realizados com base nessa tecnologia. O conceito de contratos inteligentes foi criado em 1994, por Nick Szabo, que o definiu como "uma transação computadorizada que executa os termos de um contrato"[70], em tradução livre. Ele explica, em outro artigo[71], que vários tipos de cláusulas contratuais podem ser incorporados a um software e hardware, tornando desvantajoso (para o faltoso), ou impossível, descumpri-las. Ele traça sua origem às máquinas de vendas de refrigerante, nas quais uma pessoa deposita uma moeda (cumprindo a previsão contratual), e a máquina, automaticamente, dispensa o produto. Torna-se, portanto, desnecessária a presença de um intermediário confiável (como o Estado, ou uma imobiliária) gerenciando os contratos.

---

[67] GRAGLIA, J. Michael; MELLON, Christopher. Blockchain and property in 2018: At the End of the Beginning. **Innovations**, v. 12, nº 1/2. Disponível em: https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00270. Acesso em: 01 dez. 2019.

[68] *Ibidem.*

[69] NIMFUEHR, Marcell. **Blockchain application land register: Georgia and Sweden leading**. Disponível em: https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa980170c. Acesso em: 01 dez. 2019.

[70] SZABO, Nick. **Smart Contracts.** 1994. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Acesso em: 28 nov. 2019.

[71] *Idem*. **The Idea of Smart Contracts**. 1997. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html. Acesso em: 28 nov. 2019.

Trazendo-os para o contexto, contratos inteligentes são possíveis de serem realizados quando armazenados em uma *blockchain*, e, quando determinada transação acontece (que pode ser um horário, evento ou uma cláusula pré-determinada), desencadeiam-se os eventos pré-programados[72]. Isso é possível graças aos elementos e as características já expostas.

Em suma, ainda que um pouco distante da realidade prática da população, a tecnologia *blockchain* é considerada por muitos como parte da Quarta Revolução Industrial[73], ao lado da Internet das Coisas e da Inteligência Artificial, tendo impacto semelhante ao do correio eletrônico[74]. Estima-se que a *blockchain* possa revolucionar os tradicionais registros públicos[75], bancos[76], e até mesmo a forma de fazer contratos[77], por serem auto executáveis[78] e, de certa forma, imutáveis[79], dada sua base criptográfica e ligação por *hashing*. Já nos dias de hoje, a tecnologia *blockchain* está sendo utilizada em finanças, sistemas bancários, Internet das Coisas, manufatura, logística, manutenção de cadeias de fornecimento, visto ser um

[72] CHRISTIDIS, Konstantinos; DEVETSIKIOTIS, Michael. *Blockchain*s and Smart Contracts for the Internet of Things. *in* **IEEE Access**, vol. 4, p. 2292-2303, 2016. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408. Acesso em: 20 nov. 2019.

[73] POLLOCK, Daniel. **The Fourth Industrial Revolution Built On *Blockchain* And Advanced With AI**. 2018. Disponível em: https://www.forbes.com/sites/darrynpollock/2018/11/30/the-fourth-industrial-revolution-built-on-*blockchain*-and-advanced-with-ai/. Acesso em: 16 nov. 2019.

[74] NERY, Carmen. **Impacto do *blockchain* deve ser similar ao do correio eletrônico**. 2018. Disponível em: https://www.valor.com.br/empresas/5804359/impacto-do-*blockchain*-deve-ser-similar-ao-do-correio-eletronico. Acesso em: 16 nov. 2019.

[75] SHIN, Laura. **The First Government To Secure Land Titles On The Bitcoin *Blockchain* Expands Project**. 2017. Disponível em: https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-*blockchain*-expands-project. Acesso em: 16 nov. 2019.

[76] SÔNEGO, Dubes. **Por que o *blockchain* pode mudar radicalmente a forma de se fazer negócios**. 2017. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2017/05/por-que-o-*blockchain*-pode-mudar-radicalmente-forma-de-se-fazer-negocios.html. Acesso em: 16 nov. 2019.

[77] CHRISTIDIS, Konstantinos; DEVETSIKIOTIS, Michael. *Blockchain*s and Smart Contracts for the Internet of Things. *in* **IEEE Access**, vol. 4, p. 2292-2303, 2016. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408. Acesso em: 20 nov. 2019.

[78] ROSIC, Ameer. **Smart Contracts: The *Blockchain* Technology That Will Replace Lawyers**. 2016. Disponível em: https://blockgeeks.com/guides/smart-contracts/. Acesso em: 20 nov. 2019.

[79] MERCADO BITCOIN. **O que é um smart contract?**. 2018. Disponível em: https://blog.mercadobitcoin.com.br/o-que-%C3%A9-um-smart-contract-b91ac7b7f21f. Acesso em: 16 nov. 2019.

"excelente mecanismo para que múltiplas entidades compartilhem de uma mesma fonte confiável, consistente e verificável"[80]. Dessa forma, urge a possibilidade de conciliar essa tecnologia com as exigências legais.

[80] Tradução livre de: "Blockchain technologies are making inroads in finance, banking, Internet of things (IoT), manufacturing, logistics, supply chain management, and other domains — mainly because they offer an excellent mechanism for multiple entities to share one consistent, verified, tamper-resistant source of truth". KADIYALA, Anant. **Nuances Between Permissionless and Permissioned Blockchains**. Disponível em: https://medium.com/@akadiyala/nuances-between-permissionless-and-permissioned-blockchains-f5b566f5d483. Acesso em: 01 dez. 2019.

3

Análise das hipóteses de conflitos entre a legislação e a *blockchain*

O principal ponto de choque entre as exigências legais e tecnologias baseadas em *blockchain* é, possivelmente, a necessidade de excluir ou modificar determinado dado armazenado – o que, em um primeiro momento, é tido como impossível em determinados tipos de *blockchain*. Em razão disso, serão estudadas soluções jurídicas[1] e técnicas[2] para *blockchains* que permitam *compliance* com as exigências legais.

O termo *compliance*, originado na legislação norte-americana para se referir a programas de empresas que tinham a finalidade de criar procedimentos internos de controle e monitoramento de operações, é bastante recente no Brasil, senão para ambientes corporativos de setores altamente regulados, como as instituições financeiras, de saúde ou multinacionais[3]. Sua origem etimológica decorre do verbo inglês *to comply*, que significa "agir de acordo com a lei, uma instrução interna, um comando ou uma conduta ética"; em outras palavras, "estar em *compliance* é estar em conformidade com as regras internas da empresa, de acordo com procedimentos éticos e as normas jurídicas vigentes"[4]. Mais

[1] IBANEZ, Luis-Daniel; O'HARA, Kieron; SIMPERL, Elena. **On *Blockchain*s and the General Data Protection Regulation**. 2018. Disponível em: https://eprints.soton.ac.uk/422879/. Acesso em 14 jun. 2019.

[2] ATENIENSE, Giuseppe; MAGRI, Bernardo; VENTURI, Daniele; ANDRADE, Everton. **Redactable *Blockchain* – or – Rewriting History in Bitcoin and Friends**. 2017. Disponível em: https://eprint.iacr.org/2016/757.pdf. Acesso em: 11 jun. 2019.

[3] BERTOCCELLI, Rodrigo de Pinho. Compliance. *In*: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINO, Otavio (Orgs.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019. p. 35-54. Disponível em: Minha Biblioteca.

[4] BERTOCCELLI, Rodrigo de Pinho. Compliance. *In*: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINO, Otavio (Orgs.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019. p. 35-54. Disponível em: Minha Biblioteca.

extensivamente, pode ser compreendido como um "instrumento de mitigação de riscos, preservação dos valores éticos e de sustentabilidade corporativa, preservando a continuidade do negócio"[5].

No Brasil, a Lei nº 12.846, de 1º de agosto de 2013, conhecida como "Lei Brasileira Anticorrupção" ou "Lei da Empresa Limpa", que instituiu a "responsabilização objetiva administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira"[6], trouxe uma definição formal. Em seu artigo 7º, a Lei afirma que, na aplicação das sanções, será levado em consideração, dentre outras coisas, "a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica"[7]. Na presente pesquisa, foi utilizada a definição de *compliance* trazida por Vanessa Alessi Manzi:

> O termo *compliance* origina-se do verbo inglês *to comply*, que significa cumprir, executar, satisfazer, realizar algo imposto. *Compliance* é o ato de cumprir, de estar em conformidade e executar regulamentos internos e externos, impostos às atividades da instituição, buscando mitigar o risco atrelado à reputação e ao regulatório/legal[8].

Com a promulgação da Lei Geral de Proteção de Dados Pessoais, as empresas que lidam com tratamento de dados pessoais passaram a ter

---

[5] *Ibidem*.

[6] BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília: Presidência da República. 2013. Art. 1º. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 23 nov. 2019.

[7] BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília: Presidência da República. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 23 nov. 2019.

[8] MANZI, Vanessa Alessi. ***Compliance* no Brasil** – consolidação e perspectivas. São Paulo: Saint Paul, 2008, p. 15.

uma série de exigências legais a cumprir, assim como os titulares dos dados agora expressamente dispõem de direitos específicos relativamente aos dados cedidos aos agentes. É necessária, portanto, adaptação das formas como os dados são coletados e do modo de armazenamento deles, caso necessário, de forma a respeitar as disposições legais.

Conforme exposto anteriormente, de maneira global se tem buscado maior transparência sobre o uso e destinação dos dados pessoais dos indivíduos. Surgem legislações visando proteger tais dados e delimitar responsáveis para cumprirem determinações legais e judiciais. As mais notórias em nosso contexto, a LGPD e a GDPR, já mencionadas anteriormente, trazem diversos conceitos, direitos e responsabilidades aos titulares e aos agentes de tratamento dos dados pessoais coletados.

Ambas as legislações, a princípio, partem de um mesmo ponto em comum – que justifica a importância do presente estudo –, qual seja, a possibilidade de identificar (um) agente que se responsabilize e gerencie os dados registrados. Por outro lado, com o surgimento de tecnologias de registro distribuído, como a *blockchain*, pode haver dificuldades de adaptação às exigências legais[9].

Nesse ponto, convém destacar que *blockchain* não é sinônimo de banco de dados distribuídos (ou "*distributed ledger technology*" – DLT). Uma DLT se refere a formas de bancos de dados descentralizados (que não dependem de uma única autoridade central para intermediar, validar ou autenticar transações e registros)[10]. É, portanto, um gênero, da qual a *blockchain* é uma espécie. Dessa forma, uma DLT não necessariamente

[9] STEINBECK, Dean. **How New EU Privacy Laws Will Impact *Blockchain*: Expert Take.** 2018. Disponível em: https://cointelegraph.com/news/how-new-eu-privacy-laws-will-impact-*blockchain*-expert-take. Acesso em: 11 jun. 2019.

[10] BELIN, Oliver. **The Difference Between Blockchain & Distributed Ledger Technology**. Disponível em: https://tradeix.com/distributed-ledger-technology/. Acesso em: 01 dez. 2019.

funciona em uma cadeia de blocos (sendo essa uma característica da *blockchain*), sendo, antes disso, somente "um tipo de banco de dados distribuído entre diferentes lugares, regiões ou participantes"[11]. Assim, nem todos os conflitos legais aqui analisados necessariamente são aplicáveis a todos os bancos de dados distribuídos, mas sim àqueles que guardam similaridades com o processo de funcionamento de uma *blockchain*.

Doneda, em 2006, alguns anos antes da invenção da *blockchain*, ao tratar do fato de que grandes bancos de dados centralizados seriam grandes ameaças à privacidade, afirmou as vantagens dos registros distribuídos:

> Certamente o processamento distribuído "democratizou" esta arquitetura, fragmentando o tratamento de dados pessoais, porém as questões referentes aos grandes bancos de dado continuam pertinentes e presentes, por exemplo, mas discussões referentes à adoção de um número de identificação único ou de cartas de identidade digitais; além do que as vantagens em termos de desempenho e custos que proporciona a computação distribuída – grid computing – certamente contribuirão para tornar tais raciocínios ainda mais relativos e cinzentos[12].

Com o surgimento da *blockchain*, contudo, outros problemas podem aparecer, pelos fatos já expostos. Em um recente livro sobre *blockchain* e criptomoedas, Tarcisio Teixeira e Carlos Alexandre Rodrigues resumem duas possíveis incompatibilidades:

> Poderá vir a se tornar inviável, sob o ponto de vista jurídico, a responsabilização do titular do banco de dados, pois isto simplesmente deixa de existir: não há, na tecnologia blockchain, um titular único do banco de dados, eis que todos

[11] *Ibidem*.

[12] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 19.

> os nós da rede possuem as mesmas cópias. O mesmo vale para outros pontos que merecem reflexão, como a imutabilidade de registros: isto pode ser interessante na maioria dos casos em que se pretende transparência (pensemos numa aplicação blockchain voltada a licitações ou cartórios, como citado), mas também pode inviabilizar a aplicação do direito ao esquecimento em casos em que se discuta a inviolabilidade da vida privada, intimidade, honra, imagem e, de resto, nos valores da pessoa e da família, tudo previsto no art. 220, §1º, art. 221 e no §3º do art. 222 da CF/88[13].

Urge verificar, portanto, se, especialmente no caso brasileiro, a nova lei foi elaborada de forma apta a recepcionar tais tecnologias, ou se mudanças precisam ser feitas, seja do lado tecnológico, seja do lado jurídico. Em razão disso, o estudo do tema e sua relação com a legislação é de suma importância e prepara tanto o mercado quanto os legisladores para possíveis alterações que eventualmente precisem ser feitas, a fim de possibilitar *compliance* entre os envolvidos.

3.1 Hipóteses de conflito entre direitos do titular de dados pessoais armazendos em uma *blockchain*

Cumpre iniciar essa parte do estudo tendo em consideração que tanto a *blockchain* quanto as leis de proteção de dados possuem, em última análise, pelo menos alguns objetivos em comum, como transparência, integridade e precisão das informações. Entretanto, ainda que os objetivos sejam parecidos, uma interpretação restritiva da lei pode inviabilizar o armazenamento de dados pessoais em uma *blockchain*[14], como se verá.

---

[13] Os autores citam, ainda, o julgado do STJ no REsp 1.334.097/RS, de 28 de maio de 2013, que aborda o tema do Direito ao Esquecimento, inclusive no âmbito da Internet. TEIXEIRA, Tarcisio; RODRIGUES, Carlos Alexandre. **Blockchain e Criptomoedas**. Salvador: Editora JusPodivm, 2019. p. 15.

[14] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

Para isso, rememora-se três importantes direitos relativos à proteção de dados. O primeiro deles é o direito à retificação, previsto constitucionalmente no remédio do *habeas data* e também no Código de Defesa do Consumidor. Neste último é previsto que os consumidores têm o direito de solicitar correções em dados inexatos, pedido que deve ser atendido em até cinco dias úteis. Em relação ao *habeas data*, em seu regulamento é previsto que, caso "constatada a inexatidão de qualquer dado a seu respeito, o interessado, em petição acompanhada de documentos comprobatórios, poderá requerer sua retificação"[15]. O parágrafo primeiro do referido artigo estabelece, ainda, prazo de dez dias para cumprimento. Na LGPD, o artigo 18, III, garante ao titular o direito a "correção de dados incompletos, inexatos ou desatualizados", enquanto o inciso VI possibilita o requerimento de sua completa eliminação[16].

Convém mencionar, nessa mesma esteira, o direito ao esquecimento, consagrado pelo STJ e dedutível das normas já estudadas, pelo qual o titular tem o direito, no âmbito digital, em termos simples, "de ter suas informações pessoais desindexadas pelos buscadores da Internet, em especial, quando tais informações não forem corretas, relevantes ou atualizadas"[17]. Há, também, o direito à portabilidade dos dados a outro fornecedor de serviço ou produto[18].

---

[15] 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: Presidência da República. 1997. Art, 4º. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 20 nov. 2019.

[16] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

[17] BELLI Luca. **STJ consagra direito ao esquecimento na Internet**: o que isso significa?. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/stj-consagra-direito-ao-esquecimento-na-internet-o-que-isso-significa-20052018. Acesso em: 01 dez. 2019.

[18] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Art. 18, V. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

De maneira simples e direta, comparando tais direitos à forma como uma *blockchain* funciona, a conclusão que vem à mente é uma só: deve-se ter cuidado ao armazenar dados pessoais em uma *blockchain*, uma vez que o titular pode requerer sua alteração ou remoção, o que, a depender da *blockchain*, seria impraticável, gerando uma violação, por parte do agente de tratamento, à LGPD.

Jan Philipp Albrecht, membro do Parlamento Europeu até 2018 e um dos responsáveis pelo GDPR, afirmou que "certas tecnologias não serão compatíveis com o GDPR se, por causa de sua estrutura, não proverem aos titulares de dados os seus direitos"[19]. Ele afirma que não necessariamente a tecnologia *blockchain* é inconciliável com o GDPR, mas que, provavelmente, ela não poderá ser utilizada para processar dados pessoais, e que a decisão de utilizá-la ou não recai sobre cada organização que processa esse tipo de dado[20]. Conclui dizendo que, "do ponto de vista de uma *blockchain*, o GDPR já está desatualizado"[21].

Outro ponto de conflito, já antecipado por Tarcisio Teixeira e Carlos Alexandre Rodrigues, é a inexistência de um único agente de tratamento que possa ser responsabilizado, uma vez que, em razão da descentralidade do registro, dezenas, centenas ou milhares de nós estão processando dados conjuntamente, sem sequer se conhecerem (pelo menos no caso de uma *blockchain* pública). Em face disso, surgem diversos questionamentos[22]:

---

[19] Tradução livre de: "Certain technologies will not be compatible with the GDPR if they don't provide for [the exercising of data subjects' rights] based on their architectural design". MEYER, David. **Blockchain technology is on a collision course with EU privacy law**. Disponível em: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/. Acesso em: 25 nov. 2019.

[20] MEYER, David. **Blockchain technology is on a collision course with EU privacy law**. Disponível em: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/. Acesso em: 25 nov. 2019.

[21] *Ibidem.*

[22] Adaptados de: "Whether public or private, a blockchain is made up of many, many, different nodes, Does each node need to be GDPR compliant? If so, who is responsible for ensuring each node is GDPR-compliant? In the event of a personal data breach, what is the appropriate jurisdiction and applicable law? Just to make things more complicated, how will EU regulators view (and answer) such issues?". KULIK, Tom. **Why Blockchain And The**

todos os nós precisa estar em *compliance* com a LGPD? Se sim, quem seria responsável por garantir que cada nó aja de acordo com ela? Caso ocorra algum vazamento de dados, qual seria a jurisdição ou a lei aplicável, caso existam nós de diferentes partes do mundo? A tais perguntas ainda não existem respostas satisfatórias.

A LGPD testifica, em seu artigo 3º, sua aplicação a qualquer operação de tratamento de dados: realizada no território nacional (inciso I); que tenha por objetivo a oferta ou fornecimento de bens ou serviços no território nacional (inciso II); se de dados de indivíduos localizados no território nacional (inciso II); se os dados foram coletados no Brasil (inciso III)[23]. Entretanto, caso apenas um nó esteja localizado no Brasil (enquanto centenas de outros se encontram em outros países), e os dados se refiram a estrangeiros, a LGPD também seria aplicada? Essa é uma pergunta ainda sem resposta, diante da desconsideração expressa pelas legislações dos bancos de dados distribuídos. Inicialmente, a conclusão que se pode chegar é que sim, uma vez que realmente os dados estão sendo tratados no Brasil; contudo, tendo em mente que os mesmos dados também estão sendo tratados em outros países, o conflito de normas se intensifica. Esse problema, contudo, é melhor contornável em *blockchains* privadas ou baseadas em autorização.

Há de se ter em mente, também, quais informações se caracterizam como dados pessoais para o escopo de incidência da LGPD. Para isso, duas coisas. Primeiro, frise-se a existência de três formas de armazenar dados em uma *blockchain*: como texto simples, através de criptografia e após o

GDPR Collide Over Your Personal Data. Disponível em: https://abovethelaw.com/2018/10/why-blockchain-and-the-gdpr-collide-over-your-personal-data/. Acesso em: 01 dez. 2019.

[23] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Art. 3º. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

processo de *hashing*[24]. Segundo, ressalta-se os dois tipos de informações existentes referentes a um usuário de uma *blockchain*: sua chave pública (da criptografia assimétrica), que é seu endereço, e as informações propriamente ditas, que são transferidas, armazenadas, etc. ("*transactional data*"[25]).

Isso posto, analisa-se as alternativas. Considerando que os dados armazenados de forma pura, ou simples, permitem a identificação de seu titular, aplica-se a LGPD, caso as informações sejam da categoria protegida legalmente. Se armazenados após criptografia, ainda assim é possível seu acesso mediante o uso de uma chave (há, portanto, a pseudonimização dos dados), razão pela qual não são considerados dados anônimos – há, portanto, a incidência da LGPD[26]. A respeito das chaves públicas, elas também podem ser consideradas como dados pessoas para fins da LGPD, uma vez que é possível associá-la a determinado usuário, sendo, afinal, seu "endereço". A conclusão decorre da semelhança com o endereço IP, tido como dado pessoal pelos tribunais europeus[27].

A questão mais difícil de ser respondida é se dados pessoais após o processo de *hashing* são considerados anônimos ou pseudonimizados, sendo a pseudonimização o "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão

[24] RABELO, Maria. **Os desafios do RGPD perante as novas tecnologias *blockchain***. 2019. Disponível em: http://revistes.ub.edu/index.php/RBD/article/view/27066. Acesso em: 14 jun. 2019.

[25] FINCK, Michèle. ***Blockchains* and Data Protection in the European Union**. 2018. Disponível em: https://edpl.lexxion.eu/data/article/12327/pdf/edpl_2018_01-007.pdf. DOI: https://doi.org/10.21552/edpl/2018/1/6. Acesso em 12 jun. 2019.

[26] RABELO, Maria. **Os desafios do RGPD perante as novas tecnologias *blockchain***. 2019. Disponível em: http://revistes.ub.edu/index.php/RBD/article/view/27066. Acesso em: 14 jun. 2019.

[27] *Ibidem.*

pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro"[28]. A diferença é que no primeiro caso a LGPD não seria aplicada, enquanto no segundo caso, sim, visto ainda ser possível associar, direta ou indiretamente, o dado ao seu titular.

Considerando que essa regra é bastante semelhante à previsão europeia, convém verificar a conclusão à qual a jurisprudência europeia chegou. Segundo Maria Paula Rebelo[29], a interpretação restritiva da norma, atualmente adotada naquele contexto, classifica uma informação após o processo de *hashing* como pseudonimizada, e não como anônima. A conclusão decorre do fato de que, apesar de o *hash* não permitir a reversão, ainda existe uma ligação do *hash* (que contém a informação) até seu titular, bem como da possibilidade de, através de tentativa e erro, encontrar a informação original pela comparação de *hashes*[30]. Apesar de improvável, é possível a associação a um indivíduo, razão pela qual mesmo um dado que passou pelo processo de *hashing* continuaria sendo um dado pessoal nos termos da LGPD. Sendo considerado dados pessoais, todos os direitos e prerrogativas previstos na LGPD seriam aplicáveis e exigíveis. Em *blockchains* privadas ou baseadas em permissão, os direitos ao esquecimento e à retificação poderiam ser cumpridos. Contudo, em *blockchains* públicas, dado o esforço e o gasto considerável para cada alteração, não seria viável considerar como prática corriqueira a realização de alterações em dados pessoais armazenados[31]. Assim, a imutabilidade dessas bases de

[28] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República. 2018. Art. 13º. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

[29] RABELO, Maria. **Os desafios do RGPD perante as novas tecnologias *blockchain***. 2019. Disponível em: http://revistes.ub.edu/index.php/RBD/article/view/27066. Acesso em: 14 jun. 2019.

[30] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

[31] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241.

dados gera conflitos claros com a legislação, o que demanda a busca por soluções técnicas ou legislativas.

3.2 Possíveis soluções técnicas ou legislativas para os conflitos

Diante de tantos conflitos gerados pela imutabilidade de uma *blockchain*, convém, inicialmente, repisar ser, em tese, possível reescrever dados registrados em uma *blockchain*. A única condição é a de que a maioria dos nós validadores (a depender do algoritmo de consentimento) da rede concordem em criar uma nova versão da *blockchain* (*fork* ou *hard fork*) que inclua essa mudança, e então continuar a usar essa versão em vez da original – tendo de revalidar todos os blocos posteriores[32]. Em uma *blockchain* privada ou de autorização, pode ser uma solução viável[33]. Entretanto, em uma *blockchain* pública, trata-se de um evento de grandes proporções, sendo que, "pelo menos na forma atual da tecnologia, há pouco ou nenhum escopo para corrigir ou remover pedaços de informação de forma regular"[34].

Uma segunda possível solução técnica foi a criação de uma *permissioned blockchain* especial, com a possibilidade de reescrever blocos antigos. Nesse caso, mesmo alterando as informações de um bloco anterior, "quebrando" a *hash* da cadeia, um "*hash* camaleão" manteria a cadeia intacta[35]. Contudo, essa *hash*, na realidade, tornaria uma *blockchain* em apenas um

---

Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

[32] MEYER, David. **Blockchain technology is on a collision course with EU privacy law**. Disponível em: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/. Acesso em: 25 nov. 2019.

[33] BUTERIN, Vitalik. **On Public and Private Blockchains**. Disponível em: https://ethereum.github.io/blog/2015/08/07/on-public-and-private-blockchains/. Acesso em: 30 nov. 2019.

[34] Tradução livre de "At least as the technology is currently designed, there is little to no scope for fixing or removing bits of information here and there on an ongoing basis". MEYER, David. **Blockchain technology is on a collision course with EU privacy law**. Disponível em: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/. Acesso em: 25 nov. 2019.

[35] ACCENTURE. **Blockchain Redaction**. Disponível em: https://www.accenture.com/_acnmedia/pdf-44/accenture-blockchain-redaction-infographic.pdf. Acesso em: 01 dez. 2019.

banco de dados comum, perdendo todas as suas características que a tornam importante[36].

Outra saída, mais razoável, seria o armazenamento de dados pessoais em um banco de dados à parte da *blockchain*[37]: os *hashes* das informações são salvos na *blockchain* enquanto as informações em si, bem como uma cópia da *hash*, ficam armazenadas em outro local ("*off-chain*")[38]. Caso o titular queira exercer seu direito ao esquecimento ou a alterações, as informações guardadas fora da blockchain são excluídas ou alteradas, de forma que o *hash* presente na *blockchain* não terá utilidade, nem será passível de uso para identificação[39]. No caso de correção dos dados, um novo *hash* deverá ser gerado e inserido. Menciona-se, nesse sentido, que uma chave pública não poderia ser armazenada fora da *blockchain*, posto que essencial para as transações[40].

Todavia, esse método sacrifica muitos dos benefícios do uso de uma *blockchain*, especialmente o principal deles: a imutabilidade. A "*off-chain*" possui as mesmas características de um banco de dados regular, e o uso da *blockchain* nesse caso apenas tornaria o sistema mais complexo e ineficiente[41]. Da mesma forma, considerando que os dados não se encontram

---

[36] RABELO, Maria. **Os desafios do RGPD perante as novas tecnologias *blockchain***. 2019. Disponível em: http://revistes.ub.edu/index.php/RBD/article/view/27066. Acesso em: 14 jun. 2019.

[37] COELHO, Fábio André; YOUNES, George. **The GDPR-Blockchain paradox**: a work around. Disponível em: https://www.researchgate.net/publication/329656420_The_GDPR-Blockchain_paradox_a_work_around. Acesso em: 30 nov. 2019.

[38] HUMBEECK, Andries Van. The Blockchain-GDPR paradox. **Journal of Data Protection & Privacy**, v. 2, nº 3, p. 208–212. Disponível em: https://www.henrystewartpublications.com/jdpp/v2. Aceso em: 28 nov. 2019.

[39] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

[40] RABELO, Maria. **Os desafios do RGPD perante as novas tecnologias *blockchain***. 2019. Disponível em: http://revistes.ub.edu/index.php/RBD/article/view/27066. Acesso em: 14 jun. 2019.

[41] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

na *blockchain*, não é possível ter certeza de quem de fato tem acesso a esses dados, o que não ocorre em uma *permissioned blockchain*, em que a transparência é maior[42]. Por fim, caso o entendimento de que *hashes* continuam sendo considerados dados pessoais, nem mesmo essa solução seria possível.

Do ponto de vista legal, a saída momentânea pode ser uma interpretação menos restritiva das normas. Caso seja realizada uma interpretação mais extensiva do direito à exclusão dos dados, por exemplo, o *compliance* seria possível caso se considerasse que o dado foi excluído ao limitar o direito de acesso a ele. Em uma *permissioned blockchain* seria possível limitar o acesso ao dado somente ao titular, impedindo que terceiros tenham acesso[43]. Caso se interprete tal fato como uma eliminação, seria possível o *compliance*.

Da mesma maneira, uma interpretação menos restrita de uma informação armazenada por *hashing*, que considerasse que a intenção da norma era proteger os dados e não tanto a quem eles se referem, bem como pela extrema dificuldade em achar um hash idêntico, considerando-a anônima, permitiria o armazenamento de dados pessoais através desse processo[44]. Tratar-se-ia de uma situação em que, comparando as vantagens do armazenamento de determinados dados em uma *blockchain* e a ínfima possibilidade de descobri-los, haveria o favorecimento à interpretação menos restritiva.

---

[42] *Ibidem*.

[43] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

[44] *Ibidem*.

A respeito da responsabilização dos agentes de tratamento, poder-se-ia onerar o criador da *blockchain*, visto que ele é quem constrói os algoritmos e a maior ou menor compatibilidade com as previsões legais[45]. Entretanto, tal figura nem sempre é identificável, como no caso do criador do Bitcoin, cuja identidade é desconhecida.

As soluções definitivas, e futuras, para o *compliance* no caso brasileiro são as mesmas mencionadas por Anisha Mirchandani em seu artigo "The GDPR-Blockchain Paradox"[46]. A primeira, seria a inclusão expressa na lei da possibilidade de armazenamento de dados pessoais em *blockchains* baseadas em permissão, excetuando a obrigatoriedade do agente de tratamento de deletar ou alterar os dados pessoais do titular de uma *blockchain*. A segunda, seria um tipo específico de consenso para armazenamento de dados em uma *blockchain*, cientificando os titulares da impossibilidade, ou severa dificuldade, de alteração. Do ponto de vista dos objetivos da LGPD, em que a lei visa garantir ao titular o controle sobre seus dados, e contanto que a *blockchain* respeite padrões de segurança e transparência, inexistiria outra afronta direta que não as referentes à alteração e exclusão.

Em terceiro lugar, poderia haver uma clarificação do significado de "eliminação" dos dados, tornando possível considerá-lo eliminado caso houvesse a restrição de seu acesso. Da mesma maneira, caso informações que passem por *hashing* também fossem consideradas anonimizadas, também haveria abertura para armazenamento de dados pessoais em *blockchain* sem violação da LGPD.

---

[45] RABELO, Maria. **Os desafios do RGPD perante as novas tecnologias *blockchain***. 2019. Disponível em: http://revistes.ub.edu/index.php/RBD/article/view/27066. Acesso em: 14 jun. 2019.

[46] MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

Até lá, a solução para a conformidade permanece na utilização de *blockchains* privadas ou baseadas em permissão, que conseguem conciliar melhor a segurança e a confiabilidade da tecnologia com o respeito à privacidade e aos direitos dos titulares.

Conclusão

Conclui-se que a Lei Geral de Proteção de Dados Pessoais não previu a hipótese de armazenamento em bancos de dados distribuídos, e há, do ponto de vista legal, total incompatibilidade com a guarda de dados pessoais em uma *blockchain* pública, visto que o titular dos dados estaria impossibilitado de exercer diversos dos seus direitos.

Em uma *blockchain* pública, a realização de alterações em blocos antigos é um evento raro, que envolve a movimentação de grandes recursos, dependendo do algoritmo de consenso utilizado. Ademais, a alteração de blocos validados não é algo desejável em uma *blockchain*, visto que esse processo gera insegurança às transações já efetuadas. Por tais razões, dados pessoais não devem ser armazenados em *blockchains* públicas, sob pena de estes ficarem em desacordo com as disposições e diretrizes previstas na Lei Geral de Proteção de Dados Pessoais brasileira.

Em relação às *blockchains* privadas ou baseadas em permissão, a criação de novas versões a cada vez que uma alteração for necessária é menos custosa e relativamente mais simples, pois os nós validadores são conhecidos e em número mais limitado.

A saída técnica mais viável no presente momento seria o armazenamento dos dados pessoais em um registro à parte (*off-chain*), possível de ser modificado ou excluído, vinculado a uma *hash* que permanece na *blockchain*, mantendo o vínculo. Contudo, caso seja interpretado que dados após o processo de *hashing* não são dados anonimizados, a mera permanência do *hash* em uma *blockchain* também violaria a LGPD.

As saídas mais seguras envolveriam alterações legislativas, com previsões específicas para bancos de dados distribuídos e/ou registros que não seriam passíveis de modificação.

Da mesma forma, a multiplicidade de agentes de tratamento concomitantes em um banco de dados distribuído gera dúvidas a respeito de quem seria o responsável legal por tornar o tratamento compatível com a legislação. A resposta mais acertada, até o momento, seria apontar para o criador do protocolo, que estabelece as bases para que a *blockchain* funcione mais ou menos de acordo com as orientações legais. Entretanto, em situações nas quais não se é possível estimar quem seria o criador, se esse não possui mais nenhuma gerência sobre o protocolo ou se a *blockchain* foi criada sob outra legislação, é impossível, no presente momento, entender quem seria o responsável – nessa situação, dá-se a entender que todos os que estão realizando o tratamento seriam responsáveis.

Verifica-se, assim, uma vez mais, que a lei nunca está ao mesmo tempo da sociedade. A existência de bancos de dados distribuídos, ainda que presentes há décadas, foi completamente desconsiderada pelo legislador. Como mencionado anteriormente, a Lei Geral de Proteção de Dados (LGPDP), assim como o GDPR, busca regular um mundo centralizado de dados, ignorando as formas alternativas descentralizados de tratamento. Em razão disso, conclui-se pela terceira hipótese, em que, atualmente, há parcial recepção, visto que *blockchains* privadas ou baseadas em permissão conseguem assegurar a proteção dos direitos dos titulares sem perder as principais características positivas que levaram a tecnologia ao sucesso. Contudo, *blockchains* públicas, em razão de sua imutabilidade e ausência de responsáveis, não estão em conformidade ao armazenar dados pessoais.

Referências

ACCENTURE. **Blockchain Redaction**. Disponível em: https://www.accenture.com/_acnmedia/pdf-44/accenture-blockchain-redaction-infographic.pdf. Acesso em: 01 dez. 2019.

ASSEMBLEIA GERAL DA ONU. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 13 nov. 2019.

ATENIENSE, Giuseppe; MAGRI, Bernardo; VENTURI, Daniele; ANDRADE, Everton. **Redactable *Blockchain* – or – Rewriting History in Bitcoin and Friends**. 2017. Disponível em: https://eprint.iacr.org/2016/757.pdf. Acesso em: 11 jun. 2019.

BARRETO JUNIOR, Irineu Francisco; FAUSTINO, André. **Aplicativos de serviços para saúde e proteção dos dados pessoais de usuários**. p. 298. Revista Jurídica. vol. 01, nº. 54, Curitiba, 2019. DOI: 10.6084/m9.figshare.7841105.

BELIN, Oliver. **The Difference Between Blockchain & Distributed Ledger Technology**. Disponível em: https://tradeix.com/distributed-ledger-technology/. Acesso em: 01 dez. 2019.

BELLI, Luca. **STJ consagra direito ao esquecimento na Internet**: o que isso significa?. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/stj-consagra-direito-ao-esquecimento-na-internet-o-que-isso-significa-20052018. Acesso em: 01 dez. 2019.

BERTOCCELLI, Rodrigo de Pinho. Compliance. *In*: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINO, Otavio (Orgs.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019. p. 35-54. Disponível em: Minha Biblioteca.

BINANCE ACADEMY. **A Beginner's Introduction to Cryptoeconomics**. Disponível em: https://www.binance.vision/economics/a-beginners-introduction-to-cryptoeconomics. Acesso em: 28 nov. 2019.

BINANCE ACADEMY. **Encryption**. Disponível em: https://www.binance.vision/glossary/encryption. Acesso em: 30 nov. 2019.

BINANCE ACADEMY. **Merkle Tree**. Disponível em: https://www.binance.vision/glossary/merkle-tree. Acesso em: 02 dez. 2019.

BINANCE ACADEMY. **Mining**. Disponível em: https://www.binance.vision/glossary/mining. Acesso em: 28 nov. 2019.

BINANCE ACADEMY. **Nonce**. Disponível em: https://www.binance.vision/glossary/nonce. Acesso em: 28 nov. 2019.

BINANCE ACADEMY. **O que é hashing?**. Disponível em: https://www.binance.vision/pt/security/what-is-hashing. Acesso em: 26 nov. 2019.

BINANCE ACADEMY. **O que é um Ataque de 51%?**. Disponível em: https://www.binance.vision/pt/security/what-is-a-51-percent-attack. Acesso em: 01 dez. 2019.

BINANCE ACADEMY. **O Que São os Algoritmos de Consenso das Blockchains?**. Disponível em: https://www.binance.vision/pt/blockchain/what-is-a-blockchain-consensus-algorithm. Acesso em: 28 nov. 2019.

BINANCE ACADEMY. **Proof of Stake**. Disponível em: https://www.binance.vision/pt/blockchain/proof-of-stake-explained. Acesso em: 28 nov. 2019.

BINANCE ACADEMY. **Symmetric vs. Asymmetric Encryption**. Disponível em: https://www.binance.vision/security/symmetric-vs-asymmetric-encryption. Acesso em: 30 nov. 2019.

BLOCKCHAIN. **Average Number Of Transactions Per Block**. Disponível em: https://www.blockchain.com/en/charts/n-transactions-per-block. Acesso em: 01 dez. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 nov. 2019.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2000**. Institui o Código Civil. Brasília: Presidência da República. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 13 nov. 2019.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília: Presidência da República. 2013. Art. 1º. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 23 nov. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jun. 2019.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 20 nov. 2019.

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: Presidência da República. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 20 nov. 2019.

BUTERIN, Vitalik. **On Public and Private Blockchains**. Disponível em: https://ethereum.github.io/blog/2015/08/07/on-public-and-private-blockchains/. Acesso em: 30 nov. 2019.

CHRISTIDIS, Konstantinos; DEVETSIKIOTIS, Michael. *Blockchain*s and Smart Contracts for the Internet of Things. *in* **IEEE Access**, vol. 4, p. 2292-2303, 2016. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408. Acesso em: 20 nov. 2019.

COELHO, Fábio André; YOUNES, George. **The GDPR-Blockchain paradox**: a work around. Disponível em: https://www.researchgate.net/publication/329656420_The_GDPR-Blockchain_paradox_a_work_around. Acesso em: 30 nov. 2019.

CONSELHO DA EUROPA. Convenção Europeia dos Direitos do Homem. Roma, 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 13 nov. 2019.

CRUZ, Eduardo. **Formas de Mineração e Diferença entre: PoW, PoS, PoC**. Disponível em: https://medium.com/@eduardo.domc/formas-de-minera%C3%A7%C3%A3o-e-diferen%C3%A7a-entre-pow-pos-poc-22a3881195b5. Acesso em: 28 nov. 2019.

DE LEON, Daniel Conte; SHELDON, Frederick.; JILLEPALLI, Ananth. **Blockchain: properties and misconceptions**. Disponível em: https://www.researchgate.net/publication/321811785_Blockchain_properties_and_misconceptions. Acesso em: 02 dez. 2019.

DI PIETRO, Maria Zanella. **Direito Administrativo**. 30 ed. Rio de Janeiro: Forense, 2017. Disponível em: Minha Biblioteca.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

ECONOMIA UOL. **Cotações**. Disponível em: https://economia.uol.com.br/cotacoes/. 2019. Acesso em: 23 nov. 2019.

ESTADOS SIGNATÁRIOS. **Convenção Americana sobre Direitos Humanos**. San José, 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 13 nov. 2019.

FINCK, Michèle. ***Blockchains* and Data Protection in the European Union**. 2018. Disponível em: https://edpl.lexxion.eu/data/article/12327/pdf/edpl_2018_01-007.pdf. DOI: https://doi.org/10.21552/edpl/2018/1/6. Acesso em 12 jun. 2019.

FORTES, Vinícius Borges. **O Direito Fundamental à Privacidade: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil**. Tese (Doutorado) - Curso de Doutorado em Direito, Programa de Pós-graduação em Direito, Universidade Estácio de Sá, Rio de Janeiro, 2015. Disponível em: https://portal.estacio.br/media/922618/ok-vinicius-borges-fortes.pdf. Acesso em 06 out. 2019.

FRANKENFIELD, Jake. **Permissioned Blockchains**. Disponível em: https://www.investopedia.com/terms/p/permissioned-blockchains.asp. Acesso em: 30 nov. 2019.

GRAGLIA, J. Michael; MELLON, Christopher. Blockchain and property in 2018: At the End of the Beginning. **Innovations**, v. 12, nº 1/2. Disponível em: https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00270. Acesso em: 01 dez. 2019.

HUMBEECK, Andries Van. The Blockchain-GDPR paradox. **Journal of Data Protection & Privacy**, v. 2, nº 3, p. 208–212. Disponível em: https://www.henrystewartpublications.com/jdpp/v2. Aceso em: 28 nov. 2019.

IBANEZ, Luis-Daniel; O'HARA, Kieron; SIMPERL, Elena. **On *Blockchains* and the General Data Protection Regulation**. p. 2. 2018. Disponível em: https://eprints.soton.ac.uk/422879/. Acesso em 06 jun. 2019.

IMF. International Monetary Fund. **Inflation rate, average consumer prices**. 2019. Disponível em: https://www.imf.org/external/datamapper/PCPIPCH@WEO/WEOWORLD/VEN. Acesso em: 23 nov. 2019.

IX CONFERÊNCIA INTERNACIONAL AMERICANA. **Declaração Americana dos Direitos e Deveres do Homem**. Bogotá, 1948. Disponível em: https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm. Acesso em: 13 nov. 2019.

KADIYALA, Anant. **Nuances Between Permissionless and Permissioned Blockchains**. Disponível em: https://medium.com/@akadiyala/nuances-between-permissionless-and-permissioned-blockchains-f5b566f5d483. Acesso em: 01 dez. 2019.

KONSTANTINOS, Christidis; DEVETSIKIOTIS, Michael.. ***Blockchain*s and Smart Contracts for the Internet of Things**. 2016. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408. Acesso em: 28 nov. 2019.

KOZLINER, Evan. Merkle Tree Introduction. Disponível em: https://medium.com/hackernoon/merkle-tree-introduction-4c44250e2da7. Acesso em: 01 dez. 2019.

KULIK, Tom. **Why Blockchain And The GDPR Collide Over Your Personal Data**. Disponível em: https://abovethelaw.com/2018/10/why-blockchain-and-the-gdpr-collide-over-your-personal-data/. Acesso em: 01 dez. 2019.

LAVADO, Thiago. **Uso da internet no Brasil cresce, e 70% da população está conectada**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml>. Acesso em: 14 out. 2019.

LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011.

MANZI, Vanessa Alessi. ***Compliance* no Brasil** – consolidação e perspectivas. São Paulo: Saint Paul, 2008, p. 15.

MCKINNEY, Scott; LANDY, Rachel; WILKA, Rachel. Smart Contracts, Blockchain, and the Next Frontier of Transactional Law. **Washington Journal of Law, Technology & Arts**, v. 13, Issue 3, 2018. Disponível em: http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1818/13WJLTA313.pdf?sequence=4&isAllowed=y. Acesso em: 01 dez. 2019.

MEDICALCHAIN. **Whitepaper 2.1**. Disponível em: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf. Acesso em: 01 dez. 2019.

MEIRELLES, Hely Lopes. **Direito administrativo brasileiro**. 28 ed. São Paulo: Malheiros, 2003.

MERCADO BITCOIN. **O que é um smart contract?**. 2018. Disponível em: https://blog.mercadobitcoin.com.br/o-que-%C3%A9-um-smart-contract-b91ac7b7f21f. Acesso em: 16 nov. 2019.

MEYER, David. **Blockchain technology is on a collision course with EU privacy law**. Disponível em: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/. Acesso em: 25 nov. 2019.

MIRCHANDANI, Anisha. The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. **Fordham Intellectual Property, Media and Entertainment Law Journal**, v. 29, nº 4º, Article 5, p. 1201-1241. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1730&context=iplj. Acesso em: 28 nov. 2019.

MISES, Ludwig von. **As seis lições**. 7 ed. São Paulo: Instituto Ludwig von Mises Brasil, 2009. Disponível em: https://mises.org.br/Ebook.aspx?id=113. Acesso em: 10 nov. 2019.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 23 nov. 2019.

NERY, Carmen. **Impacto do *blockchain* deve ser similar ao do correio eletrônico**. 2018. Disponível em: https://www.valor.com.br/empresas/5804359/impacto-do-*blockchain*-deve-ser-similar-ao-do-correio-eletronico. Acesso em: 16 nov. 2019.

NIMFUEHR, Marcell. **Blockchain application land register: Georgia and Sweden leading**. Disponível em: https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa980017oc. Acesso em: 01 dez. 2019.

ONLINE TOOLS. **SHA256**. Disponível em: https://emn178.github.io/online-tools/sha256.html. Acesso em: 26 nov. 2019.

PEÑA, Carlos. **O Bitcoin foi o que impediu minha família de morrer de fome na Venezuela**. 2017. Disponível em: https://www.mises.org.br/Article.aspx?id=2771. Acesso em: 23 nov. 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais** - comentários à Lei n. 13.709/2018 LGPD - São Paulo: Saraiva Educação, 2018. Disponível em: Minha Biblioteca.

POLLOCK, Daniel. **The Fourth Industrial Revolution Built On *Blockchain* And Advanced With AI**. 2018. Disponível em: https://www.forbes.com/sites/darrynpollock/2018/11/30/the-fourth-industrial-revolution-built-on-*blockchain*-and-advanced-with-ai/. Acesso em: 16 nov. 2019.

RABELO, Maria. **Os desafios do RGPD perante as novas tecnologias *blockchain***. 2019. Disponível em: http://revistes.ub.edu/index.php/RBD/article/view/27066. Acesso em: 14 jun. 2019.

ROQUE, Leandro. **Como ocorreu a crise financeira americana**. 2018. Disponível em: https://mises.org.br/Article.aspx?id=1696. Acesso em: 23 nov. 2019.

ROSIC, Ameer. **Smart Contracts: The *Blockchain* Technology That Will Replace Lawyers**. 2016. Disponível em: https://blockgeeks.com/guides/smart-contracts/. Acesso em: 20 nov. 2019.

SHIN, Laura. **The First Government To Secure Land Titles On The Bitcoin *Blockchain* Expands Project**. 2017. Disponível em: https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-*blockchain*-expands-project. Acesso em: 16 nov. 2019.

SÔNEGO, Dubes. **Por que o *blockchain* pode mudar radicalmente a forma de se fazer negócios**. 2017. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2017/05/por-que-o-*blockchain*-pode-mudar-radicalmente-forma-de-se-fazer-negocios.html. Acesso em: 16 nov. 2019.

STEINBECK, Dean. **How New EU Privacy Laws Will Impact *Blockchain*: Expert Take.** 2018. Disponível em: https://cointelegraph.com/news/how-new-eu-privacy-laws-will-impact-*blockchain*-expert-take. Acesso em: 11 jun. 2019.

SZABO, Nick. **Smart Contracts.** 1994. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Acesso em: 28 nov. 2019.

SZABO, Nick. **The Idea of Smart Contracts**. 1997. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html. Acesso em: 28 nov. 2019.

TEIXEIRA, Tarcisio; RODRIGUES, Carlos Alexandre. **Blockchain e Criptomoedas**. Salvador: Editora JusPodivm, 2019.

ULRICH, Fernando. **Bitcoin – A Moeda na Era Digital**. – São Paulo: Instituto Ludwig von Mises Brasil, 2014. Disponível em: https://mises.org.br/Ebook.aspx?id=99. Acesso em: 16 mar. 2019.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia, de 07 de dezembro de 2000**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN. Acesso em: 21 out. 2019.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 19 nov. 2019.

UNIÃO EUROPEIA. **Regulamento (CE) nº 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000.** Bruxelas. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32001R0045&from=PT. Acesso em: 19 nov. 2019.

UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Acesso em 11 jun. 2019.

UNIÃO EUROPEIA. **Tratado que estabelece uma Constituição para a Europa. Roma, 2004**. Disponível em: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_pt.pdf. Acesso em: 19 nov. 2019.

A Editora Fi é especializada na editoração, publicação e divulgação de pesquisa acadêmica/científica das humanidades, sob acesso aberto, produzida em parceria das mais diversas instituições de ensino superior no Brasil. Conheça nosso catálogo e siga as páginas oficiais nas principais redes sociais para acompanhar novos lançamentos e eventos.

www.editorafi.org
contato@editorafi.org