UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO

VINICIUS GABRIEL KREY

IMPACTOS DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS A TECNOLOGIA *BLOCKCHAIN*

Porto Alegre
2021

VINICIUS GABRIEL KREY

IMPACTOS DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS A TECNOLOGIA *BLOCKCHAIN*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação da Faculdade de Direito da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Dra. Kelly Lissandra Bruch.

Porto Alegre

VINICIUS GABRIEL KREY

IMPACTOS DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS A TECNOLOGIA *BLOCKCHAIN*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação da Faculdade de Direito da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Data da aprovação: _____/_____/_____

BANCA EXAMINADORA:

_____

Profª. Drª. Kelly Lissandra Bruch

Orientadora

_____

Prof. Dr. Fabiano Menke

_____

Prof. Me. Mauricio Brum Esteves

RESUMO

A *Blockchain* viabilizou o surgimento do *bitcoin*, dos *smart contracts* e outras tecnologias disruptivas. Com o surgimento das legislações de proteção de dados ao redor do mundo, vislumbra-se as primeiras incompatibilidades entre a proteção de dados e essa tecnologia. A *Blockchain*, por um lado, baseia-se em um modelo descentralizado funcionando através da união de usuários, independente de um sistema central. As novas legislações de proteção de dados, por outro lado, nasceram sob uma lógica centralizada que propõem a centralização da informação na mão dos agentes de tratamento e dos encarregados de dados pessoais. Outro agravante consiste no caráter imutável da *Blockchain* e, portanto, na impossibilidade de alterar ou excluir um registro realizado na *Blockchain*, o que entra em contraste com alguns direitos trazidos pelas legislações. Assim, tendo em vista a atualidade temática e a tensão existente entre proteção de dados pessoais e *Blockchain*, o presente estudo questiona se as legislações brasileiras e europeias de proteção de dados são compatíveis com o uso da tecnologia *Blockchain*. Desta forma, o trabalho pretende analisar a possibilidade de conciliar os direitos previstos nas legislações de proteção de dados, em especial o direito ao apagamento de dados pessoais, da União Europeia e do Brasil com o uso da *Blockchain*. Para isso, o estudo pretende fazer uma análise acerca das noções genéricas sobre as espécies, características e funcionamentos da *Blockchain*. Na sequência, o trabalho procura entender as legislações de proteção de dados e os direitos previstos no Regulamento Geral sobre a Proteção de Dados (Diretiva 2016/679) e na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Também analisa os principais pontos de tensão entre as regulações e a *Blockchain*. Ainda, o estudo procura identificar as principais técnicas e meios em que é possível conciliar a *Blockchain* e as legislações de proteção de dados. Para essa pesquisa, foi utilizado o método dedutivo e exploratório, levando em consideração as legislações de proteção de dados, as decisões proferidas por autoridades nacionais, o posicionamento da literatura e da jurisprudência, bem como o funcionamento e as características técnicas da *Blockchain*. É necessário salientar que, por tratar-se de um tema muito recente, ainda não se pode aferir com certeza os impactos das novas legislações à *Blockchain*, no entanto, preliminarmente, entende-se que é possível conciliar os direitos dos titulares previstos nas legislações de proteção de dados com a tecnologia referida, bastando empreender técnicas

específicas para isso, como, por exemplo, (i) utilização de criptografia irreversível, (ii) uso de *side chain* e (iii) técnica de *off-chain*.

Palavras-chave: LGPD. RGPD. *Blockchain*. Compatibilidade. Direito ao esquecimento. Eliminação de dados. Dados Pessoais.

ABSTRACT

Blockchain enabled the emergence of bitcoin, smart contracts and other disruptive technologies. With the emergence of data protection legislation around the world, the first incompatibilities between data protection and this technology can be seen. Blockchain, on the one hand, is based on a decentralized model working through the union of users, independent of a central system. The new data protection legislation, on the other hand, was born under a centralized logic that proposes the centralization of information in the hands of the processing agents and those responsible for personal data. Another aggravating factor is the immutable nature of the Blockchain and, therefore, the impossibility of altering or deleting a record made in the Blockchain, which is in contrast to some rights brought by legislation. Thus, in view of the topical issue and the tension between personal data protection and Blockchain, this study questions whether Brazilian and European data protection legislation is compatible with the use of Blockchain technology. The work intends to analyze the possibility of reconciling the rights provided for in data protection legislation, in particular the right to erase personal data, from the European Union and Brazil with the use of the Blockchain. For this, the study intends to analyze the generic notions about the species, characteristics and functioning of the Blockchain. Next, the work seeks to understand the data protection legislation and the rights provided for in the European General Data Protection Regulation (Directive 2016/679) and in the General Law on Brazilian General Data Protection Law (Law N°. 13.709/2018). It also analyzes the main tension points between the regulations and the Blockchain. Furthermore, the study seeks to identify the main techniques and means in which it is possible to reconcile the Blockchain and data protection legislation. For this research, the deductive and exploratory method was used, taking into account data protection legislation, decisions issued by national authorities, the position of literature and jurisprudence, as well as the functioning and technical characteristics of the Blockchain. It should be noted that, as this is a very recent topic, the impacts of the new legislation on the Blockchain cannot be gauged with certainty, however, preliminarily, it is understood that it is possible to reconcile the rights of holders provided for in the legislation of data protection with the aforementioned technology, simply by undertaking specific techniques for this, such as, for example, (i) use of irreversible cryptography, (ii) use of side chain and (iii) off-chain technique.

Keywords: LGPD. GDPR Blockchain. Compatibility. Right to be forgotten. Data erasure. Personal data.

AGRADECIMENTOS

Agradeço, antes de tudo, à minha família por todo carinho e suporte durante toda caminhada.

Agradeço à minha orientadora e amiga, Kelly, pelo constante apoio e por seus valiosos ensinamentos durante toda minha trajetória acadêmica.

Agradeço aos colegas e amigos deixados no Silveiro Advogados, em espacial ao Mauricio, pela constante contribuição para minha formação acadêmica e profissional.

Por fim, agradeço aos meus verdadeiros amigos por todo apoio e parceria ao longo de toda caminhada.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AGPD	Agência Espanhola de Proteção de Dados
CNIL	Commission Nationale Informatique & Libertés
CF	Constituição Federal
DPO	Data Protection Officer
DPD	Diretiva de Proteção de Dados
DLT	Distributed Ledger Technology
LGPD	Lei Geral de Proteção de Dados Pessoais
RGPD	Regulamento Geral de Proteção de Dados
STF	Supremo Tribunal Federal
TJUE	Tribunal de Justiça da União Europeia
UE	União Europeia

SUMÁRIO

1. INTRODUÇÃO

A Idade Contemporânea é marcada pela ascensão do avanço tecnológico responsável por consolidar a Era Digital que está sendo marcada pelo protagonismo das tecnologias físicas, digitais, ambientais responsáveis por transformar a vida humana, revolucionando o mercado, criando novos espaços e tecnologias, e encurtando distâncias.

Nessa nova era o crescimento e a descoberta de novas tecnologias foi inevitável, de modo que, a Internet ganhou adesão mundial originando novos espaços como o ciberespaço. Diante disso, os novos negócios e o mercado se voltaram para esse novo espaço que foi preenchido por marcas como Google, Amazon, Microsoft, Facebook, Apple e entre outras, que se tornaram gigantes nesse meio.

Essas gigantes revolucionaram o mercado, implementado novos modelos de negócios através de dados referentes aos seus usuários, clientes e afins, para melhorar seus processos, estratégias e desempenho, entregando uma experiência personalizada, a partir dos seus hábitos de consumo, hobbies, preferências e pesquisas. Nessa lógica, atualmente os dados equivalem para nova economia à importância do petróleo para a velha economia, firmando-se como os maiores ativos das grandes marcas mundiais.

Nas últimas décadas intensificou-se o uso, processamento e armazenamento de dados, uma vez que com o surgimento da *big data*, da *machine learning* e da inteligência artificial nunca se produziu tantos dados em um período tão curto de tempo. Evidente, que esse uso desenfreado de dados trouxe, em um primeiro momento, vantagens e benefícios, mas ao mesmo tempo gerou riscos e malefícios aos cidadãos em geral, que tiveram seus dados pessoais vazados e sua privacidade violada em diferentes e repetidas ocasiões.

Assim, por consequência desse uso desenfreado e muitas vezes irresponsável de dados, legislações e regulações surgiram ao redor do mundo visando regular esse tema carente de medidas duras e imponentes. Nesse sentido, destaca-se o Regulamento Geral de Proteção de Dados (“RGPD”) da União Europeia, em vigor desde 2016, o qual impôs à todas as empresas e organizações, independente de porte

ou área de atuação, regras rígidas para coletar, processar, compartilhar e resguardar dados pessoais.

O RGPD inovou ao trazer uma legislação extraterritorial, posto que qualquer empresa que realize o tratamento de dados de pessoas que se encontrem na União Europeia pode estar sujeita às regras do RGDP, tornando efetivamente global a esfera de aplicabilidade da regulação. Devido a esse caráter global da regulação, o Brasil acompanhado de outros países sancionaram medidas e diretrizes para o tratamento de dados pessoais, a Lei Geral de Proteção de Dados Pessoais (“LGPD”) foi sancionada em agosto de 2018.

Para atender as demandas da Era Digital, e sobretudo da economia de dados referida anteriormente, novas tecnologias foram desenvolvidas. A *Blockchain* é reflexo dessa necessidade e configura um novo paradigma para o armazenamento e gerenciamento de dados.

Como já é de conhecimento público a *Blockchain* está por detrás do funcionamento do *Bitcoin*, contudo suas funções vão além, podendo criar *smart contracts*, diminuir custos na cadeia de suprimentos, sistemas de pagamentos, armazenamento em nuvem, proteção e negociação dos ativos de propriedade intelectual. Inclusive, acredita-se que com a *Blockchain* o titular dos dados pessoais poderá alcançar a verdadeira soberania dos dados, essa promessa está alinhada tanto com o RGPD quanto à LGPD, posto que ambas dispõem que o titular tenha o controle sobre os seus próprios dados.

Apesar das promessas da *Blockchain* para o alcance da soberania dos dados por parte dos titulares, há também diversos perigos, uma vez que em determinadas espécies de *Blockchains*, como regra geral, não é possível alterar ou excluir um registro realizado em uma *Blockchain*. De modo que, surge a dúvida se essa tecnologia estaria em confronto direto com as regulações de proteção de dados pessoais e os direitos que elas asseguram, especificamente o direito ao apagamento de dados pessoais.

Por essa razão, tendo em vista a atualidade temática e a tensão existente entre proteção de dados pessoais e *Blockchain*, a análise que este trabalho pretende realizar diz respeito sobre a sobre a possibilidade de conciliar os direitos previstos nas

legislações de proteção de dados, em especial o direito ao apagamento de dados pessoais, da União Europeia e do Brasil com o uso da *Blockchain*.

Desse modo, tomando como base estudos literários, legislativos e jurisprudenciais, a referida análise ocorrerá em dois momentos: no primeiro serão analisados os aspectos descritivos e gerais sobre a *Blockchain* e proteção de dados, e no segundo tratar-se-á da problemática central do conflito entre a promoção da inovação e os direitos fundamentais de privacidade e proteção de dados.

Assim, na primeira parte, serão analisadas as legislações de proteção de dados, os direitos previstos no RGPD e na LGPD, principalmente aqueles relativos ao direito ao apagamento dos dados pessoais, ainda, será examinado as diferenças entre o direito ao apagamento, ou, exclusão dos dados pessoais e o direito ao esquecimento, ou, a ser esquecido no âmbito europeu e brasileiro. Na sequência, será realizada uma análise acerca das noções genéricas sobre as espécies, características e funcionamentos da *Blockchain*.

Já, na segunda parte, analisar-se-á os principais pontos de tensão entre as regulações e a *Blockchain*. Após, será realizado um estudo visando identificar as principais técnicas e meios em que é possível conciliar a *Blockchain* e as legislações de proteção de dados. Por fim, realizar-se-á uma análise acerca da ponderação entre a promoção da inovação e os direitos fundamentais de privacidade e proteção de dados.

Em síntese, pretende-se com este trabalho verificar se as legislações de proteção de dados são compatíveis ao uso da *Blockchain*, sobretudo em relação ao direito ao apagamento de dados pessoais, levando em consideração as legislações de proteção de dados, as decisões proferidas por autoridades nacionais, o posicionamento da literatura e da jurisprudência e o funcionamento e as características técnicas da *Blockchain*.

2. PRIMEIRA PARTE

2.1. DOS ASPECTOS GERAIS PRIVACIDADE E DA PROTEÇÃO DE DADOS

2.1.1. Da Privacidade à Proteção de Dados

Como primeiro ponto importante de análise, encontram-se as noções introdutórias acerca das recentes legislações de proteção de dados. Nesse sentido, em um primeiro momento pretende-se contextualizar o surgimento do direito à privacidade e o caminho traçado até chegarmos em um direito à proteção de dados pessoais. Ato contínuo, serão apresentados os princípios, direitos e principais medidas trazidas e exigidas pelo RGPD e pela LGPD.

O conceito de privacidade nem sempre teve um único significado, adotando diferentes roupagens ao longo da história. O que antes era definido como o "direito a ser deixado só"[1], expressão cunhada pela primeira vez por Thomas McIntyre Cooley, jurista estadunidense e Presidente da Suprema Corte de Michigan, em 1888[2], decai diante de um mundo em que o intenso fluxo de informações e o desenvolvimento de novas tecnologias pode influir de forma direta na esfera privada dos indivíduos. Isso não significa que o conceito anterior seja equivocado, mas que sua carga semântica não coincide com o que ele efetivamente representa[3]. A partir desse descompasso entre as primeiras noções de privacidade e realidade atual, poderemos entender, sinteticamente, a origem da proteção de dados pessoais.

A doutrina moderna do direito à privacidade ganhou um pontapé inicial com Brandeis e Warren em seu artigo *The right to privacy*[4]. Os autores apresentaram esse novo direito explorando a jurisprudência da época demonstrando que o tema da privacidade já vinha sendo utilizado nos tribunais dos Estados Unidos da América. Ademais, a obra procurou relacionar a tutela da privacidade ao progresso tecnológico, uma vez que o avanço tecnológico possibilita novas formas de veiculação e coleta de

---

[1] WARREN, Samuel; BRANDEIS, Louis Brandeis. **The right to privacy**, em: 4 Harvard Law Review 193, 1890.

[2] CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro.** Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, edI 2017. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552017000200213&lng=en&nrm=iso>. Acesso em 23 de Abril de 2021.

[3] DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019, p. 29.

[4] WARREN, Samuel; BRANDEIS, Louis Brandeis. **The right to privacy**, em: 4 Harvard Law Review 193, 1890.

informações sobre as pessoas, razão pela qual entendia-se como necessário a existência de um direito à privacidade[5].

Ainda nos Estados Unidos da América a matéria da privacidade foi alvo de diversas discussões, no âmbito dos Tribunais podemos citar os casos *Olmstead v. United States*[6], de 1928 e *Katz v. United States*[7], de 1967. No primeiro, tratava-se da aplicação da Quarta Emenda à Constituição do Estados Unidos[8], no tocante ao direito contra buscas e apreensões não autorizadas na residência, documentos e bens de uma pessoa, em um caso envolvendo grampos telefônicos. No julgamento, cumpre destacar o voto do juiz Brandeis que ressaltou a necessidade de atualizar a interpretação da Quarta Emenda de acordo com o progresso científico, mesmo que vencido o argumento proferido por Brandeis fundamentou o segundo caso de 1967, momento em que a Quarta Emenda passou a ser aplicada diante de ameaças tecnológicas.

O direito à privacidade ganhou espaço nos ordenamentos jurídicos somente no final do século XIX. Nos primórdios, esse direito foi reservado para extratos sociais bem determinados, tendo em vista a preponderância de demandas ligadas à privacidade por pessoas de elevada projeção social.[9] A título exemplificativo desse direito à privacidade reservado às pessoas de elevadas classes sociais, pode-se mencionar o caso envolvendo o poeta Alexander Pope e o escritor Jonathan Swift de 1741[10]. No caso concreto, um editor publicou sem autorização correspondência privada trocada entre os literatos, na ocasião a sentença distinguiu a propriedade de uma carta, como um documento físico e o direito de autorizar a publicação de uma carta, reconhecendo o direito de propriedade de Pope sobre as próprias cartas, bem como o direito de publicar as cartas como um direito que permanece ao autor.

---

[5] DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais.** Em: DONEDA, Danilo; SCARLET, Ingo Wolfgang, MENDES, Laura Schertel, JUNIOR, Otavio Luiz Rodrigues (Coords.). Tratado de proteção de dados pessoais – Parte I. Rio de Janeiro: Forense, 2021. E-book Kindle.
[6] *Olmstead v. United States,* 277 U.S. 438, 478 [1928]
[7] Katz v. United States, 389, U.S. 347 (1967).
[8] Para esclarecimento, a Quarta Emenda à Constituição dos Estados Unidos é uma das emendas feitas na Carta dos Direitos e refere-se à proteção contra buscas e apreensões arbitrárias, assim a emenda proíbe a busca e apreensão sem que haja motivo razoável e mandado judicial baseado em causa provável.
[9] DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019, p. 33.
[10] Pope v. Curl, 26 Eng. Eep. 608 (1741).

Como aponta Doneda[11], esse elitismo da privacidade nos tribunais permaneceu como um modelo majoritário até a década de 1960. Quando o intenso desenvolvimento tecnológico, isto é, a capacidade técnica de coletar, processar e utilizar a informação, fez com que a informação ganhasse mais importância nas esferas jurídica, econômica e social. Com isso, não eram só pessoas de elevada projeção social que estavam sujeitas a ter seus direitos à privacidade violados, mas também uma grande parcela da população.

Nessa perspectiva, as demandas que agora moldam o conceito de privacidade são de outra ordem, posto que a exposição indesejada de uma pessoa frequentemente acontece a mais a partir da divulgação de seus dados pessoais do que por motivos de violação da sua correspondência.[12]

O documentário *The Great Hack*[13]*,* também denominado de *Privacidade Hackeada*, de 2019, expõe essa mudança de ordem das demandas que se relacionam com o direito à privacidade ao abordar o escândalo de dados do Facebook-Cambridge Analytica. Em linhas gerais, o escândalo envolvia a coleta e utilização, pela Cambridge Analytica, de dados pessoais de até 87 milhões de usuários do Facebook para influenciar a opinião de eleitores em diversos países do globo.

Somos cada vez mais identificados a partir dos nossos dados pessoais, que passam a ser indicativos de aspectos da nossa personalidade, de modo que carecem de proteção como direitos. Concebendo, assim, a privacidade com uma liberdade negativa, capaz de resguardar as pessoas contra abusos na coleta, tratamento e processamento de seus dados pessoais.

Portanto, percebe-se que o direito à proteção de dados pessoais consiste em um braço do direito à privacidade que se sofisticou e assumiu características próprias a ponto de possuir ordenamentos jurídicos próprios.

No âmbito dos ordenamentos jurídicos, a primeira tentativa de elaborar um sistema de proteção de dados na Europa, ocorreu na Alemanha Ocidental de 1970,

---

[11] DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019, p. 33.
[12] Pope v. Curl. Eng. Rep. 608 de 1741.
[13] AMER, Karim; NOUJAIM Noujaim. 2019. **The Great Hack**. Estados Unidos: Netflix.

denominada de Lei de Proteção de Dados pessoais do *Land*[14] de Hesse[15]. Essa lei inspirou outros estados alemães, motivo pelo qual foi promulgada uma lei federal sobre o tema em 1977, a *Bundesdatenschutzgesetz*. Contudo, a primeira lei nacional sobre proteção de dados surgiu na Suécia acerca do controle de banco de dados, em 1973. Seguindo o exemplo do país sueco, outras nações europeias legislaram sobre o tópico, tais como Noruega, Dinamarca, Áustria, Luxemburgo e Islândia[16].

Em 1983, uma decisão proferida pelo Tribunal Constitucional alemão foi fundamental para o desenvolvimento e a consolidação de um direito à proteção de dados, tratava-se de um caso em que reclamações constitucionais foram ajuizadas contra o recenseamento geral da população que fora determinado pela Lei do Censo de 1983. A lei alemã exigia que os dados sobre profissão, moradia e local de trabalho dos cidadãos fossem informados ao Estado para fins de apurar estudos estatísticos, tais como o estágio de crescimento populacional, distribuição espacial da população, além disso, autorizava o Estado comparar às informações coletadas com aqueles presentes nos registros públicos, visando preencher lacunas informativas nos órgãos da administração pública[17].

Ao analisar o caso, o Tribunal reconheceu que:

> "*Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG - Lei Federal sobre a Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso."*[18]

---

[14] O termo *Land* (no plural *Länder*) é utilizado para definir um estado Alemão.
[15] GVB1 I S.625 de 7 de Outubro de 1970.
[16] DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. São Paulo: Thomson Reuters Brasil, 2019, p. 192.
[17] MARTINS. Leonardo. Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais. Volume 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS. 2016. p. 56
[18] SCHWABE, Jürgen; MARTINS, Leonardo. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Konrad-Adenauer-Stiftung, 2005, p. 239 e 240. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf. Acesso em 25 de abril de 2021.

Nesse sentido, na visão de Doneda[19], a Corte reconheceu a existência de um direito à autodeterminação informacional, garantindo ao cidadão "*o direito de controlar a amplitude da divulgação ou utilização de qualquer aspecto relacionado a sua personalidade*".

Também são raízes da Proteção de Dados Pessoais no contexto europeu a Convenção Europeia de Direitos Humanos de 1953 e a Convenção de Direito à Privacidade de 1991, que por sua vez inspiraram a Diretiva de Proteção de Dados (DPD) ou Diretiva 46/95/CE, que unificou às legislações de Proteção de Dados Pessoais na União Europeia.

Nessa perspectiva, o Regulamento Geral de Proteção de Dados 216/679[20] (RGPD ou, no acrônimo anglófono pelo qual é mais conhecido, GDPR) foi concebido como uma atualização do DPD de 1995, tendo como um dos principais objetivos possibilitar ao titular dos dados pessoais o controle sobre seus dados pessoais, bem como aumentar significativamente as multas para os casos de não cumprimento da legislação. Essa atualização não acrescenta muitos conceitos, mas define as diferenças entre controladores e operadores, reforça o entendimento europeu sobre o direito a ser esquecido e o direito à portabilidade dos dados pessoais.

Um dos principais dispositivos do RGPD diz respeito à sua aplicação extraterritorial, conforme artigo 3 do RGPD[21]. De acordo com o regulamento, sua aplicação incide também sobre as entidades que, mesmo não estabelecidas na União Europeia, efetuam atividades relacionadas ao tratamento de dados pessoais de titulares que se encontram no seu território, quando o tratamento se relacionar à oferta

---

[19] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SCARLET, Ingo Wolfgang, MENDES, Laura Schertel, JUNIOR, Otavio Luiz Rodrigues (Coords.). Tratado de proteção de dados pessoais – Parte I. Rio de Janeiro: Forense, 2021. E-book kindle.

[20] UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

[21] "Artigo 3º: Âmbito de aplicação territorial 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União." UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

de bens ou serviços, sejam eles remunerados ou não, ou ao controle do seu comportamento, desde que ocorrido na União Europeia. Dessa forma, é possível que o RGPD impacte as entidades brasileiras que desenvolvem essas atividades.

A transferência internacional de dados, conforme Capítulo 5 do regulamento europeu[22], também é alvo de regulamentação por parte do RGPD, uma das hipóteses trazidas pela Lei em que é permitida a transferência internacional de dados prevê a sua realização a países que apresentem um nível adequado de proteção de dados – categoria na qual o Brasil não foi reconhecido até o momento.

Desse modo, tendo em vista o caráter extraterritorial da lei, países como Austrália, Turquia, África do Sul e México têm aprovado legislações de proteção de dados e trabalhado para alcançar um nível adequado de proteção de dados pessoais no país.

Refletindo a tendência global[23], a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)[24] entrou em vigor no Brasil no ano de 2020. No contexto brasileiro, assim como no europeu, a temática da proteção de dados também ganhou destaque a partir da segunda metade do século XX, a partir de 1970 já se debatia em território nacional acerca dos conflitos existentes entre a tecnologia dos bancos de dados computadorizados e a privacidade dos cidadãos.

Nessa linha, surgiram no Brasil alguns projetos de lei para regularizar e monitorar o uso indevido de dados registrados em dispositivos eletrônicos de processamento de dados, como é o caso do Projeto de Lei nº 4.365 de 1977[25]. Outras

---

[22] “Artigo 45º (…) Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado.” UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

[23] ALBRECHT, Jan. P. How the GDPR Will Change the World. European Data Protection Law Review, [s. l.], v. 2, n. 3, p. 287-289, 2016. Disponível em: https://edpl.lexxion.eu/article/edpl/2016/3/4/display/html. Acesso em 27 de nov. de 2020.

[24] BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

[25] BRASIL. Câmara dos Deputados. Projeto de Lei PL nº 4.365 de 1977, de autoria do Deputado Faria Lima. Cria o Registro Nacional de Banco de Dados e estabelece normas de proteção da intimidade contra o uso indevido de dados arquivados em dispositivos eletrônicos de processamento de dados. Diário do Congresso Nacional, ano XXXII, n. 137, 08 de nov. de 1977, p. 79.

noções importantes de proteção de dados, surgiram a partir do Projeto de Lei nº 2.796 de 1980[26], que assegurava aos cidadãos o acesso as informações sobre sua pessoa constantes em bancos de dados. Ambas as propostas não se tornaram leis.

Nesse mesmo período, nos estados do Rio de Janeiro e São Paulo, ganharam força e foram aprovadas legislações estaduais, que permitiam aos cidadãos o acesso e a retificação de seus dados pessoais registrados em base de dados operadas nos estados. Segundo Danilo Doneda[27], tais legislações já traziam noções importantes para o panorama da proteção de dados com os conceitos de "finalidade" e "consentimento informado". Além disso, no momento de redemocratização com a promulgação da Constituição de 1988[28] garantiu-se proteção constitucional da privacidade (artigo 5º, inciso X, da Constituição Federal), e do sigilo das comunicações (artigo 5º, inciso XII, Constituição Federal), além da garantia de habeas data (artigo 5º, inciso LXXII, da Constituição Federal, e Lei nº 9.507/97[29]), isto é, aquilo a que os juristas chamam de "remédio constitucional" 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, e para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Ainda sobre a evolução legislativa do país, vale lembrar a Lei de Acesso à Informação (Lei nº 12.527 de 2011)[30] que consagrou o direito constitucional de liberdade informativa no âmbito da administração pública, bem como a Lei do

---

[26] Id. Projeto de Lei PL nº 2.796 de 1980, de autoria da Deputada Cristina Tavares. Assegura aos cidadãos acesso as informações sobre sua pessoa constantes de bancos de dados e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0jixvnje56mya95us1hz6hhwj1058108.node0?codteor=1172300&filename=Dossie+->. Acesso em: 10 de outubro 2021.

[27] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SCARLET, Ingo Wolfgang, MENDES, Laura Schertel, JUNIOR, Otavio Luiz Rodrigues (Coords.). Tratado de proteção de dados pessoais – Parte I. Rio de Janeiro: Forense, 2021. E-book kindle.

[28] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 jun. 2021

[29] BRASIL. Lei nº 9.507, de 12 de novembro de 1977: Regula o direito de acesso a informação e disciplina o rito processual do habeas data. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm> Acesso em: 23 ago. 2021.

[30] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 14 de novembro de 2021.

Cadastro Positivo (Lei nº 12.414 de 2011)[31] que proibiu o registro de informações excessivas ou sensíveis sobre os consumidores. Nota-se que, até o momento, a matéria dispunha de uma sistemática própria, como ocorria em outros países, o que começou a mudar com a promulgação do Marco Civil da Internet, o qual reforçou a ideia de inviolabilidade da vida privada e da intimidade nas atividades desenvolvidas no ambiente digital[32].

Por fim, em 2018 foi sancionado o Projeto de Lei da Câmara nº 53 de 2018, o qual culminou no surgimento da Lei Geral de Proteção de Dados Pessoais[33]. Entendido o contexto histórico do surgimento do RGPD e da LGPD, faz-se necessário conhecer as noções genéricas e os institutos previstos em ambas as legislações.

2.1.2 Das legislações de proteção de dados europeia e brasileira

Ambas as legislações apresentadas, tanto o RGPD quanto a LGPD, reforçam a ideia de que dado pessoal consiste em uma informação relativa a uma pessoa natural identificada ou identificável. Nesses termos, é considerada identificável uma pessoa natural que possa ser identificada, direta ou indiretamente. Ou seja, mesmo aquelas informações que precisam ser combinadas com outras informações para identificar o titular dos dados pessoais estão abarcadas no conceito de dado pessoal.

Outro conceito importante trazido pelas legislações é o de tratamento de dados pessoais, que também possui significados semelhantes em ambas legislações. Conforme o artigo 4º do RGPD[34], o tratamento de dados consiste em:

---

[31] BRASIL. Lei nº 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Acesso em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em 14 de novembro de 2021.

[32] "Artigo 7º: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação". BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 23 agosto 2021.

[33] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de agosto de 2021.

[34] UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

> *"uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição."*

Já para LGPD, o conceito de tratamento de dados pessoais está disposto no artigo 5º, inciso X da Lei[35]. A saber:

> "*toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".* Nota-se que ambas as legislações procuraram trazer significados bem amplos para o tratamento de dados, a fim abarcar todas as situações possíveis."

As leis em análise também compartilham os mesmos personagens principais: a) titular dos dados, pessoa a quem se referem os dados pessoais que são objetos de tratamento; b) controlador de dados, pessoa a quem compete as decisões do tratamento de dados pessoais; c) operador ou processador de dados, pessoa que realiza o tratamento de dados pessoais em nome do controlador de dados; e d) DPO ou encarregado, pessoa responsável por atuar como um canal de comunicação entre os controladores e operadores, titulares e autoridades.

Ambas também compartilham de princípios, direitos e obrigações semelhantes. Dentro do que estabelece o RGPD, sete princípios fundamentais foram estabelecidos para o tratamento de dados pessoais. São eles:

- Lealdade, imparcialidade e transparência: o processamento de dados pessoais deve ter uma justificativa legal para acontecer, além da transparência do motivo apresentado.
- Limitação de propósito: a coleta de dados pessoais deve ter fins específicos, explícitos e legítimos.
- Minimização de dados: a coleta de dados pessoais deve estar limitada apenas ao necessário para aquilo que se destina seu uso.
- Precisão: dados precisos e só utilizados quando necessário.

[35] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de agosto de 2021.

- Limitação de armazenamento: o formato dos dados pessoais deve permitir a identificação apenas do necessário a ser utilizado.
- Integridade e confidencialidade: o processamento dos dados pessoais deve garantir a segurança dos mesmos.
- Prestação de contas: O responsável pelo uso dos dados deve cumprir rigorosamente os princípios.

De forma semelhante, a LGPD traz os princípios que devem ser observados para o tratamento de dados pessoais. São eles:

- Finalidade e Adequação: o tratamento de dados deve se dar para um propósito legítimo e específico, informado à pessoa; outros usos dos mesmos dados para outros propósitos não são permitidos.
- Necessidade: deve-se realizar o tratamento mínimo necessário para a realização da finalidade, sem dados excessivos.
- Qualidade, Livre Acesso e Transparência: as pessoas devem possuir informações claras, precisas e facilmente acessíveis sobre o tratamento dos seus dados, os quais devem estar corretos e atualizados.
- Segurança e Prevenção: devem ser adotadas medidas técnicas e administrativas para proteger os dados pessoais e prevenir a ocorrência de incidentes.
- Não-discriminação: o tratamento não pode ser realizado para fins discriminatórios, ilícitos ou abusivos.
- Responsabilização e Prestação de Contas: quem trata dados pessoais deve estar preparado para demonstrar a conformidade com a LGPD e a eficácia das medidas adotadas para a sua proteção.

Ambas as legislações preveem hipóteses em que o tratamento de dados pessoais será considerado lícito, nesse sentido todo o tratamento de dados pessoais deve ocorrer respeitando pelo menos um dos autorizativos legais trazidos pela legislação. No caso do RGPD, são seis hipóteses previstas no art. 6º, quando:

> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Cumpre destacar, que a LGPD é mais abrangente que o RGPD ao elencar 10 hipóteses em que o tratamento de dados pessoais poderá ser realizado:

> "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, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

Evidente, que ambas as legislações não se preocupam apenas com os meios e com as finalidades pelas quais ocorrem o tratamento de dados pessoais, mas também procuram assegurar mais segurança e protagonismo aos titulares de dados pessoais. De modo que, os princípios acima detalhados podem ser utilizados para derivar uma série de direitos para os titulares de dados e obrigações para os controladores. Nesse contexto, iremos nos dedicar ao estudo do direito ao apagamento e à eliminação dos dados pessoais, respectivamente, previsto no art. 17 do RGPD[36] e no art. 18, inciso IV da LGPD[37].

2.1.3 O direito ao apagamento e à eliminação dos dados pessoais

Inicialmente, visando dar continuidade ao estudo da temática da proteção de dados, este tópico pretende contextualizar o direito ao apagamento dos dados e o direito à eliminação previstos no RGPD e na LGPD, respectivamente. Também será

---

[36] "Artigo 17º. Direito ao apagamento dos dados («direito a ser esquecido») 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6º, nº 1, alínea a), ou do artigo 9º, nº 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21º, nº1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21º, nº 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8º, nº 1." UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

[37] "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (…) IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;". BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de agosto de 2021.

objeto de análise a noção de direito ao esquecimento previsto no RGPD e se existe direito ao esquecimento no Brasil, no âmbito da LGPD.

Na LGPD, o direito à eliminação dos dados pessoais está previsto no artigo 18, inciso IV da legislação, e consiste no direito à "eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nessa Lei". Essa noção de eliminação de dados trazida pela legislação brasileira, aproxima-se do direito ao apagamento que já era previsto na Diretiva Europeia 95/46[38], que foi substituída pelo Regulamento Europeu 2016/679, também conhecida como RGPD.

O RGPD através de seu artigo 17 e também nos *consideranda* 65 e 66, procura positivar o "direito ao apagamento de dados" também denominado no mesmo dispositivo de "direito a ser esquecido". Vale lembrar que o conceito de direito a ser esquecido trazido pela legislação, já foi utilizado em outras oportunidades e tomou noções distintas do mero apagamento de dados pessoais.

Nesse sentido, será analisado o direito ao esquecimento no contexto europeu, antes que se possa adentrar ao direito à eliminação de dados previsto na lei brasileira.

O direito a ser esquecido, ou direito ao esquecimento, não pode ser considerado novo em solo europeu, tendo em vista a existência de diversas decisões judiciais que trataram do assunto, das quais algumas delas serão exploradas neste trabalho. Na visão de Parentoni[39], o

> *"direito ao esquecimento é a faculdade de obstar o processamento informatizado, a transferência ou publicação de dados pessoais, além de exigir que sejam apagados, sempre que a sua preservação esteja causando constrangimento ao sujeito envolvido, desde que não exista razão de interesse público que justifique a preservação."*

Acerca da temática, vale lembrar os casos ocorridos na Alemanha, Lebach I e II, apresentados por Robert Alexy no livro a Teoria dos Direitos Fundamentais[40]. Em 1969[41], próximo à cidade de Lebach, na Alemanha, quatro soldados do Exército

---

[38] MALDONADO, Viviane. Capítulo III – Dos Direitos do Titular. In: MALDONADO, Viviane; BLUM, Renato (Coords.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: 2ª Ed. Thompson Reuters Brasil, 2020. E-book kindle.

[39] PARENTONI, Leonardo. Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014) (pp.539-618) Tomo 1: Capítulo Chapter: O Direito ao Esquecimento (Right to Oblivion). Editora Quartier Latin do Brasil, São Paulo, 2016, p. 577;

[40] ALEXY, Robert. Teoria dos Direitos Fundamentais. São Paulo: Malheiros, 2015. p. 99 e ss.

[41] MALDONADO, Viviane. Direito ao Esquecimento. Barureri, SP: Novo Século Editora, 2017, p. 168.

Alemão foram assassinados enquanto dormiam e as armas que guardavam, roubadas. Em 1970, houve a condenação dos criminosos a penas diversas. Em 1972[42], a emissora de televisão ZDF planejava exibir um documentário com o título "O Assassinato de Soldados em Lebach". Na época prevista para a exibição do documentário, um dos envolvidos no crime estava perto de ser liberto da prisão e sustentava que a exibição do programa, no qual ele era identificado, dificultaria o seu processo de ressocialização.

O Tribunal Estadual rejeitou o pedido de medida cautelar para proibição do documentário e o Tribunal Superior Estadual negou provimento ao recurso contra essa decisão,[43] inconformado, o demandante ajuizou reclamação constitucional contra as decisões. No âmbito do Tribunal Constitucional Federal[44], a argumentação se deu em três etapas. Primeiro, percebeu-se uma colisão entre "proteção da personalidade" e "liberdade de informar por meio de radiodifusão", princípios de valores do mesmo nível hierárquico. Esse conflito, chamado pelo tribunal de "colisão", ocorre quando há um choque entre princípios cujos valores, em abstrato, estão em mesmo nível hierárquico. Logo, a solução do caso não ocorre pela declaração de invalidade de uma das duas normas. Já na segunda etapa, o Tribunal sustentou a precedência geral da liberdade de informar quando se tratar de uma informação atual sobre atos criminosos. Contudo, na terceira parte o Tribunal entendeu que no caso a "repetição de noticiário televisivo sobre grave crime, não mais revestido de um interesse atual pela informação, coloca em risco a ressocialização do autor", decidindo que a proteção da personalidade tem precedência frente à liberdade de informar.

Ainda, em 1999, no que ficou conhecido como o caso Lebach II, revisitou-se a temática do direito ao esquecimento[45]. Na ocasião, a televisão alemã SAT 1 produziu uma série sobre crimes que marcaram a história, diferentemente do ocorrido alguns anos atrás, os produtores tomaram cuidado para não divulgar o nome e as imagens de algumas das pessoas envolvidas. Novamente, os envolvidos no Caso

[42] MALDONADO, Viviane. Direito ao Esquecimento. Barureri, SP: Novo Século Editora, 2017, p. 168.
[43] MALDONADO, Viviane. Direito ao Esquecimento. Barureri, SP: Novo Século Editora, 2017, p. 170-173.
[44] MALDONADO, Viviane. Direito ao Esquecimento. Barureri, SP: Novo Século Editora, 2017, p. 170-173.
[45] MALDONADO, Viviane. Direito ao Esquecimento. Barureri, SP: Novo Século Editora, 2017, p. 173.

Lebach I contestaram a exibição da série sob argumentos semelhantes aos expostos no primeiro caso.

No entanto, no presente caso, o Tribunal Constitucional Federal[46] adotou o entendimento de que o direito de informação preponderava sobre o direito à privacidade em que foi alegado violação, tendo em vista que as identidades dos envolvidos foram resguardadas. Além disso, no tocante aos argumentos relativos à dificuldade de ressocialização, o Tribunal rechaçou o argumento dado o transcurso de tempo da ocorrência do crime, de maneira que os riscos para ressocialização foram minorados ao longo do tempo.

A título exemplificativo, cita-se o emblemático caso do homicídio de Walter Sedlmayr[47], ator que foi assassinado por dois meio-irmãos em 1990, ambos foram condenados à prisão perpétua. Ocorre que em decorrência de benefício de livramento condicional, ambos foram soltos nos anos de 2007 e 2008, momento em que postulou-se a remoção de informações referentes aos autores do crime que eram identificados como assassinos na plataforma Wikipedia.

Em primeira instância, o Tribunal de Hamburgo decidiu a menção dos nomes dos meio-irmãos na plataforma violavam o direito à privacidade. No entanto, no ano de 2009, ao decidir acerca do tema, a Corte Constitucional Alemã afastou a pretensão, sob o argumento de que tal ato era uma restrição à liberdade de imprensa trazida pela constituição, de maneira que os demandantes deveriam aceitar um grau de intromissão em suas privacidades.

É evidente que no caso relatado acima não se reconheceu o direito ao esquecimento, mas houve discussões sobre elementos atinentes à privacidade e ao interesse público.

Assim, verifica-se que o direito ao esquecimento não é novidade no contexto europeu[48]. Contudo, o direito ao esquecimento ganhou notoriedade e repercussão

---

[46] MALDONADO, Viviane. Direito ao Esquecimento. Barureri, SP: Novo Século Editora, 2017, p. 174-176.

[47] MALDONADO, Viviane. Capítulo III – Dos Direitos do Titular. In: MALDONADO, Viviane; BLUM, Renato (Coords.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: 2ª Ed. Thompson Reuters Brasil, 2020. E-book kindle.

[48] MALDONADO, Viviane. Capítulo III – Dos Direitos do Titular. In: MALDONADO, Viviane; BLUM, Renato (Coords.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: 2ª Ed. Thompson Reuters Brasil, 2020. E-book kindle.

mundial em 2014 com o caso entre Mario Costeja González e o Google.[49] O caso originou-se a partir da publicação, em 1998, do jornal *La Vanguardia*, de dois editais de leilão de propriedade pertencentes a Mario Costeja González para o pagamento de dívidas com a seguridade social, tais publicações figuravam como um dos primeiros resultados de pesquisa ao buscar pelo nome de Costeja na ferramenta de busca.[50]

Em 2009, Mario Costeja sob o argumento de que a dívida objeto da publicação já havia sido quitada, requereu ao jornal responsável pelas publicações a supressão dessa informação. Em sua resposta, o jornal informou que não iria excluir a publicação uma vez que se tratava de publicação oficial, de ordem do Ministro do Trabalho e de Seguridade Social. Diante da negativa, Costeja solicitou ao Google Spain que excluísse tais informações através de requerimento encaminhado à matriz norte-americana do Google, que se demonstrou inexitoso.

Diante das negativas, o requerente ajuizou reclamação junto à Agência Espanhola de Proteção de Dados (AGPD). A AGPD acolheu o pedido de Costeja referente ao Google, mas afastou a responsabilidade do jornal em excluir as publicações. Na ocasião, o Google impetrou recurso apelando à Suprema Corte Espanhola a nulidade da decisão preferida. O principal argumento utilizado pela apelante era de que o processamento de dados pessoais era efetuado fora da União Europeia.

O órgão jurisdicional nacional submeteu o caso ao Tribunal de Justiça da União Europeia (TJUE), colocando em pauta três pontos principais: a) a aplicação ou não da Diretiva 95/46-CE acerca da territorialidade; b) a definição da natureza da atividade desempenhada pelos motores de busca; e c) a possibilidade ou não de apagamento de dados licitamente publicados. Em 13 de maio de 2014, o Tribunal de Justiça da União Europeia, reconheceu em favor do demandante, Mario Costeja González, o direito ao esquecimento (C-131/12)[51] atinente à informação antiga

[49] UNIÃO EUROPEIA. Tribunal de Justiça Europeu. Grande Secção. Pedido de Decisão Prejudicial C-131/12. Google Spain SL e Google Inc. Agência Española de Protección de Datos (AEPD). Relator: M. Ilešič. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131. Acesso em 19 de abr. de 2021.
[50] MALDONADO, Viviane. Direito ao Esquecimento. Barureri, SP: Novo Século Editora, 2017, p. 170-103.
[51] UNIÃO EUROPEIA. Tribunal de Justiça Europeu. Grande Secção. Pedido de Decisão Prejudicial C-131/12. Google Spain SL e Google Inc. Agência Española de Protección de Datos (AEPD). Relator: M.

encontrada por meio do buscador Google e que não há necessidade ou legítimo interesse quanto à sua subsistência. Na ocasião, o TJUE fixou que:

> *"não se discute que entre os dados encontrados, indexados e armazenados pelos motores de busca e postos à disposição dos seus utilizadores figuram também informações sobre pessoas singulares identificadas ou identificáveis e, portanto, 'dados pessoais' na acepção do artigo 2.º, alínea a), da referida diretiva."*[52]

Ademais, o TJUE ao reconhecer o direito ao esquecimento assegurou o direito à desindexação das informações à pedido do interessado, desde que não se trate de figura pública, hipótese em que há interesse público em ter acesso a determinadas informações. Nota-se que no caso em questão garantiu-se não a exclusão das publicações realizadas pelo jornal, mas, sim, a desindexação dessas informações dos motores de busca.

Uma vez contextualizado o direito ao esquecimento, pode-se passar para análise do dispositivo legal dividido em 3 tópicos dispostos dentro do artigo 17 do Regulamento Europeu[53]. No primeiro item, elenca hipóteses em que o direito ao apagamento poderá ser requerido, a saber:

> a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
>
> b) O titular retirar o consentimento em que se baseia o tratamento dos dados nos termos do artigo e não existir outro fundamento jurídico para o referido tratamento;
>
> c) O titular opõe-se ao tratamento nos termos do artigo 21º, nº 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21º, nº 2;
>
> d) Os dados pessoais foram tratados ilicitamente;

Ilešič. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131. Acesso em 19 de abr. de 2021.

[52] UNIÃO EUROPEIA. Tribunal de Justiça Europeu. Grande Secção. Pedido de Decisão Prejudicial C-131/12. Google Spain SL e Google Inc. Agência Española de Protección de Datos (AEPD). Relator: M. Ilešič. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131. Acesso em 19 de abr. de 2021.

[53] ." UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

> e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
>
> f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8º, nº 1.

Ainda, a legislação dispõe que, quando:

> "[...] o responsável tratamento pelo tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos"[54].

Por último, o RGPD[55] prevê exceções em que o tratamento mencionado acima não se aplica, para fins de: (i) exercício de liberdade de expressão e informação; (ii) cumprimento de obrigação legal que exija o tratamento de dados pessoais; (iii) interesse público no domínio da saúde pública; (iv) arquivo de interesse público, em razão de de investigação científica ou histórica ou para fins estatísticos; e para (v) efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Nessa linha, o titular de dados pessoais que pretender fazer valer o direito ao apagamento ou esquecimento previsto na normativa europeia, necessita invocar uma das hipóteses previstas no item 1 do artigo 17. Cabe ao responsável pelo tratamento proceder com o apagamento da informação, uma vez não verificada hipótese legal para conservação da informação. Impende mencionar, ainda, que quando se trata de

---

[54] UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

[55] UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

apagamento de dados a regra geral é de que não basta a ocultação das informações, a legislação exige a completa eliminação dos arquivos, sistemas e backups.

Em análise à redação do inciso I do art. 17 do RGPD, verifica-se que a questão temporal não é relevante para o reconhecimento do direito ao esquecimento naquele contexto, basta que se retire o consentimento a qualquer tempo[56]. Ou seja, a compreensão de direito ao esquecimento trazida pelo RGPD distancia-se dos elementos adotados pela doutrina clássica nos casos relatados anteriormente[57], em que há pressuposição da perda do interesse público pelo mero transcurso de tempo como pilar justificado da invocação do direito.

Além disso, vale destacar que o direito ao esquecimento como vêm sendo ventilado na doutrina nos últimos diz respeito ao caso Mario Costeja González contra o Google, referente a desindexação do seu nome das informações encontradas em motores de busca da internet. Já o direito ao esquecimento trazido pelo RGPD, simplesmente, faz alusão ao direito ao apagamento de dados quando os dados pessoais não cumprem mais a finalidade que originou sua coleta ou quando ocorre a revogação do consentimento que baseia o tratamento de dados.

Por conseguinte, em matéria de proteção de dados no contexto europeu, o legislador optou por tratar o direito ao apagamento dos dados como sinônimo de direito ao esquecimento, mesmo que o conceito de direito ao esquecimento da legislação se afaste da sua concepção clássica e doutrinária, que vem sendo construída nos últimos anos.

No Brasil não há possibilidade de entendimento similar, uma vez que trata-se de institutos jurídicos distintos. Recentemente, o STF definiu que:

> *"É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício de liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade*

[56] MALDONADO, Viviane. Capítulo III – Dos Direitos do Titular. In: MALDONADO, Viviane; BLUM, Renato (Coords.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: 2ª Ed. Thompson Reuters Brasil, 2020. E-book kindle.

[57] MALDONADO, Viviane. Capítulo III – Dos Direitos do Titular. In: MALDONADO, Viviane; BLUM, Renato (Coords.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: 2ª Ed. Thompson Reuters Brasil, 2020. E-book kindle.

> *e da personalidade em geral e as expressas e específicas previsões legais nos âmbitos penal e cível."*[58]

Tal decisão teve origem no caso Aida Cury e consiste em recurso interposto em ação de reparação de danos ajuizada pela família de Aída Curi contra a TV Globo. No caso concreto, a jovem Aída foi violentada sexualmente por três homens e morta. O crime ganhou grande repercussão na época dos fatos e, passados quase cinquenta anos dos eventos, o programa de TV "Linha Direta Justiça", da TV Globo, trouxe exposições explícitas do referido crime, relembrando a história e trazendo dores aos familiares. O debate se debruçou sobre a contraposição de dois princípios constitucionais fundamentais: de um lado, a garantia constitucional à plena liberdade de expressão e manifestação do pensamento, independentemente de censura (CF, art. 220) e, de outro, o direito à privacidade e à tutela da dignidade da pessoa humana (CF, art. 5º, inciso X).

Nessa perspectiva, tem-se que a legislação brasileira[59] prevê a possibilidade de eliminação dos dados pessoais desnecessários, excessivos e tratados em desconformidade com a lei. Tal instituto não se confunde com o direito ao esquecimento, conforme decidiu o STF, e diz respeito exclusivamente à eliminação dos dados nas circunstâncias descritas, tendo em vista que os dados pessoais devem ser sempre necessários, adequados e lícitos.

Em síntese, conclui-se que o conceito de direito ao esquecimento trazido pelo RGPD é sinônimo de direito ao apagamento, rompendo com os elementos clássicos associados ao direito ao esquecimento.

Na Lei Geral de Proteção de Dados Pessoais, o legislador opta por trazer apenas o direito à eliminação dos dados pessoais, através do artigo 18, inciso VI da lei. De forma semelhante a legislação da UE, a LGPD também traz hipóteses em que

---

[58] BRASIL. Supremo Tribunal Federal. RE nº 1.010.606-RJ. Recorrente: Nelson Cury e Outros. Recorrido: Globo Comunicação e Participações S/A. Relator: Ministro Dias Toffoli. Rio de Janeiro, 11 de fevereiro de 2021.

[59] "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (…) IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;". BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de agosto de 2021.

o dado pessoal pode ser conservado[60], são elas: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; c) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou d) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Uma vez entendido as noções genéricas e os institutos previstos em ambas as legislações estudados, faz-se necessário aprofundar as noções acerca da tecnologia *Blockchain*.

[60] "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes 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." ;". BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de agosto de 2021.

2.2 DOS ASPECTOS GERAIS DA TECNOLOGIA *BLOCKCHAIN*

A tecnologia *Blockchain*, surgiu em 2008, foi criada por uma pessoa ou um grupo sob o pseudônimo de Satoshi Nakamoto[61], como uma inovação tecnológica da criptomoeda bitcoin.

A tecnologia funciona como um registro distribuído de dados, também denominada de *Distributed Ledger Technology* (DLT) ou sistema de livro-razão distribuído, sem interferência de terceiros, propõe a imutabilidade, a transparência e a descentralização. Assim, a *Blockchain* é uma nova tecnologia para o armazenamento de dados, configurando, também, em uma nova plataforma que possibilita novas aplicações, podendo ser um instrumento de certificação e controle de diversos tipos de transações. Ou seja, a *Blockchain*

> [...] pode ser útil para a gestão de transações de qualquer moeda, como acontece com o bitcoin, e como pode acontecer com ativos da BM&FBovespa, ou moedas do mercado Forex, ou uma criptomoeda que você deseje criar, etc, mas essas serão sempre apenas algumas aplicações para ele, pois seu conceito se encaixa mais em uma plataforma, e portanto, em tese, você pode armazenar com o blockchain toda e qualquer transação, compilada em metadados, com blocos que são adicionados em cadeia numa ordem linear e cronológica, armazenados em uma rede distribuída e teoricamente para sempre[62].

Para Klaus Schwab[63], fundador do Fórum Econômico e Mundial, a tecnologia consiste em um livro contábil compartilhado, criptograficamente seguro e confiável, que não é controlado por um usuário único, mas pode ser inspecionado por todos. Veja que diferentemente dos sistemas tradicionais que necessitam de intermediários, a tecnologia *Blockchain* é auto sustentável, capaz de funcionar de maneira segura e íntegra sem a necessidade de intervenções de terceiros.

A título exemplificativo, é possível citar uma transação bancária que em sistemas tradicionais dependeria de um terceiro - instituição bancária, responsável por autorização para efetuar a transação. Na *Blockchain* essa autorização seria validada

---

[61] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [s.l.: s.n.], 2008. Disponível em <https://bitcoin.org/bitcoin.pdf>. Acesso em 01 de out. de 2021.
[62] FIGURELLI, Rogério. BLOCKCHAIN: Uma análise estratégica para humanos e robôs. Trajecta. Edição do Kindle, 2017.
[63] SCHWAB, Klaus. A Quarta Revolução Industrial. Tradução de Daniel Moreira Miranda. 1. ed. São Paulo: Edipro, 2016, p. 30.

pelo próprio sistema, sem a necessidade de intervenção um terceiro, garantindo uma transação mais rápida, confiável e de menor custo. Nesse sentido, tem-se uma tecnologia com potencial para romper com os sistemas e métodos antigos.

Conforme já referido, a primeira implementação da *Blockchain* em uma aplicação concreta se deu em 2008, quando da divulgação do estudo "*Bitcoin: A Peer-to-Peer Electronic Cash System*"[64]. O estudo tratava-se da criação de sistema de intercâmbio de ativos, capaz de funcionar de forma descentralizada e independente de instituições financeiras tradicionais. Além disso, o trabalho faz críticas ao modelo de comércio adotado na internet, com a tecnologia *Blockchain* seria possível a operacionalização da criptomoeda *Bitcoin.*

Vale destacar que a tecnologia *Blockchain* não está por trás apenas da *Bitcoin*, podendo funcionar e revolucionar as mais diversas atividades. Inicialmente, as primeiras funções versavam sobre o registro permanente de documentos públicos e privados[65], tendo em vista o caráter imutável da *Blockchain*. Atualmente, com maior fama e visibilidade a *Blockchain* pode viabilizar avanços para o setor público, como cartórios e juntas comerciais. A Estônia[66], por exemplo, possui sua própria *Blockchain* que permeia boa parte todos setores políticos e governamentais no país

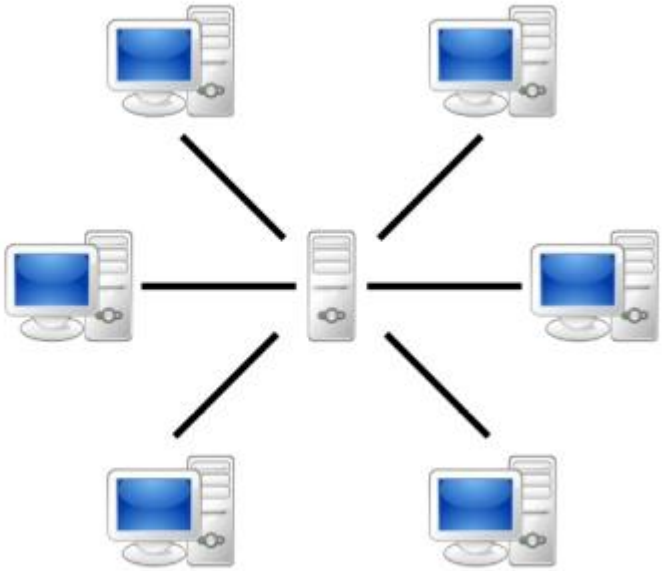
Para compreendermos a *Blockchain* e suas possíveis implicações no âmbito da privacidade e da proteção de dados, devemos entender os conceitos técnicos e o seu funcionamento.

A *Blockchain* tem em seu pilar principal a descentralização, de modo que a tecnologia funciona sem qualquer poder ou sistema central, basta apenas a união de vários usuários. Essa lógica se difere dos sistemas tradicionais, geralmente atrelados a um servidor central que autoriza os usuários de determinada rede consultar, inserir e alterar as informações da rede.

---

[64] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [s.l.: s.n.], 2008. Disponível em https://bitcoin.org/bitcoin.pdf. Acesso em 01 de set. de 2021.
[65] MORGAN, Pamela. Using Blockchain Technology to Prove Existence of a Document. https://empoweredlaw.wordpress.com/2014/03/11/using-blockchain-technology-to-prove-existence-of-a-document/. Acesso em 04 de set. de 2021.
[66] E-ESTONIA. KSI Blockchain in Estonia. Disponível em: https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf. Acesso em 04 de set. de 2021.

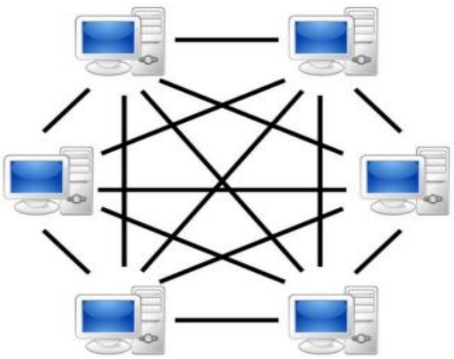
Figura 1 - Modelo Centralizado



Fonte: BIEG, Mauro. 12 ago. 2007. Disponível em https://upload.wikimedia.org/wikipedia/commons/f/fb/Server-based-network.svg. Acesso em 24 set. 2021

Nessa linha, no modelo adotado pela *Blockchain*, também denominado de Peer to Peer ou P2P, que consiste em uma arquitetura descentralizada todos os dispositivos do sistema agem de forma híbrida, ora atuando como meros usuários - realizando transações, ora como servidores - armazenado e validando a consulta, inserção e alteração de informações. De modo que, cada dispositivo da rede pode ser descrito como um nó ou ponto, esses dispositivos, diferentemente do que ocorre nos sistemas tradicionais, possuem o mesmo nível hierárquico.

Figura 2 - Modelo descentralizado

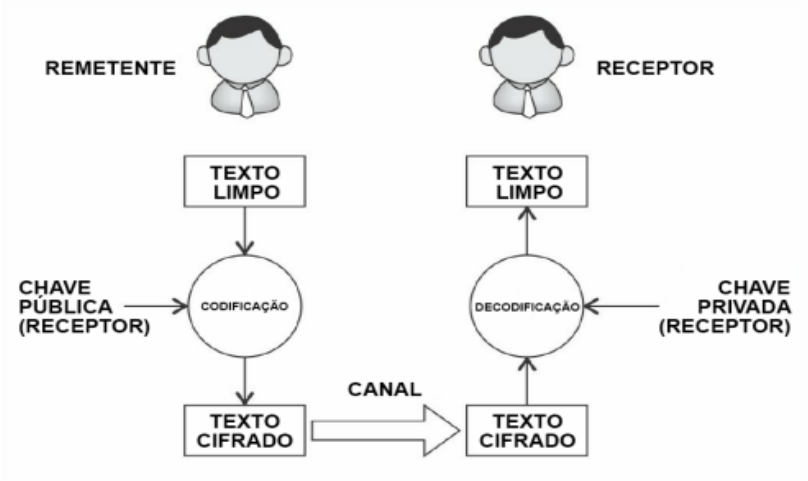


Fonte: UFRJ. Disponível em https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/p2p/images/funcionamento.png. Acesso em 24 set. 2020.

Outro ponto positivo da *Blockchain*, também proposto através de uma arquitetura descentralizada é seu nível de segurança, tal característica é assegurada através da criptografia. Na *Blockchain*, a encriptação de informações é possível através do algoritmo de chave assimétrica e da função de *hash*.

As técnicas de criptografia assimétricas pressupõem duas chaves distintas concedidas a um indivíduo: uma pública, à qual todos podem ter acesso, e outra privada, à qual somente o indivíduo detentor da chave pública possui acesso[67]. Por esse motivo, o modelo é também conhecido como criptografia de chave pública[68]. Basicamente, a chave pública é utilizada para cifrar um conteúdo e chave privada para decifrar tal conteúdo. Desse modo, quando um arquivo é criptografado por um indivíduo através de sua chave pública, a única possibilidade de se descriptografar tal arquivo é através da chave privada desse mesmo indivíduo, essa chave privada deve ser mantida em sigilo a fim de que apenas os indivíduos desejados possam acessar o conteúdo criptografado. Através desta técnica de criptografia, caso terceiros tenham acesso ao arquivo codificado, não será possível acessar ao conteúdo presente no arquivo, tendo em vista que terá acesso a dados totalmente embaralhados e inteligíveis.

Figura 3 - Técnica de criptografia assimétrica



[67] MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 28.
[68] BASHIR, Imran. Mastering Blockchain. 2 ed. Birmingham: Packt, 2018, p. 80. E-book. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1789486&lang=pt-br&site=ehost-live. Acesso em: 04 de maio de 2021.

Fonte: MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 81.

A outra primitiva criptográfica utilizada é o caso das funções *hash* criptográficas, que transformam textos ou arquivos, de tamanhos variados, para uma sequência de caracteres de tamanho fixo, denominada *hash* [69]. Através dessa função um arquivo é fragmentado em vários pedaços menores, que são embaralhados e transformados em um código de tamanho fixo. O resultado dessa modalidade de operação se demonstra no quadro abaixo que contém exemplos de textos traduzidos pelo algoritmo *hash* baseado no padrão SHA-1.

Tabela 1 – Exemplos de hash

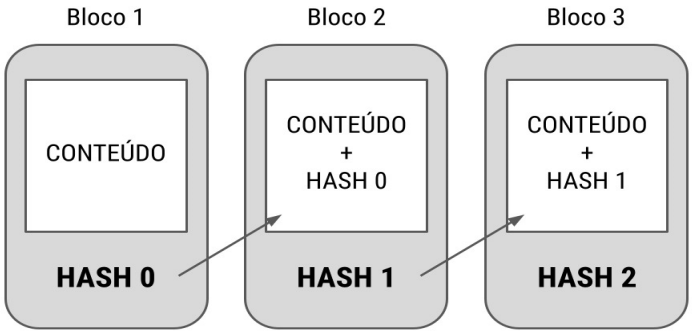
Mensagem	**Texto traduzido pela função hash (Padrão SHA-1)**
Proteção de Dados	c00fc4961c1a5fd19be3f15d3a5e91b4ee68e017
PROTEÇÃO DE DADOS	289e9c6893cb4c875180653df51065b0d5f1989e

Fonte: autoria própria.

Com relação à estrutura dos blocos, tecnicamente, a *Blockchain* consiste em uma cadeia de blocos que contém um conteúdo atrelado a uma espécie de impressão digital. A revolução é que o próximo bloco da cadeia irá conter a impressão digital do bloco anterior e seu próprio conteúdo, o que irá gerar sua própria impressão digital e assim sucessivamente[70].

A título exemplificativo, podemos utilizar a figura abaixo.

Figura 4 – Estrutura da cadeia de blocos



[69] BASHIR, Imran. Mastering Blockchain. 2 ed. Birmingham: Packt, 2018, p. 82. E-book. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1789486&lang=pt-br&site=ehost-live. Acesso em: 04 de maio de 2021.

[70] PRADO, Jean. O que é blockchain: indo além do bitcoin. 2018. Disponível em: <https://tecnoblog.net/227293/como-funcionablockchain-bitcoin/>. Acesso em: 13 de março de 2021.

Fonte: autoria própria.

A impressão digital é conhecida como *hash,* que como já adiantado, consiste em uma função matemática responsável por pegar o conteúdo do bloco e gerar um código formado por número e letra capaz de representar o conteúdo inserido no bloco. Desse modo, o *hash* irá servir como uma assinatura do bloco, no caso de alteração do conteúdo do bloco, o *hash* também muda, tornando possível verificar se um bloco foi alterado.

Para um novo bloco compor uma *Blockchain*, esse novo bloco precisa ser validado através de seu *hash*, enquanto esse novo conteúdo aguarda para ser integrado à rede *Blockchain*, eles permanecem em área denominada de *pool*. Ao mesmo tempo, os dispositivos que compõem a rede competem entre si para achar um bloco válido, ao encontrar esse bloco o dispositivo irá notificar os demais dispositivos da rede para que seja validado o novo bloco e encadeado a rede, esse processo é conhecido como mineração[71].

É extremamente raro e difícil gerar um *hash* idêntico a um *hash* já existente. Com isso, a partir do momento que um bloco é validado, é extremamente custoso criar um segundo bloco, com alguma modificação, que também seja válido. Com essa garantia, a cadeia acaba se tornando praticamente imutável.

Portanto, a *Blockchain* é uma tecnologia que faz uso de uma arquitetura distribuída e descentralizada para registrar transações, impedindo, como regra geral, um registro de ser alterado retroativamente, tornando este registro imutável.

A *Blockchain* pode ser pública ou privada. Na *Blockchain* pública ou não permissionada, os usuários têm acesso às próprias validações por meio de uma rede de nós. Os computadores, por vezes denominados de nós, são responsáveis por guardar os dados de forma definitiva, criando uma cadeia de dados de armazenamento criptografado. Cada novo nó precisa ser confirmado pelos outros nós existentes, ao contribuir com o funcionamento da rede esses usuários são remunerados.

[71] LAGO, Lucas. Blockchain: confiança através de algoritmos. Boletim, vol. 2, n. 4. São Paulo: CEST/USP, 2017.

Por outro lado, na *Blockchain* privada o usuário está em um ambiente que tem um órgão regulamentador, responsável por convidar ou autorizar o usuário a fazer parte, configurando um modelo de rede centralizada e permissionada. Contudo, ainda é possível prover aos usuários uma rede com autenticação, validação e arquitetura criptografada.

Para além das *Blockchains* públicas e privadas, vale ressaltar que modelos híbridos[72] surgiram ao longo do tempo. Uma vez que as *Blockchains* públicas oferecem mais novidades e complicações do ponto de vista da privacidade e da proteção de dados. O foco do presente repousa principalmente nesse modelo.

Passamos agora a uma análise de implicações das possíveis tensões entre as regulações de proteção de dados e a *Blockchain*.

[72] Who are the administrators of blockchains?. Great Wall of Numbers:
Business Opportunities and Challenges in Emerging Markets, 2017. Disponível em: <https://www.ofnumbers.com/2017/10/19/who-are-the-administrators-of-blockchains/>. Acesso em: 12 de março de 2021.

3. SEGUNDA PARTE

3.1. IMPACTOS E TENSÕES ENTRE ÀS REGULAÇÕES DE PROTEÇÃO DE DADOS E A *BLOCKCHAIN*

Desde os primórdios, o avanço tecnológico tornou-se um dos principais responsáveis por transformar a vida humana, e consequentemente a sociedade e todas as relações que ali se constituíam. Desse modo, ao longo da história inúmeros foram os momentos em que o desenvolvimento tecnológico e o Direito estiveram em conflito.

Os direitos trabalhistas, por exemplo, são decorrentes do surgimento das máquinas e do processo industrial que revolucionou as relações entre empregados e empregadores. Recentemente, o surgimento da inteligência artificial já trouxe e promete novos desafios para o Direito, seja no campo da responsabilidade civil de robôs dotados de inteligência artificial ou na produção de obras por sistemas dotados de inteligência artificial. Para Michèle Finck[73], o Direito sempre esteve atrasado em relação às mudanças tecnológicas, mas essa divisão tornou-se mais relevante e aguda à medida que o ritmo de inovação se acelera na Era Digital.

Com a *Blockchain*, esse cenário se repete pelo fato de a tecnologia constituir uma invenção da Era Digital, e portanto, possuir algumas tensões com o Direito. Tendo em vista que não há um grau hierárquico entre o Direito e a tecnologia[74], um não poderá prevalecer sobre o outro, de modo que as leis e regulações devem ser aplicadas, de maneira a não asfixiar o potencial inovador das novas tecnologias.

Uma vez apresentada algumas considerações iniciais acerca das tensões entre Direito e tecnologia, bem como a necessidade harmonizar ambos os conceitos. É necessário avançar para os próximos passos visando entender as principais incongruências entre a *Blockchain* e as legislações europeia e brasileira de proteção de dados pessoais, e na sequência encontrar possíveis caminhos para conciliar as incongruências encontradas.

---

[73] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 28. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 15 de set. de 2021.

[74] MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 68.

Conforme foi visto na primeira parte desse trabalho, a *Blockchain* configura uma tecnologia capaz de registrar e armazenar dados, além de garantir a irretratabilidade, a auditabilidade e a imutabilidade. Ainda, foi visto que a *Blockchain* rompeu com o modelo tradicional de sistemas, ao adotar um sistema descentralizado de armazenamento em que as informações ficam distribuídas em diferentes nós de uma mesma rede, impedindo e dificultando a possibilidade de fraudes e ataques cibernéticos.

Ao mesmo tempo, estudou-se o contexto histórico e a evolução do direito à proteção de dados, bem como as noções, direitos e deveres trazidos pelo Regulamento Geral de Proteção de Dados Pessoais da União Europeia e pela Lei Geral de Proteção de Dados Pessoais. Vale lembrar que ambas as legislações são produtos do uso desenfreado e irresponsável de dados que ocorreu nas últimas décadas.

Analisando a tecnologia e as documentações referidas foi possível encontrar interesses e reflexos positivos do contato entre *Blockchain* e a LGPD e o RGPD, uma vez que, ao fim e ao cabo, ambas pretendem combater abusos e inseguranças decorrentes do tratamento de dados. Além disso, a *Blockchain* pode ser um excelente meio para viabilizar e assegurar os direitos dos titulares de dados previstos nas legislações[75], como conceder ferramentas para os titulares controlarem e fiscalizarem o tratamento de seus dados, garantindo a soberania sobre os dados pessoais que lhes dizem respeito.

No entanto, em que pese existam interesses e finalidades complementares entre as legislações de proteção de dados e a tecnologia, os métodos utilizados por cada uma são distintos e incompatíveis. Nessa perspectiva, a *Blockchain* e os DLT's, de forma geral, configuram estruturas descentralizadas, através de redes *peer-to-peer* e criptografadas. A LGPD e o RGPD, por outro lado, propõem a centralização da informação na mão dos agentes de tratamento e dos encarregados de dados pessoais. De todo modo, antes de identificarmos todos os possíveis pontos de tensão,

[75] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 29. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 15 de set. de 2021.

devemos entender se os dados armazenados em uma DLT configuram dados pessoais.

3.1.1 Dos dados pessoais armazenados na *Blockchain*

Para entender se a *Blockchain* se enquadra nos parâmetros de aplicações do RGPD e da LGPD, deve-se revisitar o conceito de tratamento e de dados pessoais, bem como quais elementos da *Blockchain* que se relacionam com a previsão legal.

Assim, de início é importante lembrar que tanto o RGPD quanto a LGPD, reforçam a ideia de que dado pessoal consiste em uma informação relativa a uma pessoa natural identificada ou identificável. Ou seja, mesmo aquelas informações que precisam ser combinadas com outras informações para identificar o titular dos dados pessoais estão abarcadas no conceito de dado pessoal.

Outro conceito que deve ser relembrado é o de tratamento de dados, que possui definições semelhantes em ambas às legislações analisadas. À luz do RGPD[76], o tratamento de dados pessoais consiste em:

> *"uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição."*

Na Lei Geral de Proteção de Dados Pessoais, o tratamento de dados consiste em:

> "*toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração."*[77]

---

[76] No original: "'Processing' is broadly defined. It refers to any operation or set of operations performed on personal data. As a result, blockchain users, nodes, and miners may engage in processing of personal data when sending, verifying, and storing transaction data. The definition of 'personal data' is also very expansive. It covers any information that relates to an identifiable person, i.e. a person who can be identified "directly or indirectly". To determine whether a person can be indirectly identified, account should be taken of all the means likely reasonably to be used by the controller or by any other party to identify the person."

[77] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de agosto de 2021.

Desse modo, uma vez que a *Blockchain* possibilita o armazenamento, processamento, coleta de dados de qualquer espécie, incluindo dados pessoais, é evidente que esse tratamento de dados deve ser submetido às legislações de proteção de dados específicas.

Ainda sobre o tratamento de dados pessoais na *Blockchain*, é possível observar quais são os dados pessoais possivelmente tratados em uma *Blockchain*. A partir do entendimento dos estudiosos e aplicadores da tecnologia[78], sabe-se que a maior parte de informações está contida e registrada diretamente no conteúdo dos blocos da rede, tais dados são denominados de dados transacionais. Desse modo, toda informação contida nos blocos de uma cadeia passível de vinculação a uma pessoa natural, configura uma hipótese de tratamento de dados pessoais.

Além dos blocos das redes, os dados pessoais podem ser tratados dentro das *Blockchain* através das chaves públicas.[79] Assim como na maioria dos sistemas, um usuário integrante de uma rede *Blockchain*, deve confirmar sua identidade por meio de criptografia assimétrica, que funciona com uma prova de compatibilidade entre uma chave privada e uma chave pública.

Os dados presentes em uma chave pública não podem ser atribuídos a um indivíduo específico, a menos que seja combinado com alguma informação adicional, tal como um nome ou um endereço. Onde estes dois conjuntos de informação são combinados, a identificação é plausível, explicando a razão pela qual as chaves públicas não podem ser qualificadas como dados anônimos. Nesse contexto, as chaves públicas funcionam como endereços de IP ou *cookies* de navegação, que podem deixar vestígios quando combinados com outras informações, as legislações entendem essa mecânica como uma “pseudonimização”. Sobre o assunto, Finck[80] expõem que:

---

[78] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 29. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[79] FINCK, Michèle. Blockchain and Data Protection in the UE. Max Planck Institute for Innovation and Competition Research Paper nº 18-01, 2017, p. 14. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322.> Acesso em: 18 de out. de 2021.

[80] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 29. Disponível em:

> A prática revela que chaves públicas podem permitir a identificação de uma pessoa natural específica. Houve exemplos nos quais titulares de dados foram vinculados a chaves públicas através da disposição voluntária de sua chave pública para receber fundos; por meios ilícitos ou quando informação adicional foi coletada de acordo com requisitos regulatórios, como quando a troca de criptoativos efetivam deveres de conhecimento sobre os clientes e combate à lavagem de dinheiro. Serviços de carteiras [digitais] ou corretoras podem de fato precisar armazenar identidades de partes do mundo real a fim de cumprir com requisitos de combate à lavagem de dinheiro enquanto as contrapartes poderão fazê-lo também por interesses comerciais próprios. A combinação de tais registros com a chave pública poderia, portanto, revelar a identidade do mundo real que se encontra escondida atrás de endereços da blockchain.[81]

Sem o prejuízo de outras formas de dados pessoais serem encontradas em uma *Blockchain*, tendo em vista o largo escopo de atuação dessa tecnologia, os componentes referidos acima são aqueles que possuem dados pessoais capazes de identificar uma pessoa natural. Evidente que outros tipos de dados poderão ser encontrados em uma *Blockchain*, caso dos dados impessoais que consistem em meras informações e os dados pessoais anonimizados.

Nesse sentido, vale lembrar os conceitos e definições trazidos pelas legislações estudadas de dados anonimizados, trata-se daquele tipo de dado que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa[82]. Dentro de uma *Blockchain* a criptografia assimétrica e as funções *hash* se aproximam do conceito de anonimização de dados trazidos pela legislação.

Como já foi referido anteriormente, a criptografia de chave pública ou assimétrica consiste no método utilizado para encriptar informações através de uma chave pública, nesse sentido, a decodificação só é possível através da chave privada

---

https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[81] No original: “Practice reveals that public keys can enable the identification of a specified natural person. There have been instances where data subjects have been linked to public keys through the voluntary disclosure of their public key to receive funds; through illicit means, or where additional information is gathered in accordance with regulatory requirements, such as where cryptoasset exchanges perform Know Your Customer and Anti-Money Laundering duties. Wallet services or exchanges may indeed need to store parties' real-world identities in order to comply with Anti-Money Laundering requirements while counter parties may do so, too for their own commercial purposes. The combination of such records with the public key could thus reveal the real-world identity that lies hidden behind a blockchain address.”

[82] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de out. de 2021.

do processo de encriptação. Desse modo, a técnica de criptografia por chave pública se assemelha ao processo de anonimização previsto nas legislações de proteção de dados, uma vez que para terceiros não detentores de ambas as chaves, os dados pessoais protegidos por essa técnica não podem ser relacionados a qualquer pessoa, já que não é possível compreender o conteúdo por trás da criptografia. Em outra perspectiva, os dados podem ser considerados dados pessoais, tendo em vista o indivíduo detentor das chaves de decodificação pode decifrar as informações, e portanto, relacionar eventuais dados pessoais com seus titulares de dados pessoais.[83]

A segunda técnica criptográfica, com maior expressividade na tecnologia, é a função *hash*. As funções de *hash*, como já visto anteriormente, consistem em um algoritmo matemático responsável por transformar um dado, seja ele um arquivo, senha, ou qualquer tipo de informação, em um conjunto alfa numérico com cumprimento fixo de caracteres. Outra distinção é a de que seu processo de encriptação é irreversível, ou seja, trata-se de uma técnica criptográfica unidirecional algo que, por si só, já afasta as ressalvas do RGPD e da LGPD.

No contexto da proteção de dados, a função *hash* é uma representação clara de um mecanismo de pseudononimização. Considerando que função *hash* é uma via de mão única em que não há possibilidade de ser submetido engenharia reversa ao processo, parece apresentar mais evoluções e garantias para privacidade, no entanto, os dados pessoais criptografados ainda podem ser qualificados como dados pessoais. O Grupo de Trabalho do Artigo 29[84], entendeu que a função *hash* é uma técnica de pseudononimização e não de anonimização, uma vez que ainda é possível vincular o conjunto de dados criptografados ao titular de dados pessoais, pois acaba assumindo as características de um dado pessoal, eis que "*ainda é possível rastrear transações até uma identidade específica por meio das técnicas analíticas de blockchain*"[85]. Justamente por isso dados criptografados por meio de funções *hash* não se

[83] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 29. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[84] Article 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, 20.

[85] PARIZI, Reza M. et al. Integrating Privacy Enhancing Techniques into Blockchains Using Sidechains. In: IEEE CANADIAN CONFERENCE ON ELECTRICAL AND COMPUTER ENGINEERING (CCECE 2019), 32., 2019, Edmonton. Sessão Especial – 2 nd International Workshop on Blockchain-oriented Cyber Security, Nova Iorque: IEEE, 2019, p. 1.

compatibilizam com dados anonimizados, mas melhor assumem a condição de dados pseudononimizados, conforme o critério estabelecido no artigo 13 da LGPD e considerando 28 do RGPD, uma vez que, em conjunto com informações adicionais, podem reerguer a ponte entre o dado e seu titular.

Portanto, percebe-se que os dois métodos de anonimização existentes no conceito tradicional de *Blockchain* podem, em determinados momentos, garantir de fato a proteção dos dados, entretanto, como observado em ambos os contextos, são passíveis de falha nesse propósito específico. Apesar disso, a ferramenta não se limita apenas a essa formatação, de modo que, influenciado pelo movimento europeu de proteção de dados, cada vez surgem mais propostas de melhoramentos na dinâmica de processamento da informação, visando maior resguardo e proteção aos dados pessoais.

Alguns estudiosos apontam como uma das alternativas ao problema narrado a criação de uma base de dados paralela e fora da *Blockchain* [86], conciliando, assim, as técnicas de *side chain* e *off chain*, na qual se registrariam os dados pessoais, protegidos por meio da criptografia. Nessa nova formatação, a *Blockchain* apenas armazenaria a informação necessária para acessar e descriptografar os dados registrados em banco de dados comum paralelo, possibilitando a retificação e apagamento de dados pessoais com maior facilidade, tornando a *Blockchain* compatível com o próprio direito ao apagamento ou à eliminação de dados, positivado no RGPD europeu no artigo 17, e na LGPD brasileira no artigo 16.

Embora se sinalize um ponto de congruência da *Blockchain* com a disciplina da proteção de dados, em uma DLT ou um sistema distribuído de registro de dados ainda é possível visualizar outros empecilhos para o processo de conciliação das legislações de proteção de dados com a *Blockchain*.

3.1.2. Dos agentes de tratamento de dados em uma *Blockchain*

O RGPD e, posteriormente, a LGPD foram concebidos em uma conjuntura em que o processamento de dados pessoais concentrava-se em uma entidade específica, nesse sentido, havia uma figura central responsável pela gestão dos dados pessoais.

---

[86] BACON, Jean; MICHELS, Johan D.; MILLARD, Christopher; SINGH, Jatinder. Blockchain Demystified: An introduction to blockchain technology and its legal implications. Londres: Queen Mary School of Law Studies, 2017, n. 268, p. 41. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218. Acesso em 28 de out. de 2021.

Entretanto, ocorre que o modelo adotado pela tecnologia *Blockchain* consiste em uma tecnologia pautada em um modelo descentralizado, em que a troca de informações não se limita a um banco de dados centralizados, mas sim, em um banco de dados distribuídos entre múltiplos dispositivos e conectados a uma rede descentralizada. Desse modo, pode-se verificar alguns empecilhos para compreender e identificar alguns conceitos essenciais trazidos pelas legislações mencionados.

Conforme já mencionado na primeira parte deste estudo, tanto o RGPD, quanto a LGPD trazem consigo três figuras que são responsáveis pelo tratamento de dados pessoais. No regulamento europeu, os agentes de tratamento são classificados como *controllers* (controladores), *processors* (processadores) e *data protection officers* (oficiais de proteção de dados), nessa mesma ordem esses atores são denominados, na legislação brasileira, de controladores, operadores e encarregados. Assim, tendo em vista o caráter descentralizado de uma rede *Blockchain*, livre de figuras centrais responsáveis pelo controle e tratamento de dados, identificar quem são essas figuras trazidas pelas legislações de proteção de dados não parece ser uma tarefa fácil. Desse modo, deve-se analisar cada uma dessas figuras visando realizar associações com alguns dos agentes que podem ser encontrados em uma *Blockchain*.

Considera-se controlador de dados pessoais à luz do RGPD,

> "*a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.*"[87]

[87] UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

De maneira extremamente semelhante, a norma brasileira identifica o controlador de dados, como o agente de tratamento a quem competem as decisões referentes ao tratamento de dados pessoais[88].

Nessa linha, em face dessas definições e para este estudo, entende-se por controladores os sujeitos que determinam as finalidades e os meios utilizados no tratamento de dados, também denominados de *nodes*. Conforme aponta estudo da autoridade francesa de proteção de dados[89], os participantes da *Blockchain* que podem adicionar informações e transacionar na *Blockchain* podem ser considerados como controladores de dados, uma vez que estão aptos a definir as finalidades e os meios pelos quais se darão o processamento de dados pessoais na rede. Por exemplo, se um notário registrar a escritura de propriedade de seu cliente na *Blockchain*, o notário estará adotando a postura de controlador dos dados pessoais de seus clientes.

Vale destacar que não são todos os intervenientes envolvidos em uma *Blockchain* que podem ser considerados controladores. Os mineradores, responsáveis pelo processo de inclusão e validação dos dados dentro de uma *Blockchain*, na maior parte dos casos, não possuem influência acerca das finalidades que levaram à inclusão de novos blocos em uma cadeia, e portanto, não podem ser considerados controladores, pois preocupam-se em manter o sistema operando e não em incluir dados e informações nas correntes de blocos. Na visão de Finck[90], os mineradores são meros servos do sistema, o que eliminaria a possibilidade de caracterizá-los como controladores.

Além disso, Finck[91] aponta que que podem ser caracterizados como controladores os usuários das redes *Blockchain*, que não constituem um nó da rede,

---

[88] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de out. de 2021.

[89] Commission Nationale Informatique & Libertés. Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. 2018, p. 1. Disponível em: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Acesso em: 25 de out. 2021.

[90] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 46. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[91] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019,

mas decidem submeter transações à uma *Blockchain*. No entanto, o autor do presente trabalho que os usuários das redes não podem necessariamente serem considerados controladores de dados à luz das legislações. Uma vez que, consubstanciado no art. 2º do RGPD e no art. 4º da LGPD, as normas não se aplicam quando o tratamento de dados é efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, e realizado por pessoa natural para fins exclusivamente particulares e não econômicos, respectivamente.

Por exemplo, à luz do regulamento europeu, uma pessoa que compre ou vende *Bitcoin*, por conta própria não pode ser considerada controladora de dados pessoais. No entanto, a referida pessoa pode ser considerada uma controladora de dados se estas transações forem realizadas como parte de um profissional ou atividade comercial, em nome de outras pessoas singulares.[92]

Outro agente de relevância para as legislações de proteção de dados, é o processador ou operador de dados pessoais. Tanto no RGPD, quanto na LGPD, o operador possui uma carga de responsabilidade menor em relação ao tratamento de dados, tendo em vista que consiste na pessoa que realiza o tratamento de dados pessoais em nome do controlador. Cabe destacar que em alguns casos a figura do operador não existirá, dado que seu papel será absorvido pelo próprio controlador, de modo que, assim como no caso do controlador sua identificação deve ser feita caso a caso.

É possível identificar a figura dos operadores no denominado *smart contracts* em que há tratamento de dados pessoais em nome dos controladores. A título exemplificativo e em consonância com o estudo da CNIL[93], podemos pensar em um programador de software que oferece uma solução a uma companhia de seguros sob a forma de *smart contracts*, permitindo reembolso automático no caso de atrasos. O

p. 46. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[92] CNIL: Commission Nationale Informatique & Libertés. Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. 2018, p. 2 . Disponível em: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Acesso em: 25 de out. 2021.

[93] CNIL: Commission Nationale Informatique & Libertés. Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. 2018, p. 2-3. . Disponível em: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Acesso em: 25 de out. 2021.

principal agente responsável pelo tratamento de dados é a companhia de seguros, qualificada na pessoa de controlador, já o agente responsável por executar as ações do controlador é desenvolvedor de softwares.

Na acepção da legislação brasileira e europeia, pode-se considerar os mineradores como operadores[94], tendo em vista suas funções se restringem ao cumprimento de comandos pré-estabelecidos.

Por fim, com relação aos DPOs ou Encarregados - sujeitos responsáveis por atuar como canal de contato entre os controladores e operadores, os titulares de dados e as autoridades, trata-se, portanto, de um papel mais institucional do que operacional. No âmbito das *Blockchain* privadas, é de fácil visualização e implementação permitir com que a rede funcione com a presença do Encarregado. Por outro lado, no âmbito das *Blockchains* públicas, não há estudos e propostas acerca do funcionamento das noções legais previstas ao Encarregado.

Por fim, superado algumas problemáticas iniciais do presente trabalho, como, os dados pessoais contidos em uma *Blockchain* e os agentes de tratamento de dados em uma *Blockchain*, passa-se agora a temática central do presente trabalho, isto é, a possibilidade de conciliar o uso da tecnologia *Blockchain* com as novas legislações de proteção de dados, sobretudo, no atinente ao direito ao apagamento de dados pessoais.

3.1.3. Exclusão de dados pessoais na *Blockchain*

O regulamento europeu, bem como a lei brasileira foram concebidas com o intuito de devolver aos indivíduos a possibilidade de controlar o tratamento dos dados pessoais que lhe dizem respeito. Acerca do tema, vale dizer que a tecnologia *Blockchain* pode ser uma fonte de dificuldades para os agentes de tratamento cumprirem as obrigações previstas no RGPD e na LGPD. Embora o exercício efetivo de alguns direitos não pareça ser problemático, a aplicação do direito ao apagamento pode representar um empecilho para o cumprimento de algumas legislações.

O direito de informação dos titulares de dados não é causa do problema, tendo em vista que o responsável pelo tratamento de dados deve fornecer informações

[94] CNIL: Commission Nationale Informatique & Libertés. Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. 2018, p. 3 . Disponível em: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Acesso em: 25 de out. 2021.

concisas, facilmente acessíveis e formuladas em termos claros para a pessoa a quem os dados dizem respeito antes de submeter dados pessoais para validação em uma *Blockchain*. O mesmo entendimento se aplica para o direito de acesso e o direito à portabilidade de dados, inclusive, a CNIL[95] considera que o exercício destes direitos é compatível com as propriedades técnicas da *Blockchain*.

Acerca da eliminação dos dados, além de uma consequência natural do término do tratamento dos dados, é um direito garantido ao titular, nos termos dos artigo 17 do RGPD e 16 e 18, inciso VI, da LGPD, como uma expressão da autodeterminação informativa[96], isto é, a liberdade do indivíduo em decidir acerca da divulgação e utilização de seus dados pessoais. Trata-se do processo de exclusão realizado através de qualquer procedimento. Contudo, na legislação brasileira assim como a norma europeia, não há maiores contornos sobre o que viria a significar esse apagamento.

Para Finck[97], a concepção do termo deveria considerar o senso comum, que envolve a ideia de destruição do dado, o que, todavia, não é nada simples em DLTs como a *Blockchain*. Sobre o termo, no julgamento do caso Google Spain versus Mario Costeja e Agência Espanhola de Proteção de Dados[98], o Tribunal de Justiça Europeu entendeu que a desindexação de dados pessoais dos mecanismos de busca na internet atinge a finalidade de exclusão de dados, conforme é sabido, o processo de desindexação dos dados pessoais limita-se a dissociação de determinadas informações dos motores de busca da internet. Desse modo, mesmo que os dados pessoais continuem existindo de alguma forma, pode-se considerar tais dados

---

[95] CNIL: Commission Nationale Informatique & Libertés. Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. 2018, p. 8 . Disponível em: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Acesso em: 25 de out. 2021.

[96] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 75. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[97] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 46. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[98] UNIÃO EUROPEIA. Tribunal de Justiça Europeu. Grande Secção. Pedido de Decisão Prejudicial C-131/12. Google Spain SL e Google Inc. Agência Española de Protección de Datos (AEPD). Relator: M. Ilešič. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131. Acesso em 28 de set. de 2021.

pessoais como excluídos, uma vez que o controlador do tratamento de dados chegou ao limite de suas possibilidades para apagar o dado.

A Autoridade Austríaca de Proteção de Dados, por sua vez, ao tratar do tema da exclusão de dados, concederam maior liberdade de escolha dos meios ao controlador.[99] Tendo em vista que as legislações de proteção não costumam trazer uma definição tão clara do que de fato se considera eliminação de dados, a Autoridade assentou o entendimento de que o próprio processo de anonimização, responsável por remover ou modificar informações que podem caracterizar uma pessoa, é suficiente para o cumprimento do dever de exclusão dos dados pessoais[100]. Nota-se que no caso em questão, não se eliminou especificamente o dado pessoal, mas sim o elo de união entre o dado e seu titular[101].

Entretanto nenhuma das decisões e casos expostos aqui referem-se especificamente ao contexto das *Blockchains*. Logo, enquanto não há um pronunciamento oficial das autoridades de proteção de dados, todo o processo interpretativo e reflexivo deve ser feito através de analogias baseadas em características de sistemas tradicionais, como a computação em nuvem, que encontram algumas similaridades com as tecnologias de DLT[102].

Pode-se citar o modelo chamado MyHealthMyData, que consiste, em uma *Blockchain* privada que trata dados pessoais sensíveis, trata-se de um *smart contract* capaz de não somente validar operações, mas também de armazenar e criar uma rede de dados da saúde centrada no paciente, que poderá ser usada em diversas aplicações, tais como pesquisas acadêmicas, hospitais, laboratórios e indústria farmacêutica. Nessa rede,

---

[99] MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 91.

[100] ÁUSTRIA. Autoridade Austríaca De Proteção De Dados. Reclamação DSB-D123.270/0009-DSB/2018. Reclamante: Dr. Xaver X. Reclamado: AG. 2018. Disponível em: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_2 70_0009_DSB_2018_00.pdf. Acesso em: 19 de out. de 2021.

[101] MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 91.

[102] MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 91.

> *"Cada usuário possui um catálogo de dados próprio, onde são armazenados os dados pessoais. Cada catálogo individual alimenta um registro central e público (a blockchain em si) com as informações neles armazenadas, entretanto não é registrado o dado em si, mas seu hash."*[103]

Assim, para alguns autores *"a blockchain mantém registros dos dados disponíveis e seu histórico associado sem a necessidade de gravar os dados pessoais em acordo com o RGPD"*.[104] No que tange à exclusão dos dados do MyHealthData, o processo é alcançado por meio da exclusão do dado inserido, que tem como consequência quebra do elo entre os dados registrados na *Blockchain* e os presentes no catálogo individual[105].

Outra alternativa, recomendada por Moslavac[106] e idêntico ao modelo de Bayle, consiste no armazenamento de dados pessoais fora da rede, guardando nela apenas os *hashe*s dos dados para posterior checagem. Soluções mais concretas já existem, como é o caso da Lition, uma infraestrutura de dupla camada baseada na rede Ethereum, composta por uma cadeia paralela privada, também denominada de sidechain, para armazenamento de dados pessoais, que permite a exclusão de dados e opera de modo independente à rede sobre a qual foi construída.

Outra possível alternativa, é mencionada por Finck,[107] e frequentemente considerada nos estudos a respeito, que está baseada na eliminação definitiva das chaves privadas que dão acesso aos dados pessoais criptografados. Dessa forma, com a eliminação da chave privada capaz de descriptografar as informações, e consequentemente, os dados pessoais em uma rede *Blockchain*, é possível com que os dados pessoais criptografados permaneçam inteligíveis ao olhar do controlador ou

---

[103] MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 92.

[104] MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 92.

[105] MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021, p. 92.

[106] MOZLAVAC, Bruno. Consent by GDPR vs. Blockchain. Revista Acadêmica Escola Superior do Ministério Público do Ceará, Fortaleza, ano XII, n. 1, p. 149-166, jan.-jun. de 2020, p. 159. Disponível em: http://www.mpce.mp.br/wp-content/uploads/2020/08/ARTIGO-149-166.pdf. Acesso em 30 de set. de 2021.

[107] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 66. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

de terceiros e sem influenciar o funcionamento do restante da rede. Cumpre destacar que com a eliminação da chave privado, os dados pessoais ainda existirão dentro da rede *Blockchain*, no entanto, não apresentarão maiores riscos.

Finck[108], com base na experiência da jurisprudência europeia, entende que dados armazenados em múltiplos locais devem ser de todos removidos quando houver uma determinação de exclusão de dados. Assim, se um controlador dentro de uma *Blockchain* recebe ordem ou pedido de exclusão de certo dado pessoal, ele deveria proceder ao solicitado em todos os dispositivos da cadeia, todavia ainda não existe um caminho claro para tal operação. Tendo em vista, em redes como a *Blockchain* faltam *"mecanismos de comunicação e coordenação entre os atores relevantes*"[109], essa carência é resultado de um sistema descentralizado sem figuras centrais capazes de garantir que todos os dispositivos da rede acatem determinadas condutas e ações. Além disso, mesmo que fosse possível garantir que todos os dispositivos das redes adotassem determinadas condutas e comportamentos, como já foi relatado anteriormente, poderiam surgir dificuldades técnicas para implementar tais ações, como, por exemplo, o apagamento de determinados dados pessoais contidos em uma *Blockchain*.

Portanto, o direito à eliminação/apagamento de dados, nos termos dos artigos 17 do RGPD e 16 e 18, inciso VI, da LGPD, dificilmente seria garantido no âmbito de uma *Blockchain*, uma vez que, atualmente, não existem técnicas capazes de garantir, de fato, a exclusão dos dados, apenas bloquear o acesso através de técnicas de criptografia.

Vale lembrar, por fim, que isso não é algo generalizável, e conforme entendem alguns estudiosos, deve ser analisado em cada caso concreto. Entretanto, é perceptível que as controvérsias existentes no tocante a conciliação do direito ao apagamento de dados pessoais e a tecnologia *Blockchain* evidenciam a necessidade

---

[108] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 77. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[109] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 77. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

de adequação das políticas de governança das tecnologias de registro distribuído, a fim de sanar as dificuldades advindas da concepção de uma *Blockchain* e criar modelos capazes de garantir o direito à privacidade e proteção de dados. De toda forma, e conforme em vários momentos se verifica, o cenário atual é otimista, uma vez que as *Blockchains* possuem uma considerável flexibilidade em atender às demandas originadas das normas de proteção de dados, podendo sofrer modificações que, em sua maioria, não alteram suas principais características, mas permitem que haja um cenário em que as tecnologias e a legislações possam coexistir.

3.2. DA CONCILIAÇÃO DOS DIREITOS FUNDAMENTAIS À PROTEÇÃO DE DADOS E DA PROMOÇÃO À INOVAÇÃO

A *Blockchain* e as legislações de proteção de dados ao redor do mundo estão em tensão. Enquanto que a LGPD e o RGPD foram moldados para uma era de dados centralizados com figuras centrais responsáveis pelo tratamento de dados, a tecnologia *Blockchain* promete um futuro de gestão descentralizada de dados, sem entes e figuras centrais. De maneira que, antes mesmo das legislações analisadas entrarem em vigor, já estavam desatualizadas no que diz respeito às tecnologias de registro distribuído, tendo em vista que alguns dos conceitos trazidos pelas legislações são de difícil aplicação no âmbito da tecnologia estudada.

De forma análoga, essas tensões também podem ser encontradas se analisarmos os fenômenos da *big data* e da inteligência artificial, uma vez que com o avanço tecnológico e o ritmo de inovação crescente, torna-se mais aguda as discrepâncias entre as legislações e a inovação tecnológica. Conforme visto nos capítulos anteriores, o RGPD, bem como a LGPD, possui conceitos e características que não podem ser aplicados facilmente à *Blockchain*. Em contrapartida, verificou-se que a tecnologia *Blockchain* e as legislações europeia e brasileira podem partilhar objetivos comuns, como, por exemplo, conceder ao titular dos dados controle sobre seus dados.

Sendo assim, o desafio reside em fazer com que a lei e a tecnologia andem juntas para garantir que a lei não impeça o progresso tecnológico, e que o progresso tecnológico se desenvolva numa forma normativamente desejável, isto é, resguardando os direitos de proteção de dados e garantindo aos titulares de dados mais soberania sobre seus dados pessoais. No contexto do presente trabalho, o desafio consiste em aplicar as legislações de proteção de dados, sem interferir negativamente no potencial inovador da *Blockchain* e ao mesmo tempo assegurar a proteção de dados através dela. Considerando que os direitos fundamentais à proteção de dados e a promoção da inovação são objetivos da União Europeia e do Brasil, deve ser adotada uma interpretação intencional das leis sempre que possível.

Assim, embora estejamos habituados a ver a tecnologia e a privacidade como antagonistas, o futuro pode colocar ambos como aliados. À luz do cenário europeu

onde a discussão encontra-se mais evoluída, a Comissão Europeia afirmou que o RGPD é uma legislação neutra que permitirá "a inovação continuar a prosperar"[110]. Até mesmo um dos mais ferozes defensores da proteção de dados têm argumentado que embora o RGPD vá mudar "*o mundo tal como o conhecemos*"[111], entende também que é possível alcançar um campo comum respeitando os direitos dos cidadãos e dos consumidores, bem como um competitivo e inovador mercado único.

Se for moldado apropriadamente, uma DLT não prejudica o objetivo da privacidade e da proteção de dados resguardados pelas legislações, mas muda os meios da sua realização. A Autoridade Europeia para a Proteção de Dados reconhece que ainda que "*as tecnologias avançadas aumentem o risco para a privacidade e proteção de dados, podem também integrar soluções tecnológicas para melhor transparência e controle para as pessoas cujos dados são processados*"[112]. Por conseguinte, à medida que se desenvolve uma indústria de *Blockchains* na União Europeia, os reguladores não devem evitar a utilização dos mecanismos à sua disposição para assegurar que a tecnologia evolua em uma forma normativamente desejável. A relação entre a lei e a inovação é multifacetada, por um lado, exige uma proteção de dados rigorosa na UE, por outro, pode funcionar como um incentivo para refinar a proteção da privacidade em tecnologias de registro distribuído e desenvolver uma indústria correspondente na UE. Desde que seja dada aos inovadores a flexibilidade necessária, o RGPD poderia estimular a inovação para evoluir numa direção compatível com as diretrizes públicas impostas. Para que isto se concretize, a discussão e a aprendizagem mútua entre a indústria e os decisores políticos não pode ser evitada.

Nesse contexto, em seu Relatório Anual de 2017[113], o Supervisor Europeu de Proteção de Dados indicou que é essencial que os estudiosos em proteção de dados comecem a examinar os conceitos por detrás da tecnologia *Blockchain* e como ela é implementada, de modo a compreender melhor como os princípios da proteção de dados podem ser aplicados. Uma parte integrante deste processo deve ser o

---

[110] EUROPEAN COMISSION, 'Questions and Answers – Data Protection Reform' (Press Release, 21 December 2015).
[111] ALBRECHT, Jan Philipp Albrecht. 'How the GDPR will change the World' (2016) 2 European Data Protection Law Review 287.
[112] Aprofundar em: https://edps.europa.eu/data-protection/our-work/technologymonitorin
[113] EUROPEAN DATA PROTECTION SUPERVISOS. Anual Repport, 2016 , p.43.

desenvolvimento de uma *Blockchain* favorável à privacidade, com base nos princípios de Privacy by design.

Aos olhos do RGPD, o ónus da gestão de dados pessoais é de responsabilidade dos controladores e operadores que manipulam dados pessoais. Com a inovação tecnológica, a *Blockchain* pode, no entanto, transformar os indivíduos em soberanos de dados que podem eles próprios, copiar, mudar, partilhar, mover os seus dados. Por sua vez, os órgãos reguladores devem cobrar e incentivar fortemente o desenvolvimento de *Blockchains* adequadas à proteção de dados, tendo em vista que, embora um certo grau de transparência numa DLT seja inevitável, a transparência só é inevitável na camada mais básica da tecnologia, podendo ser construídas camadas adicionais de encriptação e ofuscação para proteger os dados pessoais.

Nessa linha, o futuro parece ser promissor para o desenvolvimento de *Blockchains* compatíveis com as diretrizes globais de proteção de dados pessoais, para fins de anonimização. A primeira alternativa denominada de Prova de Conhecimento Zero[114] consiste em uma forma de registro onde somente o registro da transação é divulgado publicamente na *Blockchain*, de modo que, os dados, os sujeitos e objeto da transação não são divulgados, tal método já foi referendado pelo Parlamento Europeu como uma forma de anonimização. Ainda, outra alternativa vista com bons olhos pelo Grupo de Trabalho do Artigo 29 do RGPD[115], trata-se da adição de ruídos aos dados, a partir do agrupamento de diversas transações e informações aleatórias, ou seja, acrescenta-se um conjunto de dados que aparentemente é inconsistente com o restante dos dados já existentes, pois não segue o mesmo padrão dos demais, impedindo e dificultando a identificação dos sujeitos envolvidos.

---

[114] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 32-33. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

[115] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019, p. 34. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 18 de out. de 2021.

Em relação ao cenário nacional, as discussões acerca da conciliação entre a Lei Geral de Proteção de Dados Pessoais e a tecnologia *Blockchain* são superficiais e, em sua maioria, repetem as tendências europeias. No entanto, a *Blockchain* tem ganhado força e sido cada vez mais usada no Brasil, o que deve intensificar e aflorar mais discussões acerca do tema.

Evidente que, apenas o tempo poderá confirmar o potencial da *Blockchain* para a soberania de dados, até o presente momento o autor não tem conhecimento do desenvolvimento de *Blockchains* para garantir a soberania dos dados aos titulares. Nesse contexto, os responsáveis por interpretar e aplicar a legislação não devem confiar cegamente que a tecnologia *Blockchain* garantirá a soberania de dados, devem, portanto, atuar como fiscalizadores, mas também incentivadores do avanço tecnológico.

4. CONSIDERAÇÕES FINAIS

Conforme exposto ao longo do presente trabalho, com a consolidação da Era Digital, decorrente do desenvolvimento de novas tecnologias, intensificou-se o uso, o processamento e o armazenamento de dados, o que em um primeiro momento acabou trazendo benefícios para os cidadãos em geral, mais tarde gerou riscos e malefícios. Por decorrência disso, reportagens e casos envolvendo vazamentos de dados tornaram-se cada vez mais comuns e ganharam espaço frequente em manchetes das grandes mídias analógicas e digitais.

Dessa forma, por consequência desse uso desenfreado de dados, bem como dos riscos e malefícios atinentes a esse fenômeno, diversas legislações e regulações de proteção de dados surgiram e se atualizaram ao redor do mundo nos últimos anos. Tais normativas visavam impor medidas para o tratamento de dados pessoais que se intensificava com o desenvolvimento de novas tecnologias, como é o caso da tecnologia *Blockchain*.

Por essa razão, ao longo deste trabalho, procurou-se analisar a possibilidade ou não de conciliar o uso da tecnologia *Blockchain* com as legislações brasileira e europeia de proteção de dados, principalmente no que diz respeito ao direito ao apagamento de dados pessoais.

Na primeira parte do trabalho, foram objeto de estudo o Regulamento Geral de Proteção de Dados da União Europeia e a Lei Geral de Proteção de Dados Pessoais do Brasil. Para isso, procurou-se compreender a perspectiva histórica e a construção de ambas as legislações, bem como conceitos e institutos fundamentais para discussão trazidos pelas regulações, tais como: dado pessoal, dado anonimizado, tratamento de dados, bases legais de tratamento de dados e entre outros. Nessa mesma linha, deu-se um enfoque especial para o direito ao apagamento de dados trazido por ambas as legislações, bem como a expressão direito a ser esquecido trazida pela legislação europeia nesse mesmo instituto.

Ainda, em um momento preliminar do trabalho, analisou-se a tecnologia *Blockchain*, a fim compreender no que consiste e qual a dinâmica de funcionamento da *Blockchain*, como também técnicas de criptográficas de informações dentro de uma *Blockchain* e as diferentes espécies da tecnologia.

A partir disso, no segundo ponto, fazendo-se uma intersecção dos estudos aprendidos acerca da *Blockchain* e da proteção dados, constatou-se que a *Blockchain* está sujeita à aplicação do RGPD e da LGPD, tendo em vista que pode haver tratamento de dados pessoais, tanto no conteúdo dos blocos, como nas denominadas chaves públicas de uma rede. Ademais, identificou-se que devido ao caráter descentralizado da *Blockchain*, podem existir algumas dificuldades para identificar dentro de uma rede *Blockchain* os agentes de tratamento de dados trazidos pelas legislações e uma vez identificado cumprir as diretrizes previstas na lei. Já no tocante à problemática principal do presente trabalho, identificou-se algumas possíveis dificuldades para garantir o direito ao apagamento de dados ao titular de dados pessoais presentes em uma *Blockchain*, tendo em vista o caráter imutável da tecnologia.

Assim, uma vez identificada às questões controvertidas, analisou-se de que forma as *Blockchains* poderiam ser compatíveis com as legislações de proteção de dados e o direito ao apagamento de dados nelas previsto. A partir do posicionamento da literatura, da jurisprudência e das autoridades de proteção de dados, constatou-se ser possível conciliar a nova tecnologia com as regulações. Para isso, conclui-se que as técnicas de *side chain* e *off chain* são aliados importantes para possibilitar a retificação e o apagamento de dados, outra via, seria utilização de criptografia irreversível para garantir a anonimização dos dados pessoas.

Embora seja possível encontrar alguns pontos de congruência entre as legislações de proteção de dados e a *Blockchain*, no atinente ao direito ao apagamento, outros empecilhos podem ser encontrados. Nesse sentido, conforme verificou-se na última parte do estudo, é necessário que a lei e o avanço tecnológico andem em juntos em uma mesma direção, a fim de que as leis e resoluções não impeçam o progresso científico e que, ao mesmo tempo, o progresso científico evolua de uma forma normativamente desejável. No caso tela, um caminho normativamente desejável consiste em conceder ao titular de dados pessoais, através do caráter revolucionário e inovador da *Blockchain*, a soberania sobre seus dados pessoais.

Por fim, vale destacar que as discussões e estudos acerca do tema ainda são escassos e merecem aprofundamento, bem como pronunciamentos e pareceres técnicos das autoridades responsáveis ao redor do mundo. É de suma importância

também que as discussões e análises avancem do campo teórico para o prático, visando a construção e a implementação de mecanismos a partir da *Blockchain* que concedam e resguardem aos titulares de dados a soberania sobre seus dados pessoais novamente.

REFERÊNCIAS

ALBRECHT, Jan. P. How the GDPR Will Change the World. European Data Protection Law Review, [s. l.], v. 2, n. 3, 2016. Disponível em: https://edpl.lexxion.eu/article/edpl/2016/3/4/display/html. Acesso em 27 de nov. de 2020.
[1] BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

ALEXY, Robert. Teoria dos Direitos Fundamentais. São Paulo: Malheiros, 2015. p. 99 e ss.

AMER, Karim; NOUJAIM Noujaim. 2019. **The Great Hack**. Estados Unidos: Netflix.

ARTICLE 29 WORKING PARTY, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, 20.

ÁUSTRIA. Autoridade Austríaca De Proteção De Dados. Reclamação DSB-D123.270/0009-DSB/2018. Reclamante: Dr. Xaver X. Reclamado: AG. 2018. Disponível em: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_2 70_0009_DSB_2018_00.pdf. Acesso em: 19 de out. de 2021.

BACON, Jean; MICHELS, Johan D.; MILLARD, Christopher; SINGH, Jatinder. Blockchain Demys1tified: An introduction to blockchain technology and its legal implications. Londres: Queen Mary School of Law Studies, 2017, n. 268. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218. Acesso em 28 de out. de 2021.

BASHIR, Imran. Mastering Blockchain. 2 ed. Birmingham: Packt, 2018. E-book. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1789486&lang=pt-br&site=ehost-live. Acesso em: 04 de maio de 2021.

BRASIL. Câmara dos Deputados. Projeto de Lei PL nº 4.365 de 1977, de autoria do Deputado Faria Lima. Cria o Registro Nacional de Banco de Dados e estabelece normas de proteção da intimidade contra o uso indevido de dados arquivados em dispositivos eletrônicos de processamento de dados. Diário do Congresso Nacional, ano XXXII, n. 137, 08 de nov. de 1977.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 jun. 2021.

BRASIL. Lei nº 9.507, de 12 de novembro de 1977: Regula o direito de acesso a informação e disciplina o rito processual do habeas data. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm> Acesso em: 23 ago. 2021.

BRASIL. Lei nº 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Acesso em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em 14 de novembro de 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Congresso Nacional, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 de agosto de 2021.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 14 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. RE nº 1.010.606-RJ. Recorrente: Nelson Cury e Outros. Recorrido: Globo Comunicação e Participações S/A. Relator: Ministro Dias Toffoli. Rio de Janeiro, 11 de fevereiro de 2021.

CNIL: Commission Nationale Informatique & Libertés. Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. 2018. Disponível em:

<https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Acesso em: 25 de out. 2021.
DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais.** Em: DONEDA, Danilo; SCARLET, Ingo Wolfgang, MENDES, Laura Schertel, JUNIOR, Otavio Luiz Rodrigues (Coords.). Tratado de proteção de dados pessoais – Parte I. Rio de Janeiro: Forense, 2021. E-book Kindle.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019.

E-ESTONIA. KSI Blockchain in Estonia. Disponível em: https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf. Acesso em 04 de set. de 2021.

EUROPEAN COMISSION, 'Questions and Answers – Data Protection Reform' (Press Release, 21 December 2015).

EUROPEAN DATA PROTECTION SUPERVISOS. Anual Repport, 2016.

FIGURELLI, Rogério. BLOCKCHAIN: Uma análise estratégica para humanos e robôs. Trajecta. Edição do Kindle, 2017.

FINCK, Michèle. Blockchain and Data Protection in the UE. Max Planck Institute for Innovation and Competition Research Paper nº 18-01, 2017, p. 14. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322.> Acesso em: 18 de out. de 2021.

FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 120 f. Relatório – Parlamento Europeu, Bruxelas, 2019. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 15 de set. de 2021.

LAGO, Lucas. Blockchain: confiança através de algoritmos. Boletim, vol. 2, n. 4. São Paulo: CEST/USP, 2017.

MALDONADO, Viviane. Capítulo III – Dos Direitos do Titular. In: MALDONADO, Viviane; BLUM, Renato (Coords.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: 2ª Ed. Thompson Reuters Brasil, 2020. E-book kindle.

MALDONADO, Viviane. Direito ao Esquecimento. Barureri, SP: Novo Século Editora, 2017.

MARTINS. Leonardo. Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais. Volume 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS. 2016.

MEWES, Luke. BLOCKCHAIN E EXCLUSÃO DE DADOS: A COMPATIBILIDADE ENTRE A TECNOLOGIA E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Monografia em Direito – Faculdade de Direito, Centro Universitário Curitiba. Curitiba, 2021.

MORGAN, Pamela. Using Blockchain Technology to Prove Existence of a Document. https://empoweredlaw.wordpress.com/2014/03/11/using-blockchain-technology-to-prove-existence-of-a-document/. Acesso em 04 de set. de 2021.

MOZLAVAC, Bruno. Consent by GDPR vs. Blockchain. Revista Acadêmica Escola Superior do Ministério Público do Ceará, Fortaleza, ano XII, n. 1, jan.-jun. de 2020, p. 159. Disponível em: http://www.mpce.mp.br/wp-content/uploads/2020/08/ARTIGO-149-166.pdf. Acesso em 30 de set. de 2021.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [s.l.: s.n.], 2008. Disponível em <https://bitcoin.org/bitcoin.pdf>. Acesso em 01 de out. de 2021.

PARENTONI, Leonardo. Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014) (pp.539-618) Tomo 1: Capítulo Chapter: O Direito ao Esquecimento (Right to Oblivion). Editora Quartier Latin do Brasil, São Paulo, 2016.

PARIZI, Reza M. et al. Integrating Privacy Enhancing Techniques into Blockchains Using Sidechains. In: IEEE CANADIAN CONFERENCE ON ELECTRICAL AND COMPUTER ENGINEERING (CCECE 2019), 32., 2019, Edmonton. Sessão Especial – 2 nd International Workshop on Blockchain-oriented Cyber Security, Nova Iorque: IEEE, 2019.

PRADO, Jean. O que é blockchain: indo além do bitcoin. 2018. Disponível em: <https://tecnoblog.net/227293/como-funcionablockchain-bitcoin/>. Acesso em: 13 de março de 2021.

SCHWABE, Jürgen; MARTINS, Leonardo. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Konrad-Adenauer-Stiftung, 2005. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf. Acesso em 25 de abril de 2021.

UNIÃO EUROPEIA. Regulamento (UE) 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). Jornal Oficial da União Europeia, n. L119/1, 04 de maio de 2016, p. 1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

UNIÃO EUROPEIA. Tribunal de Justiça Europeu. Grande Secção. Pedido de Decisão Prejudicial C-131/12. Google Spain SL e Google Inc. Agência Española de Protección de Datos (AEPD). Relator: M. Ilešič. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131. Acesso em 19 de abr. de 2021.

Who are the administrators of blockchains?. Great Wall of Numbers:
Business Opportunities and Challenges in Emerging Markets, 2017. Disponível em: <https://www.ofnumbers.com/2017/10/19/who-are-the-administrators-of-blockchains/>. Acesso em: 12 de março de 2021.