IV ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

JOSÉ RENATO GAZIERO CELLA

AIRES JOSE ROVER

FERNANDO GALINDO AYUDA

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Danielle Jacon Ayres Pinto; Fernando Galindo Ayuda; José Renato Gaziero Cella; – Florianópolis: CONPEDI, 2021.

Inclui bibliografia
ISBN: 978-65-5648-407-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, desenvolvimento, sustentabilidade e smart cities.

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança. IV Encontro Virtual do CONPEDI (1: 2021 : Florianópolis, Brasil).

CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
ePós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IV ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

No IV Encontro Virtual do CONPEDI, realizado de 09 a 13 de novembro de 2021, o grupo de trabalho "Direito, Governança e Novas Tecnologias I", que teve lugar na manhã de 09 de novembro de 2021, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos e um graduando. Foram apresentados 21 artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente na sala virtual.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em cinco blocos, quais sejam a) inteligência artificial; b) proteção de dados; c) mídias sociais; d) governança, sociedade e poder judiciário; e e) novas tecnologias e direitos humanos.

A inteligência artificial foi objeto do primeiro bloco de trabalhos, com as exposições e debates sobre os seguintes artigos: 1. Soft law e standard global: caminhos para regulação dos sistemas de inteligência artificial de Pollyanna Maria Da Silva, Matheus De Andrade Branco; 2. A utilização da inteligência artificial e dos algoritmos e seu potencial para a melhoria da sustentabilidade e licenciamento ambiental de Deilton Ribeiro Brasil; 3. A regulação da inteligência artificial e novos contornos para caracterização da responsabilidade civil de Hérica Cristina Paes Nascimento, Maique Barbosa De Souza e Patrícia Da Silveira Oliveira; 4. Organização da informação e do conhecimento jurídico com vieses digitais e eletrônicos de José Carlos Francisco dos Santos; 5. Legal technology: os desafios para aplicação de decisões automatizadas de Anabela Cristina Hirata e Zulmar Antonio Fachin.

A proteção de dados foi o pano de fundo do segundo bloco de artigos apresentados, em que os problemas decorrentes de suas dinâmicas foram apresentados e debatidos a partir dos seguintes trabalhos: 1. Nossos dados, as big techs e o direito de Marcos Alexandre Biondi e José Carlos Francisco dos Santos; 3. Justiça eleitoral e proteção de dados. Reflexões

preliminares sobre suas competências e a lgpd de Eduardo Botão Pelella; 4. Blockchain, proteção de dados e autodeterminação informativa: um estudo na perspectiva da lgpd de Anderson Souza da Silva Lanzillo, Luana Andrade de Lemos e Lukas Darien Dias Feitosa.

As discussões acerca da utilização das mídias sociais congregaram as apresentações dos seguintes trabalhos: 1. O efeito manada decorrente das redes sociais como transformador do estado democrático de direito de Isadora Kauana Lazaretti e Alan Felipe Provin; 2. Pós-verdade; fake news; redes sociais e desinformação: o mau uso das tics e a ofensa aos direitos da personalidade de Dirceu Pereira Siqueira e Mayume Caires Moreira; 3. Internet: entre emancipação e alienação na esfera pública democrática de Natalia Maria Ventura da Silva Alfaya e Marcella da Costa Moreira de Paiva; 4. A proteção normativa da infância e adolescência no Brasil: da promessa constitucional à exposição de corpos adolescentes no instagram de Rosane Leal Da Silva e Ana Carolina Sassi; 5. A inserção digital de qualidade como direito fundamental na era de hiperconectividade? O direito a acessar direitos de Paulo de Tarso Brandão e Gabrielle Amado Boumann.

Os temas de governança, sociedade e poder judiciário foram objeto de discussão dos seguintes artigos: 1. O impacto das tecnologias disruptivas no mercado de trabalho e o dever do estado de Sabrinna Araújo Almeida Lima e Andre Studart Leitão; 2. A preferência pela utilização de atos sob a forma eletrônica e o incentivo às inovações tecnológicas na nova lei de licitações e contratos administrativos de João Walter Cotrim Machado e Augusto Martinez Perez Filho; 3. Os registros públicos na era da tecnologia blockchain de Iuri Ferreira Bittencourt, Fabio Fernandes Neves Benfatti e Fabiano Nakamoto.

Por fim, o quinto bloco trouxe para a mesa o debate sobre as novas tecnologias e os direitos humanos, com os seguintes artigos: 1. Relações espaciais feministas, negras, queer, trans e periféricas nas cidades “inteligentes” de Stéphani Fleck da Rosa; 2. O transumanismo e o pós-humanismo: uma visão dos direitos humanos à luz da evolução tecnológica e da sustentabilidade de Ricardo Fabel Braga e Luciana Machado Teixeira Fabel; 3. As novas tecnologias e uma necessária disrupção legislativa na lei do inquilinato de Thiago Leandro Moreno e Carlos Renato Cunha; 4. Dignidade humana dos refugiados ambientais e governança global: violação e transgressões da dignidade dos refugiados nas fronteiras do Acre de Ionara Fonseca Da Silva Andrade e Patrícia De Amorim Rêgo.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Direito, Governança e Novas

Tecnologias”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito brasileira, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. Aires José Rover

Prof.ª Dr.ª Danielle Jacon Ayres Pinto

Prof. Dr. Fernando Galindo

Prof. Dr. José Renato Gaziero Cella

BLOCKCHAIN, PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMATIVA: UM ESTUDO NA PERSPECTIVA DA LGPD

BLOCKCHAIN, DATA PROTECTION AND INFORMATIONAL SELF-DETERMINATION: A STUDY FROM THE PERSPECTIVE OF THE GENERAL PERSONAL DATA PROTECTION LAW

Anderson Souza da Silva Lanzillo [1]
Luana Andrade de Lemos [2]
Lukas Darien Dias Feitosa [3]

Resumo

As características elementares do Blockchain impõem desafios para a proteção de dados pessoais e a autodeterminação informativa. Diante disso, o presente artigo objetiva identificar quais são esses desafios em face das obrigações da LGPD, no que concerne principalmente à proteção de dados pessoais e ao direito do usuário à autodeterminação informativa. O método de abordagem foi o dedutivo, por meio de pesquisa teórico-descritiva de caráter qualitativa, consistindo em pesquisa bibliográfica e documental. Como conclusão, verificou-se que o Blockchain não é, em todas as suas variáveis, incompatível com a LGPD, mas requer uma adequação à referida regulação no seu desenvolvimento.

Palavras-chave: Blockchain, Proteção de dados, Dados pessoais, Autodeterminação informativa, Lgpd

Abstract/Resumen/Résumé

The elemental characteristics of the Blockchain imposes challenges for the protection of personal data and informational self-determination. This article aims to identify what are the challenges according to the LGPD's obligations, mainly concerning the protection of personal data and the user's right to informative self-determination. The approach method was deductive, through theoretical-descriptive qualitative research, and the technical procedures consisted of bibliographical and documentary research. It was concluded that the Blockchain is not, in all its variables, incompatible with the LGPD, but requires an adaptation to the referred regulation in its development.

Keywords/Palabras-claves/Mots-clés: Blockchain, Data protection, Personal data, Informational self-determination, Lgpd

[1] Professor Doutor do Departamento de Direito Privado da Universidade Federal do Rio Grande do Norte

[2] Mestranda em Direito pela Universidade Federal do Rio Grande do Norte

[3] Mestrando em Direito pela Universidade Federal do Rio Grande do Norte

1. INTRODUÇÃO

A tecnologia está modificando rapidamente e profundamente a maneira com que as pessoas se relacionam e, como consequência inevitável, o Direito também é atingido. Em uma sociedade cada vez mais globalizada e interconectada, e com o surgimento constante de inovações tecnológicas, surge para a seara jurídica o constante desafio de harmonizar as normas com os esses avanços.

Como ocorre comumente em contextos de desenvolvimento tecnológico, as inovações técnicas costumam impactar a sociedade numa velocidade que a legislação não consegue acompanhar. Se a legislação vigente não consegue trazer respostas satisfatórias para os problemas que uma nova tecnologia cria, novas soluções são demandadas, tanto na seara legislativa quanto judiciária.

A tecnologia *Blockchain* se trata de um desses avanços. Em 2008, através do pseudônimo de Satoshi Nakamoto, foi publicado o artigo que deu início a criação da criptomoeda *bitcoin*, a qual tinha como protocolo base o *Blockchain*. Desde então, diversos questionamentos jurídicos envolvem o assunto, principalmente no que concerne a sua regulação.

Se por um lado esse recurso vem se mostrando verdadeiramente revolucionário, principalmente no que concerne à garantia da confiabilidade das informações armazenadas, capacidade de rastreio de qualquer tipo de processamento realizado e possibilidades de compartilhamento de forma segura, o uso dos Blockchains ainda necessita de adequações que respondam às demandas legislativas internacionais, possibilidades de controle externo e proteção de dados pessoais.

Em outro ponto, ainda no contexto do desenvolvimento tecnológico, os dados sensíveis dos usuários conectados no ambiente digital estão constantemente sendo coletados e examinados por organizações públicas ou privadas em prol de processos de personalização de serviços, otimização de vendas ou manipulação de resultados.

Diante do quadro exposto, com o advento da Lei Geral de Proteção de Dados (LGPD) e do reconhecimento pelo Supremo Tribunal Federal (STF) da proteção de dados pessoais como direito fundamental, insere-se na esfera normativa a incerteza quanto à compatibilidade do *Blockchain* com o direito à proteção de dados e à autodeterminação informativa na perspectiva da LGPD.

Desse modo, o presente artigo tem como objetivo principal identificar os problemas e desafios do uso da tecnologia *Blockchain* em face das obrigações impostas pela Lei Geral de

Proteção de Dados, principalmente no que concerne à proteção de dados pessoais e ao direito do usuário à autodeterminação informativa.

O método de abordagem utilizado para o desenvolvimento da pesquisa foi o dedutivo, por meio de pesquisa teórico-descritiva de caráter qualitativa, uma vez que parte da pesquisa atual sobre dados pessoais e *Blockchain* para a formulação de seus resultados. Os procedimentos técnicos usados foram pesquisa bibliográfica e documental.

Por fim, quanto a sua estrutura, o presente artigo aborda no primeiro tópico a proteção dos dados pessoais e sua tutela jurídica no âmbito dos direitos fundamentais e da LGPD, continua no segundo tópico com a explicação do surgimento da tecnologia *Blockchain* e seus impactos na gestão da informação, e se aprofunda no terceiro tópico nos problemas/desafios do uso da tecnologia *Blockchain* em face da tutela dos dados pessoais, com as considerações finais no quarto e último tópico.

2. OS DADOS PESSOAIS E OS MARCOS JURÍDICOS DE SUA TUTELA JURÍDICA NO BRASIL

No atual estado das capacidades computacionais, onde a convivência diária com sistemas de informações é cada vez maior, seja no âmbito profissional, seja mesmo para demandas pessoais, o volume de informações de cunho pessoal que diariamente são disponibilizadas é imenso, dados esses que, de acordo com o tratamento realizado, podem ser utilizados para identificar, parametrizar e, até mesmo, condicionar padrões de comportamento, consumo ou mesmo sócio-políticos.

Nesse contexto, legislações de proteção de dados pessoais foram pensadas de forma a proteger diversos direitos fundamentais individuais. Ainda que, numa análise inicial, essas legislações tenham como foco principal a proteção da integridade pessoal e da privacidade propriamente dita - como a LGPD, que tem como objetivo, segundo o texto da lei, a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[1] - inegavelmente o espectro de cobertura do direito à proteção dos dados pessoais se amplia sobre os mais diversos aspectos sociais (OOSTVEEN; IRION, 2018).

[1] Lei Federal 13.709/2018, Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Esse direito, portanto, vai além da proteção individual contra a invasão de terceiros à sua esfera privada, mas também tem como propósito possibilitar ao titular dos dados o controle sobre o acesso e a utilização das suas informações pessoais.

A sociedade contemporânea, cada vez mais baseada em acumulação e circulação de informações, impõe o reconhecimento dos dados como recurso essencial para o funcionamento da sociedade e, por conseguinte, a necessidade do estado e do setor produtivo de se adequar a essa nova realidade, onde a noção de privacidade evolui do mero sigilo à possibilidade do titular ter controle dos seus dados pessoais (RODOTÀ, 2008).

Diante desse contexto, desde meados do século XX surgiram leis e normas, como a legislação francesa[2], alemã[3] e, finalmente, a Regulamento Geral sobre a Proteção de Dados[4] (GDPR, em sua sigla em inglês), com o intuito de estabelecer uma rede de proteção aos dados pessoais que buscam garantir, essencialmente, que o titular dos dados possua controle não só sobre a disponibilização dessas informações, mas sobre os usos após tal disponibilização.

O desenvolvimento do arcabouço legislativo de proteção dos dados pessoais tem como principal característica a mudança do enfoque das leis, inicialmente mais técnicas e de linguajar pouco acessível até, mais recentemente, com um olhar mais amplo, voltado à tutela dos direitos fundamentais e condizente com a própria evolução tecnológica do tratamento de dados (DONEDA, 2011).

A LGPD define dados pessoais como aquelas informações relacionadas a pessoas naturais identificadas ou identificáveis e estabelece, ainda, como dado pessoal sensível, informações que tratem, em referência a uma pessoa natural, sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico[5] (BRASIL, 2018).

---

[2] Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada Informatique et Libertées - Lei 78-17 de 6 de janeiro de 1978

[3] Bundesdatenschutzgesetz, Lei Federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977

[4] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: https://gdpr-info.eu

[5] Art. 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Dados pessoais, portanto, são informações que, de forma isolada ou combinada a outras informações, possuem a capacidade de identificar o seu titular, isto é, aquele a quem se refere aquelas informações. Esses dados, quando reunidos em uma determinada base de dados, compõem o perfil de uma pessoa, a sua própria identidade (KLEE; NETO, 2019).

Adequar o direito de acordo com a atual evolução tecnológica, principalmente numa época onde os dados e informações - pessoais ou não - tem se mostrado uma necessidade cada vez mais relevante, social e economicamente, para o próprio exercício de nossas liberdades. O direito à proteção dos dados pessoais se apresenta como elemento chave nesse contexto, tendo o ordenamento jurídico papel fundamental na configuração de um contexto legal que estabeleça um ambiente que possibilite ao cidadão o controle sobre suas informações (DONEDA, 2020).

Apesar da assunção de que o acesso não autorizado às informações pessoais é ilegítimo, para, além disso, é imperativa a consolidação do entendimento de que o acesso, ainda que legítimo, aos dados pessoais não autoriza a quem controla ou processa os dados o uso indiscriminado dessas informações. A legislação de proteção de dados pessoais, ao estabelecer que todo tratamento dessas informações deve ter especificada uma finalidade, além de dar fundamento para a própria organização dos sistemas de coleta e processamento de dados pessoais, obriga o controlador a respeitar estas finalidades inicialmente propostas (BIONI, 2021).

A proteção de dados pessoais deve ser analisada sob uma perspectiva subjetiva, onde a proteção do indivíduo contra ameaças a sua personalidade quando da coleta, processamento, utilização e circulação de dados pessoais e, sob uma perspectiva objetiva, garantindo a capacidade do indivíduo de controlar fluxo de seus dados (MENDES, 2014).

Os debates sobre proteção de dados pessoais colocam, portanto, o direito à autodeterminação informativa em destaque, direito esse que possui origens históricas ligadas diretamente à proteção da personalidade como direito fundamental. Restringir a capacidade do indivíduo de controlar o uso de suas informações é um atentado direto à sua autonomia individual e, no fim das contas, um ataque contra à sua própria liberdade (MENDES, 2020; DE ARAGÃO, 2020).

A Constituição Federal estabelece a proteção à privacidade individual, proteção essa consolidada pelo direito civil, em especial no microssistema legal que se debruça sobre o tema da privacidade de dados, como o Código de Direito do Consumidor[6], a Lei de Acesso à

[6] Lei nº 8.078, de 11 de setembro de 1990.

Informação[7], o Marco Civil da Internet[8], a Lei do Governo Digital[9] e a atual Lei Geral de Proteção de Dados Pessoais (LGPD)[10].

Especificamente, a LGPD se fundamenta na ideia central de que as pessoas tenham conhecimento e controle sobre a coleta e o processamento de seus dados pessoais, principalmente daqueles ditos sensíveis, possibilitando uma limitação desse processo de acordo com o respeito à privacidade e a intimidade do titular dos dados, à liberdade de expressão, de informação, de comunicação e de opinião, com foco no desenvolvimento econômico e tecnológico sem perder de vistas o respeito aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania da pessoa humana[11] (BRASIL, 2018).

A proteção dos dados pessoais se justifica, portanto, na defesa dos direitos fundamentais individuais, em especial o direito à privacidade e, mais recentemente, no próprio direito à proteção de dados pessoais, que interfere, direta ou indiretamente, em outras liberdades e direitos fundamentais como a liberdade de pensamento, de crenças, de livre associação e o direito a não-discriminação (OOSTVEEN; IRION, 2018).

Essa proteção se consolida, no texto legal, a partir de instrumentos como a anonimização dos dados durante o processamento e compartilhamento das informações, de acordo com as peculiaridades de cada dado e as respectivas autorizações - legais e individuais; a exigência do consentimento livre e esclarecido do uso dos dados, garantindo o direito à retificação e até mesmo o apagamento dos dados, de acordo com as previsões legais; o respeito à finalidade proposta ao tratamento do dado, sempre de forma suficiente e adequada ao contexto do processamento; bem como a adoção de condutas transparentes, seguras e responsáveis, com a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas[12] (BRASIL, 2018).

---

[7] Lei nº 12.527, de 18 de novembro de 2011.
[8] Lei nº 12.965, de 23 de abril de 2014.
[9] Lei nº 14.129, de 29 de março de 2021.
[10] Lei nº 13.709, de 14 de agosto de 2018.
[11] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
[12] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

No Brasil, o Supremo Tribunal Federal[13] atualmente entende que o tratamento e a manipulação de dados pessoais devem receber as mesmas proteções garantidas pela Constituição Federal no que se refere aos direitos e garantias fundamentais (art. 5º, caput), ainda que não haja previsão expressa no referido artigo. O estabelecimento do direito fundamental à proteção de dados pessoais, para o STF, surge diretamente da necessidade de proteção à dignidade da pessoa humana num contexto de contínua exposição das pessoas aos riscos de comprometimento da sua autodeterminação informacional nas relações sociais e econômicas atuais.

Ainda nesse contexto, tramita hoje no senado federal a PEC 17/2019 que, entre outros temas, propõe a inclusão da proteção de dados pessoais entre os direitos e garantias fundamentais expressamente previstos na Constituição Federal.

O que se depreende, portanto, é o consenso de que o processamento e tratamento de dados pessoais deve ter como finalidade precípua o benefício das pessoas, em especial o titular dos dados. O direito à proteção dos dados pessoais, portanto, apesar de não ser absoluto, deve ser sempre considerado de acordo com a função social do uso dos dados, em equilíbrio com os demais direitos fundamentais e em obediência aos princípios estabelecidos pela normativa em vigor.

3. A TECNOLOGIA BLOCKCHAIN E OS IMPACTOS NO MUNDO JURÍDICO

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

[13] STF - ADI: 6387 DF 0090566-08.2020.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 07/05/2020, Tribunal Pleno, Data de Publicação: 12/11/2020.

A tecnologia *Blockchain* se trata de um desses avanços tecnológicos disruptivos que suscita o estranhamento. Em 2008, através do pseudônimo de Satoshi Nakamoto, foi publicado o artigo que deu início a criação da criptomoeda *bitcoin*, a qual tinha como protocolo base o *Blockchain*. Desde então, diversos questionamentos jurídicos envolvem o assunto, principalmente no que concerne à sua regulação, mas também no que diz respeito ao potencial do seu uso.

No artigo publicado, intitulado "*Bitcoin: a peer-to-peer eletronic cash system"*, ou, em tradução livre, "Bitcoin: um sistema ponto-a-ponto de dinheiro eletrônico", Satoshi Nakamoto propôs um modelo de criptomoeda, com o fim de reproduzir as características da moeda física no ambiente virtual, o alicerce para tanto seria a tecnologia que ele denominou por *Blockchain.*

No referido artigo, a forma mais simples do *Blockchain* foi descrita como um banco de dados descentralizado, de ponto a ponto, que, de forma autônoma, mantém uma cadeia de blocos, nos quais são armazenados dados criptografados, protegidos de eventuais adulterações (NAKAMOTO, 2008).

Cada bloco da cadeia é uma unidade de registro de informações e, para ser validado, se conecta com um bloco anterior, em ordem cronológica, de maneira que se forma uma cadeia de registros em sequência, que não pode ser copiada, alterada ou quebrada e fica armazenada na internet.

A proposta foi inaugurada para eliminar a necessidade de um terceiro confiável intermediando as transações, visto que os próprios usuários participantes desempenham a função de validar qualquer informação adicionada. Nessa lógica, a segurança da transação é baseada na prova criptografada não reversível, e não na confiança depositada em um agente mediador, o que evita fraudes e diminui os custos das transações (NAKAMOTO, 2008).

Dentre suas principais características positivas, a tecnologia *Blockchain* garante: mais celeridade nas transações; segurança contra as perdas ou adulterações das informações; integridade dos dados; transparência nas operações; rastreabilidade dos acréscimos ou alterações; descentralização do controle; e economia no funcionamento (PORTO *et al.*, 2019).

As criptomoedas são as aplicações mais conhecidos do protocolo, contudo, elas foram pensadas para reproduzir as características da moeda física, de maneira que os envolvidos não precisariam confiar uns nos outros. Atualmente, sistemas de *Blockchain* podem ser configurados de diversas maneiras para criar aplicativos com diferentes propriedades, dessa forma, a participação pode ser limitada, a plataforma pode ser mais ou menos descentralizada e mais ou menos anônima (BACON, 2017).

Após o desenvolvimento na sua utilização, fala-se geralmente na existência de quatro tipos de *Blockchain*, sendo eles (BRASIL, 2020): (1) pública não permissionada, em que todos podem participar do mecanismo de consenso; (2) pública permissionada, na qual apenas uma parte restrita pode participar do mecanismo; (3) privada permissionada, em que o dono é quem define os usuários e quais nós podem participar do mecanismo; e (4) privada não permissionada, em que o mecanismo é aberto a qualquer nó, mas existe restrição quanto à realização de transações e visualização.

Diante da proposta disruptiva, para além do seu uso no setor financeiro, verificou-se um crescente interesse no potencial do uso do *Blockchain* para as relações jurídicas, como: a concepção de contratos inteligentes; a criação de cartórios automatizados; o registro de imóveis em sistema eletrônico de *Blockchain;* o desenvolvimento de novos sistemas de governança; a utilização do *Blockchain* em processos licitatórios; entre outros.

Mais especificamente, em nível governamental, para a construção de um Governo Digital, o *Blockchain* pode ser usado para auxiliar no desenvolvimento de politicas públicas e no monitoramento e controle de certas tarefas públicas, a exemplo da emissão de passaportes, entrega de benefícios, arrecadação de impostos, elaboração de sistemas de votação e outros (CORRALES; FENWICK; HAAPIO, 2013).

No Brasil, a Lei do Governo Digital[14] dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência da administração pública, primando especialmente pela desburocratização, inovação, transformação digital e participação do cidadão[15] (BRASIL, 2021). Objetivos esses que podem ser alcançados ou acelerados com o uso do *Blockchain.*

Nesse sentido, a Estratégia de Governo Digital[16] para o período de 2020 a 2022 estabelece expressamente como iniciativas para o uso de tecnologias emergentes nos serviços públicos do futuro a disponibilização de, pelo menos, nove conjuntos de dados por meio de soluções de *Blockchain* na administração pública federal, até 2022, e a implementação de recursos para a criação de uma rede *Blockchain* do Governo federal interoperável, com uso de identificação confiável e de algoritmos seguros[17] (BRASIL, 2020).

---

[14] Lei Federal nº 14.129, de 29 de março de 2021.

[15] Art. 1º Esta Lei dispõe sobre princípios, regras e instrumentos para o aumento da eficiência da administração pública, especialmente por meio da desburocratização, da inovação, da transformação digital e da participação do cidadão.

[16] Decreto nº 10.332, de 28 de abril de 2020.

[17] Iniciativa 8.3. Disponibilizar, pelo menos, nove conjuntos de dados por meio de soluções de **blockchain** na administração pública federal, até 2022.
Iniciativa 8.4. Implementar recursos para criação de uma rede **blockchain** do Governo federal interoperável, com uso de identificação confiável e de algoritmos seguros.

Pelo exposto, depreende-se que o *Blockchain* se trata de uma inovação diretamente relacionada à organização social, em moldes que se coadunam com o avanço tecnológico e o desenvolvimento de uma sociedade mais colaborativa, configurando-se em um verdadeiro mecanismo de consenso.

4. O USO DA TECNOLOGIA BLOCKCHAIN E SUA CONFORMIDADE AOS DEVERES IMPOSTOS PELA LGPD

As características tecnológicas elementares do *Blockchain* impõem desafios importantes no que se refere à proteção de dados pessoais, tanto na perspectiva do uso no setor privado quanto como estratégia tecnológica para o setor público.

Especificamente no que se refere à proteção de dados pessoais, o processamento desses dados utilizando-se tecnologia *Blockchain* deverá ter sua compatibilidade com a legislação analisada caso a caso, de acordo com as especificidades técnicas e a organizacional do modelo de *Blockchain* utilizado. Apesar disso, é fato que alguns elementos específicos merecem uma atenção específica sobre sua relação com a legislação (KUNER et al, 2018; FINCK, 2019).

Como já mencionado, *Blockchain* é uma tecnologia capaz de construir uma base de dados aberta e distribuída, cujos dados se encontram numa estrutura conectada, onde cada nó possui todas as informações, inclusive aquelas referentes a atualizações, conexões com blocos anteriores e acessos a essas informações (ESPOSITO, 2018).

No artigo onde Nakamoto (2008) apresenta sua proposta tecnológica, ele explica que cada nova alteração ou novo dado incluído na cadeia do *Blockchain* tem um registro de data e hora, além da manutenção dos dados anteriores com os respectivos registros de data e hora de inclusão na cadeia.

Desse modo, ainda que haja a correção/retirada de um determinado dado, essa informação ainda é acessível, o que conduz ao primeiro, e talvez mais importante, desafio a ser superado que é a necessidade de precauções específicas de proteção de dados sigilosos ou legalmente protegidos, como os dados pessoais, antes de sua inclusão no *Blockchain.*

Essa preocupação ganha especial importância quando do uso dessa tecnologia para o armazenamento e compartilhamento de informações que são, quase que em sua totalidade, protegidas por lei, como os dados clínicos e de saúde de um indivíduo, por exemplo.

Esposito (2018), ao analisar a utilização do *Blockchain* no armazenamento e compartilhamento de dados de saúde e, apesar dos benefícios quanto à garantia da integridade dos dados e a possibilidade de compartilhamento dessas informações em escala global, deixa clara a necessidade de proteção dos dados pessoais e de saúde antes de sua inclusão no bloco.

Põe-se, como segundo desafio, a necessidade desses sistemas de armazenamentos de dados pessoais com o uso de tecnologia *Blockchain* a adoção de estratégias de anonimização e criptografias, que já vêm sendo utilizadas nas criptomoedas.

Além dos obstáculos já discutidos, a determinação da LGPD de que os controladores dos dados pessoais devem possibilitar a revisão ou mesmo o apagamento das informações de acordo com o requerimento dos titulares dos dados é outro problema a ser superado. E este é um desafio bastante significativo principalmente por que no *Blockchain*, esse tipo de modificação dos dados é, propositalmente, muito onerosa, como elemento essencial da estratégia de garantia da integridade dos dados e aumento da confiança no sistema (FINCK, 2019).

Qualquer sistema que trabalhe com armazenamento de dados sensíveis, como àqueles da saúde deverão, portanto, buscar uma solução técnica que consiga respeitar essas determinações legais, possibilitando a revisão ou o apagamento dos dados em caso de requerimento do titular dos dados (ESPOSITO, 2018).

Por fim, um outro problema que um sistema de *Blockchain* deverá se debruçar quando estiver lidando com o armazenamento de dados pessoais são as estratégias para evitar que quebras de seguranças surjam por meio dos proprietários de cada nó.

Apesar da tecnologia ser bastante robusta no que diz respeito às questões de segurança, os proprietários dos nós podem se mostrar um ponto fraco do sistema, já que um erro desses atores pode comprometer, em teoria, toda a cadeia (FABIANO, 2017).

A LGPD prevê, em semelhança da lei de proteção de dados pessoais europeia, a figura do controlador, pessoa física ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais. Dessa forma, segundo a legislação, todo dado pessoal coletado deve possuir pelo menos um responsável por sua coleta, armazenamento, processamento e, eventualmente, descarte.

Na lógica do *Blockchain*, contudo, essa realidade pode ser posta à prova, haja vista ser base da tecnologia a descentralização das informações. Isso faz com que a distribuição de responsabilidades se torne complexa e onerosa, especialmente à luz dos contornos incertos que a noção de controle sob a luz da LGPD se apresenta no contexto dos *Blockchains* (FINCK, 2019).

Os agentes, públicos e privados, que possuem a pretensão de utilizar essa tecnologia para armazenamento e processamento de dados pessoais, necessitarão criar um sistema com estabelecimento claro de responsabilidades entre os participantes da cadeia, bem como o agente regulador necessitará se debruçar sobre o esclarecimento dessa situação.

Além dessas da necessidade do correlacionamento dos aspectos técnicos com as obrigações vigentes nas leis de proteção de dados pessoais, dada a características dos sistemas de *Blockchain* em garantir a perspectiva de compartilhamento dos dados a nível internacional, os agentes organizadores dos sistemas de *Blockchain* deverão se preocupar com a adequação de suas regras às determinações que cada país adota, haja vista a característica básica da tecnologia em distribuir o armazenamento dos dados por toda a cadeia de participantes.

5. CONSIDERAÇÕES FINAIS

Em face das obrigações impostas pela Lei Geral de Proteção de Dados, o uso da tecnologia *Blockchain* se apresenta como um desafio para os agentes públicos e privados, mas não como uma impossibilidade.

Apesar de em um primeiro momento o sistema, por suas características inerentes, parecer ser incompatível com a regulação destinada à proteção dos dados pessoais, observa-se que o modelo organizacional do *Blockchain* pode ser construído de maneira a atender a legislação.

A natureza aberta, pouco burocrática e potencialmente anônima de sistemas de *Blockchain,* como as utilizadas por algumas criptomoedas, se mostra de certa forma problemática sob a perspectiva legal e regulatória.

Questões como a segurança dos dados espalhados por toda a cadeia do *Blockchain,* a garantia de anonimato, a equiparação dos usuários a controladores e a dificuldade para a realização de alterações ou mesmo apagamentos de dados pessoais são alguns dos desafios a serem enfrentados, conforme exposto.

A forma como o protocolo foi sugerido aparentemente dificulta sobremaneira o exercício do direito à autodeterminação informativa, a identificação e a responsabilização do controlador e a garantia da segurança dos dados pessoais.

Nada obstante, o *Blockchain* proposto em 2008 inaugurou o uso da tecnologia, mas não limitou os desdobramentos, sendo possível no contexto atual que o sistema seja desenvolvido com a figura clara de um controlador, assim como com a definição das responsabilidades de cada nó e a segurança dos dados sensíveis.

Por exemplo, no tipo de *Blockchain* privado não permissionado o mecanismo de consenso é aberto para qualquer nó, mas há restrições tanto na realização de transações como na visualização da cadeia. Dessa forma, a segurança dos dados é mantida e a figura do controlador é definida.

Nesse quadro de possibilidades, o maior desafio do uso da tecnologia *Blockchain* parece rondar principalmente as nuances do exercício do direito à autodeterminação informativa, visto que uma vez inseridos na cadeia o registro se torna imutável. Essa característica garante a integridade dos dados, a rastreabilidade dos acréscimos e a segurança contra perdas das informações, contudo não atende, *prima facie*, ao direito do titular de requerer a eliminação do dado.

Para tanto, no caso da construção de um sistema *Blockchain* apto para armazenar dados sensíveis, o agente controlador precisará garantir que os dados não sejam incluídos explicitamente na cadeia ou, caso sejam, que possam ser eliminados a qualquer tempo sem que a informação permaneça registrada.

Isso poderia ser pensado, presume-se, em um tipo de *Blockchain* permissionado com dados privados, no qual, não sendo necessário dar transparência pública aos conteúdos das transações, a cadeia registraria tão somente a movimentação, ou os próprios dados, mas criptografados, em que apenas o titular do dado e o controlador teriam a chave para acessar o conteúdo.

A materialização técnica do protocolo que consiga atender o direito fundamental à proteção de dados pessoais e o direito à autodeterminação informativa é o grande desafio verificado, para os agentes públicos e privados, em prol de interesses individuais ou coletivos, que desejem utilizar a tecnologia.

Pelo exposto, depreende-se que o uso da tecnologia *Blockchain* não é, em todas as suas variáveis, incompatível com a proteção de dados pessoais e a autodeterminação informativa na perspectiva da Lei Geral de Proteção de Dados, apenas requer uma adequação à referida regulação desde o seu desenvolvimento, com o estabelecimento claro da responsabilidade dos participantes da cadeia.

REFERÊNCIAS

BACON, Jean et al. **Blockchain demystified**. Queen Mary School of Law Legal Studies Research Paper, n. 268, 2017.

BIONI, Bruno. Regulação de dados é uma janela de oportunidade. In: **Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes**. Org. Bruno Ricardo Bioni – São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021. Disponível em: https://observatoriolgpd.com/wp-content/uploads/2021/08/1629122407livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf#page=14. Acesso em: 19 de setembro de 2021.

BRASIL. **Estratégia de Governo Digital.** Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.332-de-28-de-abril-de-2020-254430358. Acesso em: 20 set. 2021.

BRASIL. **Lei de Acesso à Informação.** 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: 15 set. 2021.

BRASIL. **Lei do Governo Digital.** Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm. Acesso em: 20 set. 2021.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 set. 2021.

BRASIL. **Marco Civil da Internet.** Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 set. 2021.

BRASIL. MINISTÉRIO DA ECONOMIA. **Blockchain**: tecnologias emergentes, blockchain. Tecnologias emergentes, Blockchain. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/blockchain. Acesso em: 15 set. 2021.

CORRALES, Marcelo; FENWICK, Mark; HAAPIO, Helena. Digital technologies, legal design and the future of the legal profession. In: **Legal Tech, Smart Contracts and**

Blockchain. Springer, Singapore, 2019. p. 1-15. Disponível em: https://doi.org/10.1007/978-981-13-6086-2_1. Acesso em: 16 set. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo. Registro da sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art 2º, caput e §§ 1º e 3º da MP 954/2020. **civilistica.com**, v. 9, n. 1, p. 1-9, 2020.

ESPOSITO, Christian et al. Blockchain: A panacea for healthcare cloud-based data security and privacy?. **IEEE Cloud Computing**, v. 5, n. 1, p. 31-37, 2018.

FABIANO, Nicola. The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard. In: 2017 **International Conference on Internet of Things for the Global Community (IoTGC)**. IEEE, 2017. p. 1-7.

FINCK, Michèle. Blockchain and the general data protection regulation. can distributed ledgers be squared with european data protection law? **Study. European Parliament**, 2019.

JABUR, Gilberto Haddad. A dignidade e o rompimento de privacidade. MARTINS, Ives Gandra da Silva; MONTEIRO JUNIOR, Antonio Jorge, (coordenadores). **Direito à privacidade.** Aparecida, SP: Idéias & Letras, p. 85-106, 2005.

KLEE, Antonia Espíndola Longoni; NETO, Alexandre Nogueira Pereira. A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. **Cadernos Adenauer [Internet]**, v. 3, p. 11-33, 2019.

KUNER, Christopher et al. Blockchain versus data protection. I**nternational Data Privacy Law**, Vol. 8, No. 2, 2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 140., p. 176-177

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Pensar-Revista de Ciências Jurídicas, v. 25, n. 4, 2020.

NAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer eletronic cash system. Bitcoin, [s. l.], p. 1-9, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 15 set. 2021.

NUNES, Caroline Castro; MA, Stephane; TEIXEIRA FILHO, Marcelo Silveira. Armazenamento descentralizado no Sistema Único de Saúde brasileiro (SUS) usando Interplanetary File System (IPFS) e Blockchain. **Revista de Direito**, v. 13, n. 01, p. 01-25, 2021.

OOSTVEEN, Manon; IRION, Kristina. The golden age of personal data: How to regulate an enabling fundamental right?. In: **Personal Data in Competition, Consumer Protection and Intellectual Property Law**. Springer, Berlin, Heidelberg, 2018. p. 7-26.

PORTO, Antônio Maristrello; LIMA JUNIOR, João Manoel de; SILVA, Gabriela Borges. **Tecnologia Blockchain e Direito Societário**: aplicações práticas e desafios para a regulação. Revista de Informação Legislativa: RIL, Brasília, DF, v. 56, n. 223, p. 11-30, jul./set. 2019. Disponível em: http://www12.senado.leg.br/ril/edicoes/56/223/ril_v56_n223_p11. Acesso em: 15 set. 2021.

RODOTÀ, Stefano. Tecnologias e Direito In: **A vida na sociedade da vigilância: a privacidade hoje**. 2008. p. 23-41.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. 297 f. Dissertação (Mestrado em Direito)-Universidade de Brasília, Brasília, 2007.