UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS – CCJ
COORDENAÇÃO DO CURSO DE DIREITO – CAMPUS JOÃO PESSOA
COORDENAÇÃO DE MONOGRAFIA

Caio Martins Lemos de Souza

BLOCKCHAIN E DIREITO À PRIVACIDADE: ANÁLISE DA LEGALIDADE DO ARMAZENAMENTO DE DADOS EM SISTEMAS CRIPTOGRÁFICOS DISTRIBUÍDOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

JOÃO PESSOA
2021

CAIO MARTINS LEMOS DE SOUZA

BLOCKCHAIN E DIREITO À PRIVACIDADE: ANÁLISE DA LEGALIDADE DO ARMAZENAMENTO DE DADOS EM SISTEMAS CRIPTOGRÁFICOS DISTRIBUÍDOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito à obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. Gustavo Rabay Guerra

JOÃO PESSOA
2021

Catalogação na publicação
Seção de Catalogação e Classificação

S729b Souza, Caio Martins Lemos de.
Blockchain e direito à privacidade: análise da legalidade do armazenamento de dados em sistemas criptográficos distribuídos à luz da lei geral de proteção de dados / Caio Martins Lemos de Souza. - João Pessoa, 2021.
36 f.

Orientação: Gustavo Rabay Guerra.
Monografia (Graduação) - UFPB/CCJ.

1. Blockchain. 2. LGPD. 3. Tratamento de dados. I. Guerra, Gustavo Rabay. II. Título.

UFPB/CCJ CDU 34

Elaborado por LUCIMARIO DIAS DOS SANTOS - CRB-645/15

CAIO MARTINS LEMOS DE SOUZA

BLOCKCHAIN E DIREITO À PRIVACIDADE: ANÁLISE DA LEGALIDADE DO ARMAZENAMENTO DE DADOS EM SISTEMAS CRIPTOGRÁFICOS DISTRIBUÍDOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

Projeto de Pesquisa apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito para matrícula na disciplina Trabalho de Conclusão de Curso.

Orientador: Prof. Dr. Gustavo Rabay Guerra

DATA DA APROVAÇÃO: 16 DE JULHO DE 2021

BANCA EXAMINADORA:

Prof. Dr. GUSTAVO RABAY GUERRA
(ORIENTADOR)

Prof. Dr. ALFREDO RANGEL RIBEIRO
(AVALIADOR)

Prof. Dr. ANDRÉ LUIZ CAVALCANTI CABRAL
(AVALIADOR)

RESUMO

A tutela da legislação sempre sofreu dificuldades para acompanhar as intensas mudanças que ocorrem com as subsequentes revoluções industriais. No mundo contemporâneo, o período de digitalização intensa atual culminou em sequenciadas e gravíssimas violações ao direito de privacidade dos cidadãos brasileiros. Tal fato, unido com interesses financeiros referentes às demandas da União Europeia, culmina na criação da Lei Geral de Proteção de Dados no Brasil. Todavia, esse processo de tutela de direitos é legislado por uma Lei Geral, que necessitará da doutrina e da jurisdição para se adequar a um meio que sofre intensas mudanças de forma recorrente, como exemplo o do desenvolvimento de Software. Junto a esse crescente interesse em resguardar os direitos dos dados pessoais dos cidadãos, a computação vive uma crescente ênfase na área de segurança de dados. Dentre as várias ferramentas nesse subgênero da computação, é o da *Blockchain* que armazena dados de forma na qual eles não possam ser adulterados ou deletados após inserção no livro de registros distribuído da ferramenta. Todavia, isso gera flagrante ilegalidade quando se depara com o art. 18 da LGPD, que prevê que certas modalidades de dados devem ser eliminadas quando do requerimento do titular dos dados.

Palavras-chave: Blockchain. LGPD. Tratamento de Dados.

ABSTRACT

The tutelage of legislation has always struggled to catch up with the intense changes that occur daily with the everchanging industrial revolution. Nowadays, the intense digitalization period culminates in recurrent violations to the citizen´s right to privacy, which in conjunction with financial interests motivated by demands from the European Union, culminates in the creation of the Brazilian "General Data Protection Regulation" (LGPD). However, the process of assuring these rights is contemplated in a generalized law, which will need doctrine and jurisdiction study to be truly adapted to a median that constantly suffers intense changes, like Software Development. At the same time there is a growing interest in assuring the rights of citizen's personal data, the area of computer sciences lives through a growing focus on data security. Among the many tools that can be used in this subarea of that science, it is Blockchain that stores its data in a way that they can not be modified or deleted after insertion on the distributed registry. That, however, conflicts with article 18 of LGPD, which grants Brazilian nationals the right to demand the exclusion of certain modes of date, when this is required by the rightful owner of the data.

Keywords: Blockchain. Data privacy. Right to privacy.

SUMÁRIO

1 INTRODUÇÃO

A proposta do presente trabalho é esclarecer que algumas medidas serão necessárias para assegurar o direito à privacidade, resguardado pela aplicação da Lei Geral de Proteção de Dados protegida pela Autoridade Nacional de Proteção de Dados, no que concerne ao uso do *Blockchain* como ferramenta de armazenamento de dados, devido ao direito ao esquecimento elencado em seu artigo 5º, inciso XIV.

Blockchain, em suma, pode ser caracterizado como um tipo de banco de dados, que é duplicado em cada computador pertencente à uma rede. É essencialmente um livro de registro distribuído e o ato de remoção de dados do seu armazenamento é de extrema dificuldade, ou até mesmo, impossível. Há de se ressalvar que tal dificuldade advém de seu originador objetivar o uso esse tipo de registro para a criação de uma criptomoeda, o Bitcoin.

No segundo capítulo, dividido em quatro subtópicos, será feita um breve histórico do que motivou a decisão de garantir o direito ao esquecimento, assim como graves ocorrências e como suas consequências poderiam ter sido minimizadas caso mecanismos legais semelhantes à LGPD existissem contemporaneamente aos ocorridos.

Em seguida, o subcapítulo 2.1 tratará de como a "*War on Terror*" dos Estados Unidos da América acabaria gerando uma grande crise de segurança, culminando em atentados terroristas. Esses atentados geraram uma crise de segurança de dados e, a partir disso, é possível analisar como uma legislação serve para resguardar os cidadãos, não só de ameaças criminais, como também da própria máquina da Administração Pública.

No subcapítulo subsequente, tratar-se-á dos acontecimentos que cercaram o delator da NSA, Edward Snowden, dos abusos à privacidade cometidos pelas agências de inteligência americanas. A partir disso, será analisado como o vazamento de vários documentos sigilosos culminou na revelação da profundidade das agências de inteligência mundo afora, que espionavam não só os países rivais, mas também seus próprios cidadãos.

No terceiro subcapítulo trataremos das eleições americanas de 2016 e a eleição brasileira de 2018. São caracterizados como processos eleitorais amplamente afetados pela utilização de meios digitais, inclusive com profundo uso de dados pessoais e pelo crescente impacto que as redes sociais demonstraram, tal como o surto das "*fake news*", que culminaram em Comissão Parlamentar de Inquérito, em curso ainda no ano de 2021. É mister também destacar o impacto

das ações tomadas pelas grandes empresas de sistemas americanos, como *Facebook* e *Twitter*, na contenção ao alastramento dos mecanismos utilizados em 2016 e 2018 e como elas podem ter reduzido os impactos de práticas ilegais na eleição de 2020.

Por fim, o último subcapítulo ater-se-á como a Lei Geral de Proteção de Dados fora concebida. Será analisado a sua importância para o ordenamento jurídico pátrio, o seu caráter principiológico, objetivando resguardar direitos abstratos como o da privacidade – que se encontravam em estado de carência devido as profundas mudanças tecnológicas causadas pelo advento dos *smart phones* e da internet – assim como a pressão externa motivadora para a sua adoção, e de como esse dispositivo é insuficiente para sanar alguns dos maiores riscos digitais, como o das notícias falsas.

O 3º capítulo abordará como veio à prominência o *Blockchain*, os principais eventos dessa ferramenta e suas principais direções futuras. Também será explorado seus benefícios e possíveis malefícios e como será necessário ajustar a ferramenta para se enquadrar nas previsões legais. Além disso, é levantado o questionamento se a lei deve se ajustar à uma realidade técnica que dificulta sua execução em texto.

Na abertura do capítulo, falar-se-á do surgimento da ferramenta, na década de 80, sua visão e como ela só acabou sendo adotada com o advento de Satoshi Nakamoto, figura ou figuras anônimas até o dia atual, criador anônimo da ferramenta de maior renome que utiliza essa tecnologia, o Bitcoin. Subsequentemente será disposto das Criptomoedas, sua conceituação e a razão do seu surgimento, além de uma breve análise sobre a necessidade de regulamentação dessas moedas e de como a falta de fiscalização faz com que elas sejam ótimas ferramentas para a evasão fiscal e lavagem de dinheiro.

Na 3ª parte desse capítulo faz-se mister abordar os *Smart Contracts*, tratando de forma breve sobre o que são, suas benesses e suas falhas, principais dentre essas à ausência de quaisquer ferramentas de mediação, propiciando nesse ambiente uma possibilidade de abuso inerente à de um ambiente não regulado.

Por último será disposto sobre o *Blockchain* como ferramenta de armazenamento de dados, principalmente tendo seu uso proposto e até planejado como forma de guardar dados de pacientes, documentos, dentre outros. Serão elencados seus benefícios ao combate à fraude e as dificuldades dessa ferramenta na exclusão de dados do armazenamento.

No capítulo final desse trabalho, almejou-se responder sobre o questionamento de como os *Blockchains*, em sua função de Banco de Dados, seriam capazes de adequar-se ao inciso VI do artigo 18 da LGPD, ou seja, de como elas respeitariam o direito ao autocontrole sobre os dados pessoais, que fora criado por tal inciso e é embasado no direito à privacidade, respaldado na Constituição Federal.

2 PRINCIAPAIS MUDANÇAS NA SEGURANÇA DE DADOS NO ANDAMENTO DA HISTÓRIA CONTEMPORÂNEA

Existem vários exemplos na literatura de ficção científica sobre distopias em que privacidade é apenas uma ilusão do cidadão. O mais famoso e citado é “1984” de autoria de George Orwell, que reimaginou políticas já utilizadas de vigilância interna por sistemas ditatoriais de uma forma moderna. Atualmente, nem se faz mister buscar exemplos literários, basta examinar a nação chinesa que já vigia seus cidadãos e possuí um sistema de crédito social. (KOBIE, 2019)

O sistema supracitado julga não só suas ações – desde crimes penais como atrasar as contas – mas também seus acompanhantes, já que ser visto no mesmo grupo com alguém de crédito “ruim” pode impactar sua pontuação, e, consequentemente, impacta privilégios: desde conseguir passaporte e empréstimos com juros baixos, caso possua uma avaliação positiva, a ser privado de utilizar aviões ou ser proibido de adquirir propriedades novas, caso sua pontuação seja negativa.

Por fim, embora tais circunstâncias pareçam impossíveis para um país democrático como o Brasil, disparos de notícias falsas em massa, tal como os vazamentos de dados sensíveis que acontecem de forma semirregular por grupos de “*hackers*”, trouxeram à tona a necessidade de resguardar o direito do cidadão brasileiro de ter seus dados removidos de qualquer forma de armazenamento. (CAPPELLI, 2021)

2.1 “GUERRA AO TERROR” E O *US PATRIOT ACT*

Para compreender o *US Patriot Act* é necessário regressar até o dia de 11 de setembro de 2001. Foi um acontecimento de forte impacto no público americano: a nação estadunidense foi atacada em dois de seus principais símbolos e, caso os passageiros do quarto avião não tivessem logrado êxito, teriam sido alvejados em três. Foi nesse contexto histórico que o congresso americano aprova o *Uniting – Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* – O *Patriot act*, que foi aprovado de forma quase unanime, com apenas um voto contrário.

Esse ato cobria vários aspectos do combate ao Terrorismo, à criação do *Department of Homeland Security*. Foi nele que o crime de Terrorismo foi tipificado na legislação americana e, embora assunto de grande controvérsia atualmente, foi em sua grande maioria recepcionado de forma pacífica pelo ordenamento jurídico americano. Todavia, vale ressalvar que suas provisões, que permitiam ao Estado tomar medidas de espionagem, foram aprovadas em caráter temporário e, embora tenham sido renovadas, a cada renovação a discussão e as suspeitas aumentavam. (LIND, 2015)

Logo, o clima da época em que fora redigido culminou na provisão mais problemática do ato, a infame seção 215, que permitiu às agências de inteligência americanas acesso a escutas telefônicas, monitoramento de e-mails e acesso a quaisquer informações de negócios por meio extrajudiciais como forma de combater o Terrorismo. O legislador americano, visando facilitar o combate ao inimigo não se atentou ao potencial de abuso que essa provisão tinha nas mãos dessas agências.

Vale a ressalva que a própria alcunha de "terrorista" – principalmente após os atentados de 2001 – fora utilizada para justificar não só essas violações dos direitos individuais dos cidadãos daquele país, como também uma desumanização que ultrapassou fronteiras nacionais. O filosofo Héctor Luis Saint-Pierre disserta acerca da definição da palavra terrorismo:

> O perigo é que dela se derivam decisões políticas que conduzem ao emprego da força. A falta de objetividade e critérios de aplicação na definição extensional faz dela uma caracterização arbitrária e, de sua aplicação, uma decisão meramente política. Além das questões ontológicas e epistemológicas dessa forma arbitrária de definição, ele obnubila o desenho estratégico e dificulta enfrentar essa ameaça eficazmente. Chama-se atenção para o uso político cada vez mais frequente desse termo para criminalizar grupos e movimentos sociais contestatários, pois assim se pretende legitimar todo tipo de meios de combate, inclusive a tortura.

Foi essa extensão que acabou por aumentar o escopo das vigilâncias das agências de combate à essas atividades, que expandiram e aprofundaram seu monitoramento dos cidadãos. O que antes era apenas o registro das chamadas feito por um suspeito, transformou-se numa escuta telefônica, e depois na utilização da câmera do mesmo telefone para conseguir gravações de vídeo das pessoas sob observação, culminando nos abusos que foram relatados na delação do ex-agente da *National Security Agency*, Edward Snowden.

2.2 A DELAÇÃO DE EDWARD SNOWDEN

Edward Snowden, ex-assistente técnico da *Central Inteligence Agency* e da *National Security Agency*, duas agências de inteligência do governo americano, destaca-se como um dos, se não o maior delator da história. Snowden se confirma como uma das figuras mais controversas dentro da política norte-americana, havendo ampla discussão se seria justo pelas revelações que fizera.

No dia 20 de maio de 2013, ele fugiu de seu posto de trabalho, em uma agência da NSA no Havaí para Hong Kong e no começo do mês de junho revelou milhares de documentos sigilosos da NSA para vários jornalistas e veículos de imprensa dentre os quais destacam-se o *The Washington Post* e o *The Guardian*. (BRENAN, 2013)

Destaca David Pozen: "Nenhum caso de delação tem sido tão louvado e vilificado que o de Edward Snowden." Do Nobel da paz à pedidos de sentença de morte por suas revelações, seu caso encontra fortes respaldos numa dicotomia moderna: segurança versus liberdade. Para os defensores da proteção, ele é um vilão que pôs por baixo anos e talvez até décadas de progresso na vigilância digital. Assim, para os que resguardam a liberdade acima de tudo, ele é um herói que colocou sua própria vida em risco para revelar abusos de poder.

Sob um viés crítico, sem dúvidas Snowden atrapalhou um aparato montado pelas agências norte americanas para combater o "terrorismo". Fator esse que pode culminar facilitando essas tais ocorrências, mas, ao mesmo tempo, foi de valor imensurável para destacar o quão frágil era a sensação de privacidade.

Todavia, há de se mencionar que embora os defensores do acesso irrestrito a esses dados aleguem que seu uso era exclusivo para os seus fins devidos, os vazamentos ora liberados pelo ex-agente comprovam que abusos não eram raros. No caso do Brasil, por exemplo, a ex-presidente Dilma teve ligações telefônicas com seus principais assessores vistoriadas utilizando essas ferramentas. (GREENWALD, 2013)

De fato, documentos liberados pelo delator comprovaram que interesses de segurança não foram os únicos que guiaram tal vigilância, tendo o Canadá obtido dados sigilosos e e-mails de funcionários do Ministério de Minas e Energia, assim como a Petrobrás, maior multinacional brasileira na época, que teve sua rede de dados violada pela NSA. (GREENWALD, 2013)

2.3 ELEIÇÕES AMERICANAS DE 2016 E BRASILEIRAS DE 2018

Impossível mencionar essas eleições sem referir a Cambridge Analytica. Embora já extinta na eleição brasileira de 2018, seu impacto ainda persiste. Suas estratégias de relações públicas não foram esquecidas com sua queda, muito pelo contrário: as sabatinas na comissão parlamentar britânica revelaram que a estratégia da firma não só funciona, como é qualificada como uma arma de engenharia social, segundo Brittany Kaiser, ex-funcionária da firma em depoimento ao *Commons Culture Committee*. Essa estratégia de relação pública tornou-se um produto cuja demanda explodiu com o sucesso do "*BREXIT*", serviço esse que a firma viria a exportar para os Estados Unidos da América.

O maior escândalo de vazamento de dados do mundo foi deflagrado em 2018, quando foi revelado que a empresa inglesa teve acesso, ilegítimo, aos dados de mais de 50 milhões de usuários do Facebook, inclusive mantendo esses dados em uso após ter afirmado tê-los deletados para a empresa americana. (CADWALLADR, 2018) A Cambridge Analytica afirmou ter 5 mil pontos de dados sobre cada cidadão americano que exercia seu direito de voto e fazia uso dessa informação para radicalizá-los, se possível. Caso fosse inviável, outra estratégia que a empresa já havia aplicado com sucesso em Trinidad & Tobago fora a de propagar a Apatia, ou seja, fazer com que os eleitores não queiram votar, seja porque acreditavam que a eleição já estava ganha ou que nenhum dos candidatos mereceria o voto. (STEUART, 2019)

A eleição americana de 2016 teve em seu pilar uma campanha de desinformação voltada quase que exclusivamente ao redor da "*Crooked Hillary*", um grupo de notícia falsas com o mesmo título que caluniavam a candidata do Partido Democrata, fazendo desde acusações plausíveis até às inacreditáveis. Embora após os vazamentos os responsáveis pela campanha do ex-presidente americano Donald Trump neguem a relevância da empresa britânica em sua campanha, o método de espalhar desinformação também logrou êxito nas eleições brasileiras de 2018 o que eleva a credibilidade das alegações feitas por executivos da CIA em entrevista com repórteres disfarçados. (ABC, 2018)

Conforme Sodré, o que se denomina de "*fake news*" ou notícias falsas é uma forma de neologismo utilizado para conceituar uma informação falsa apresentada como se fosse verídica. Outro jurista tratando do mesmo tema, Stanger, leciona que esse termo se tornou vocábulo comum globalmente a partir de notícias inverídicas publicadas de forma oposta. Há sinônimos no português para tal palavra: boatos, fofocas ou simplesmente mentiras. (SODRÉ, 2018)

Segundo Laura Chinchilla, observadora da Organização dos Estados da América: “medir o impacto de *fake news* na eleição é difícil”. Porém, a realidade é que embora seja difícil de quantizar sua importância, tal estratégia que serviu de pilar para a Cambridge Analytica durante a “*Brexit*” e a “*Crooked Hillary*”, ganhou prominência global, e mesmo sem sua empresa fundadora foi utilizada de forma ampla nas eleições presidenciais de 2018.

Há que se destacar uma peculiaridade adotada no Brasil, que foi o alastramento dessas notícias em sistemas de mensagens. Diferente da americana, que fora centrada no alastramento de notícias falsas pela rede social do *Facebook*, a nacional fora centrada no aplicativo de celular *Whatsapp* que, também faz parte do grupo Facebook. Essa mudança trouxe dificuldades no combate a esse veículo de difusão de informações falsas. (CASADO, 2018)

O judiciário já estava alerta para o fenômeno das notícias falsas. De fato, em junho de 2018, Luiz Fux, na época presidente do TSE, junto com representantes de dez partidos políticos, firmaram um acordo para a manutenção de um ambiente eleitoral imune à disseminação de notícias falsas nas eleições do mesmo ano. Contrário ao senso comum, o que aconteceu naquele ano já era esperado, todavia, o volume e meio de dispersão novo dificultou muito na sua contenção. (TRE DO PARÁ, 2018)

Não há consenso sobre os impactos do uso dessas estratégias de comunicação criadas pela Cambridge Analytica nas eleições de 2020 dos Estados Unidos da América, haja vista que a própria empresa já havia sido dissolvida há 2 anos. Além disso, as empresas de tecnologia já haviam desenvolvido os meios para interferir com tais mecanismos sociais, ao contrário do que ocorreu em 2016. Por fim, é notório que mesmo com todas essas medidas para desestimular o uso das notícias falsas isso ainda ocorreu de forma ampla. Demonstrando que esse tipo de disseminação de informações como forma de veículo de relações públicas ainda será um desafio da contemporaneidade.

2.4 A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL: ORIGEM E OBJETIVOS

A Lei Geral de Proteção de dados, publicada em 14 de agosto de 2018 e cujas sanções passarão a ser aplicadas a partir de agosto de 2021; é um instrumento novo e de certa forma desconhecido do ordenamento jurídico nacional. A LGPD tem um processo originário que remete à criação da Lei Aurea, ambos os diplomas legais tiveram suas concepções motivadas por pressões internacionais pois a União Europeia, ao proclamar a *General Data Protection*

Regulation, restringiria suas empresas a somente poderem contratar empresas de países com níveis adequados de proteção de dados. (COTS, 2018)

Tal pressão externa culminaria em impactos financeiros ainda mais fortes para as empresas brasileiras de sistemas, que acabariam impossibilitados de quaisquer coleta e uso de dados europeus, não havendo paridade legislativa. Tal fator culminou com o interesse do congresso nacional em alavancar projetos de leis já existentes, porém de baixa prioridade.

Outro grande impulsionador para a promulgação desse dispositivo legal foi citado caso da Cambridge Analytica, que manipulou dados pessoais de inúmeros nacionais de vários países para influenciar em várias eleições, e segundo seus executivos a principal líder da campanha do ex-presidente americano Donald Trump em apenas 3 anos. Esse caso chocou o mundo e elevou a necessidade atual de legislar sobre tema tão atual como o da proteção de dados.

Portanto, ao legislador coube essa necessidade a ser suprida, ou o Brasil se enquadraria nos países confiáveis segundo a GDPR ou teríamos mais esse motivo para a marginalização das empresas nacionais que já enfrentam os demais problemas de manter um negócio no país, como corrupção, burocracia, impostos altos e de alta complexidade, dentre outros.

Embora a motivação central fora econômica, a legislação veio em bom tempo para os cidadãos brasileiros, pois com as inovações tecnológicas constantes na computação demonstra que há uma necessidade de tutela legal. Dispositivo esse que objetiva o resguardo da privacidade e direito à vida íntima dos brasileiros que é contemplado em viés constitucional, no seu artigo 5º inciso X dispondo que: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”, agora tem essa proteção constitucional expandida e atualizada para os meios modernos que de certa forma interferem com esse princípio. (BRASIL, 1988)

É mister destacar que o Brasil já havia peças legislativas importantes na área que antecedem a LGPD, como o Marco Civil da Internet e a resolução do CFM 1.821/2007, todavia insuficientes para satisfazer os pré-requisitos estabelecidos no GDPR europeu. O MCI serviu de prévia experiência fundamental para a elaboração da LGPD, notável pela manutenção de definições prévias que foram aprofundadas, como a de “dados pessoais” ou “tratamento de dados”, assim como parte de seus princípios, como o respeito à privacidade, liberdade de expressão, respeito ao direito do consumidor, dentre outros.

Segundo Patrícia Peck, a legislação de proteção de dados pessoais ocorre de forma principiológica, ou seja, a lei traz dentro de si um rol de princípios que devem ser respeitados. A LGPD objetiva, desse modo, a não só proteger os direitos dos titulares desses dados, dotando-os de poder para controlar a manipulação desses, bem como limitando o que pode ser feito por aqueles dispostos a tratá-los. (PECK, 2018)

Segundo preconiza Ronaldo Lemos, um dos maiores desafios da LGPD será o de navegar a amplitude do seu texto, que diverge da GDPR ao deixar um espaço mais amplo para o doutrinador guiar um "debate verdadeiramente local" sobre a aplicação da lei. Tarefa essa que será de suma importância, pois os valores previstos em suas sanções chegam a valores elevados como o de 50 milhões de reais ou 2% do faturamento da pessoa jurídica. O que demonstra a importância que a doutrina, jurisprudência e à Autoridade Nacional de Proteção de Dados devem ter para evitar que tais sanções tragam consequências econômicas. (COTS, 2018)

Em consonância a Peck, defende que não basta a criação da Autarquia, é necessário que ela eduque e capacite. Destacando a importância da Autoridade Nacional de Dados (ANPD), cuja criação é prevista no instrumento legal, é uma autarquia que deve atuar de forma proativa para encontrar medidas viáveis de implementar novas regulações, gerando o menor impacto possível nos setores produtivos que serão fortemente afetados pela legislação. Nesse sentido, o setor de *startups* de tecnologia da informação tem seu protagonismo, ainda mais as que atuam no setor público, com maior ênfase ainda às que lidam com dados sensíveis como os de saúde.

Fica, portanto, ressalvado que embora a legislação tenha sido um passo importante na resguarda dos direitos dos cidadãos, por ser ampla e principiológica restam dúvidas de como sua aplicação ocorrerá de fato. O doutrinador Ronaldo Lemos destaca que um dos principais pontos da aplicação da LGPD será devido ao termo Geral, não estando ele na lei por acaso, responsabilizando toda e qualquer pessoa física e jurídica que utilize dados pessoais de formas indevidas, ele defende também o entendimento de que, embora a ANPD só possa começar a fazer sanções a partir de agosto de 2021, nada impediria o judiciário aplique as sanções dispostas na Lei. (LEMOS, 2020)

Por fim, a lei objetiva propiciar um ambiente digital onde o respeito ao direito da autotutela dos dados é contemplado, dados esses que anteriormente eram usados e comercializados sem consulta. O controle dos dados pessoais é um passo importante para a adaptação do direito à nova era da informação digital, haja vista que se demonstrou necessário por todo o processo histórico que motivou as peças legislativas.

3 BLOCKCHAIN: TECNOLOGIA DE REGISTROS DISTRIBUÍDOS COM O EMPREGO DE CRIPTOGRAFIA AVANÇADA

A tecnologia *Blockchain* é principalmente associada à sua vertente mais conhecida, a das criptomoedas, como o *Bitcoin*. Ela é um banco de dados de registros de transações descentralizado e mantido em uma, ou mais, rede de computadores mundo afora. Ao invés de uma única autoridade central, como um Banco Central, esse registro de transações é supervisionado por uma comunidade ampla e nenhum único indivíduo tem o poder de mudar ou apagar uma transação presente nesse banco de dados. (SARMAH, 2018)

Diverge dos bancos de dados majoritariamente usados nos tempos hodiernos justamente por sua descentralização e por sua difícil manipulação dos dados após inseridos. No seu nível básico, sua função mais importante é justamente essa supervisão comunitária fazendo com que os livros de registro distribuídos dessa tecnologia sejam de dificílima manipulação. Em 2008, esse conceito foi somado à várias outras tecnologias para formar as criptomoedas atuais, sendo a primeira e mais famosa delas o Bitcoin. (NSIT. 2018)

Outro mecanismo de segurança da ferramenta é que a rede tem acesso aos livros de registro de todos os integrantes da ferramenta e ao realizar uma transação tem essa comparação de registro sendo feita por todos eles, após essa igualdade ser estabelecida é que a transação ocorre de fato, passando agora a integrar o livro de registro de todos os integrantes da rede. Essa integração ocorre com a ligação dessa transação com a última que ocorrera antes dessa, já essa última está ligada a penúltima e assim sucessivamente formando uma corrente de blocos de transações, uma *Blockchain.*

A origem desse mecanismo é, ao contrário do senso comum, anterior à criação do *Bitcoin*, de fato em um artigo de 1976 estariam as bases para a tecnologia que seria de tamanha relevância para o avanço da criptologia. O artigo "*New Directions in Cryptography*" já propõe o conceito de livros de registro descentralizados, ou distribuídos embora que de forma mais teórica que prática, compreensível, considerando a incipiência da Internet naquele tempo. Subsequentemente veio a tecnologia de marcação temporal, no artigo "*How To Timestamp a Digital Document*" de Stuart Harber e Scott Stornetta que elaboram o conceito da marcação temporal pela data ao invés do meio. (DIFFIE, HELLMAN. 1976)

Depois disso temos o surgimento do conceito de Dinheiro Digital ou “e-cash” que surgiu em modelo proposto por David Chaum, conceitos esses importantes para a construção do *Blockchain,* pois as principais falhas nessas moedas digitais iniciais foi a do “*Double spending*”, onde o dinheiro digital era copiado e utilizado mais de uma vez de forma análoga à como o dinheiro papel pode ser falsificado, mecanismos que bloqueavam tal fenômeno seriam incorporados, como o consenso da comunidade. (CHAUM. 1983)

Todos esses conceitos são integrados em 2008 por um, ou vários, utilizando o pseudônimo de Satoshi Nakamoto, considerado o inventor da tecnologia *Blockchain* quando publicou o artigo “*Bitcoin: A Peer-to-Peer Eletronic Cash System*” o resumo desse artigo propunha um sistema de transações eletrônicas que funcionária de forma independente à terceiros, firmado nas tecnologias de criptologia e com uma solução para o principal problema que havia exterminado as moedas digitais anteriores, o *Bitcoin* não possuiria o problema do “*Double spending*” por meio do livro de registro descentralizado e do consenso da comunidade que ocorre a cada instante que uma transação ocorre, sendo o livro de registro de cada “moeda” comparado com os demais da rede.

3.1 ASPECTOS GERAIS DA CRIPTOECONOMIA

A ascensão quase que meteórica do Bitcoin desde sua incepção em 2009, saindo de algo que não possuía valor intrínseco para uma ferramenta econômica cujo valor, embora flutuante, seja de meados de 40 mil dólares a unidade, trouxe um gigante interesse na área das criptomoedas, gerando um grande número de outros instrumentos semelhantes mundo afora.

Sua origem segue o viés da necessidade histórica, assim como o homem deixou de usar dinheiro moeda e começa a transladar para dinheiro papel com o advento dos bancos e das grandes viagens comerciais o dinheiro papel começou a ser substituído pelo dinheiro eletrônico já há certo tempo, notavelmente com o advento dos cartões de débito e crédito, mais recentemente com as transações eletrônicas ficando cada vez mais ágeis e fáceis de serem feitas devido aos telefones móveis e semelhantemente notamos esse fenômeno com a adoção do Pix no Brasil.

A diferença dessa mudança de dinheiro físico para o digital que já ocorre às criptomoedas é que não há controle dessas pelos mecanismos financeiros nacionais. De fato, é

devido a uma ampla desconfiança desses instrumentos financeiros que o(s) autor(es) Satoshi Nakamoto vem a remover de forma explicita esse intermediador e garantidor que é presente na nossa história financeira, deixando em sua troca um sistema que independe não só desse terceiro, mas como até mesmo os agentes realizando as trocas não precisam se conhecer. (CHOHAN, 2017)

Após a disseminação das ideias de Nakamoto veio a plataforma para as transações por bitcoin sendo desenvolvida de forma aberta com o lançamento do Bitcoin-Client e o concomitante lançamento dos Bitcoins propriamente ditos. Nakamoto teria então minerado o primeiro bloco de Bitcoins, referidos como “Bloco Genesis”, logo após a primeira transação da história com Bitcoins foi realizada do criador para Hal Finney, no total de 10 Bitcoins.

Foi essa ausência de rastreabilidade, assim como sua independência de autoridades financeiras e nacionais que fizeram o Bitcoin ter um de seus primeiros adotantes famosos, ou melhor infame, o *Wikileaks* que publicou diversos documentos confidenciais de vários países, inclusive do Brasil, foi um dos primeiros parceiros proeminentes da moeda, nesse período, meados de 2010, a moeda tinha valor flutuante e no geral era determinado por transação, sendo uma das mais famosas da comunidade a compra de 2 pizzas por 10.000 bitcoins, com o valor atual em reais de 1.8 bilhões. (ÉPOCA NEGÓCIOS, 2018)

O ano de 2013 trouxe consigo mudanças profundas para a moeda em ascensão, antes dele o Bitcoin estava voando por baixo dos radares das entidades reguladoras, ao fim desse ano o Bitcoin já estaria regulado, embora ainda não em formato de lei, nas principais economias do mundo. Os EUA por meio do *American Financial Crime Enforcement Network* estabeleceram regras gerais para moedas digitais descentralizadas, dentre elas o *Bitcoin,* a violação de algumas dessas traz inclusive a sanção de confisco das contas envolvidas.

Visível, portanto, a ascensão dessa criptomoeda, e como esse processo célere envolveu muito dinheiro, esses altos valores financeiros trouxeram gigantes interesses na área que culminaram com as inúmeras criptomoedas que existem hoje, todavia, esse desenvolvimento não se deu completamente cercado de legalidade, o objetivo de Nakamoto de desenvolver um mecanismo financeiro de difícil rastreio não passou desapercebido pelos mal intencionados, de lavagem de dinheiro à um atual gigante esquema de Ponzi com uma outra, ao que tudo indica, falsa criptomoeda esse ramo do Blockchain trouxe consigo desafios inéditos aos operadores do direito.

Desde a incepção das criptomoedas, céticos alegaram que elas poderiam ser utilizadas para os que intencionam evadir as leis, empoderando hackers e criminais, seu anonimato, sua facilidade de transpor fronteiras e a falta de regulações claras são de extremo apelo para aqueles que desejam evitar as organizações de fiscalização. Há dois grandes exemplos com o Bitcoin, e outro de suma relevância com as criptomoedas no geral, a começar pelo *Silk Road* o infame site criado por Ross William Ulbritch, autointitulado "*Dread Pirate Roberts*". (POPPER, 2015)

Autointitulado de anarquista, Ulbritch sonhava com um mercado online onde pessoas poderiam comprar de tudo sem a interferência do governo, de narcóticos a outros itens ilícitos. Antes do advento das criptomoedas já existia a chamada "*Dark Web*" que nada mais é que a parcela da internet não disponível nos motores de busca, sites como Google e Yahoo. Os usuários que navegam essas partes da Internet geralmente o fazem para conseguir acesso à conteúdo proibido ou simplesmente não difundido no resto da internet, eles já possuíam meios de manter suas identidades sigilosas, fazendo uso de ferramentas como Tor ou redes virtuais privadas, ferramentas essas que dificultam ou até impossibilitam o rastreio de suas máquinas, porém, indispunham antes do advento das criptomoedas de um mecanismo de pagamento adequado.

Ulbritch foi talvez o primeiro a notar que o Bitcoin e as criptomoedas no geral sanavam esse problema, o de poder fazer transações financeiras sem ter que quebrar o anonimato. Criando uma espécie de mercado livre do crime, ele conectou traficantes, desde aqueles pertencentes ao crime organizado à até os que fazem plantio próprio ao consumidor de uma forma nunca feita, como as transações em bitcoin não deixam indícios das identidades dos que as realizam.

Todavia, esse crescimento trouxe consigo atenção que acabou gerando a operação "Marco Polo" realizada pelo *Federal Bureau of Investigation* dos EUA, como não seria possível o rastreio financeiro, a polícia americana utilizou a única parte do negócio impossível de se digitalizar para conseguir começar os rastreios, a logística. Todavia, logo notaram que o negócio não seguia a estruturação de uma organização criminosa tradicional, era uma espécie de "Bazaar" do crime e o método de ficar apreendendo usuários não levaria ao fim do mercado em si.

O FBI americano prende Ulbritch após quase 3 anos de funcionamento do site, chegando inclusive a causar uma queda na valorização da moeda que logo recuperou-se. Há principal

problemática com as criptomoedas é seu potencial como forma de lavagem de dinheiro, transferências de difícil, se não, impossível rastreio com moedas cuja origem é desconhecida e que pode ser transformada em valores legais com facilidade ajudam muito na ocultação de patrimônio, por exemplo, crime previsto no Brasil.

A verdade é que assim como preconiza Jacqueline de Souza Abreu as criptomoedas ainda não são consideradas com a profundidade e incidência adequada no que diz ao seu tratamento, suas implicações e suas consequências jurídicas associadas ao uso dessa tecnologia. Já o forense Michael Doran destaca que os benefícios da integridade, confidencialidade e integridade quando somados com as baixas taxas cobrados pelos softwares que aceitam o uso das criptomoedas como forma de pagamento além do baixo risco aos comerciantes são grandes motores que impulsionaram sua adoção. (ABREU. 2017)

Também digno de destaque é que o anonimato das transações financeiras é direito que já existe no Brasil, esse é respeitado no uso das criptomoedas, todavia um problema inicial com a legislação local é encontrado quando consideramos que as transações de Bitcoin são irreversíveis, sendo reversíveis apenas dependendo da boa vontade do vendedor, cuja identidade pode ser desconhecida pelo comprador. Está evidente então uma primeira lacuna legal no uso das criptomoedas, violando o direito de desistência do consumidor presente no Artigo 49 do Código de Defesa do Consumidor. (BRASIL, 1990)

Outro problema gerado pela ausência de regulação é um temor justificável de que o uso das criptomoedas possa facilitar crimes como lavagem de dinheiro, tráfico de drogas, pirâmides financeiras, estelionato e evasão de dívidas. As facilidades geradas por esse ambiente inédito podem atrair usuários que pretendem utilizar esse ambiente inédito para violar limites previstos em leis que ainda não se adaptaram à essa nova ferramenta.

O jornalista James Melik arguiu que uma das problemáticas da criptomoeda é que ao abrir uma conta bancária convencional o indivíduo precisa apresentar documentos válidos além de necessitar comprovar uma residência real enquanto para criação de conta de criptomoedas a única necessidade é de um endereço de IP válido que pode ser falsificado com uso de ferramentas feito proxies, simulando IP distinto daquele do usuário. (MELIK, 2012)

Por fim, no caso específico da “Rota da Seda” site americano que servia de “Hub” de distribuição para o tráfico de drogas não só conseguimos claramente notar que incorreram no crime de tráfico como também, ao utilizar *bitcoins*, mister que seja acoplado também o crime

de lavagem de dinheiro, pois as bitcoins provenientes desse comércio ilícito são mais fáceis de serem reutilizados que o dinheiro proveniente de atividades ilícitas.

Como sabe-se a lavagem de dinheiro conforme prevista na lei 12.683/2012 é a utilização de empresas ou meios afins, visando transformar o capital adquirido através de atividades ilegais em capital "limpo" ou legal, podendo então ser depositado em contas bancárias e utilizado de forma aberta sem atrair a atenção das autoridades pertinentes. Fácil notar que a *bitcoin*, devido a seu anonimato, alta demanda e capacidade de ser minerado apresenta uma brecha que pode e já deve estar em utilização para esses fins. (BRASIL, 2012)

Outro grande problema com as criptomoedas causados pelo seu anonimato e pela lacuna legal na qual ainda operam, causou um dos maiores esquemas de estelionato e pirâmide financeira do mundo, chegando ao montante de 3.4 bilhões de euros em cerca de 2 anos os promotores americanos atualmente processam os principais líderes do *OneCoin* com fraude e lavagem de dinheiro. Embora o valor da suposta criptomoeda tenha chegado à 29,95 euros no seu pico na realidade ela não possui valor algum, *OneCoin* não disponibilizou aos investidores forma alguma de rastrear seus valores e não pode ser utilizada para comprar nada. (DOLMETSCH, 2019)

Embora seja verdade que o advento de estelionatos já tenha sofrido aumentos com a popularização da Internet, pois ela interconectou mais os seres humanos e essa conexão fez com que os "agressores" que a utilizam para explorar pessoas, conseguissem fazê-lo através de computadores com uma maior facilidade, as criptomoedas, em desvio de sua finalidade por essas pessoas, dificultam também o trabalho da polícia ao investigar pessoas que praticam atos não só como os do *OneCoin*, que foi um esquema gigantesco. Mas também, charlatões que praticam estelionato, como preconizado no artigo 171 do código penal, e chantageadores, como por exemplo os grupos de hackers que ainda esse ano pararam um duto de Petróleo nos EUA que buscavam um resgate em criptomoedas.

Por fim, fica claro que embora as criptomoedas possuam enorme potencial financeiro, de quebrar ainda mais barreiras para a circulação de capital e de remover dos bancos o controle total dos valores em circulação ela traz consigo desafios inéditos e uma necessidade clara de regulamentação para sanar seu potencial uso de má-fé.

3.2 SMART CONTRACTS

Uma das principais invenções decorrentes do *Blockchain* foi a criação dos *smart contracts*: contratos de execução automáticas regulados por código de computador. Tais mecanismos permitem uma celeridade na execução contratual que ocorre automaticamente assim que as condições forem satisfeitas, realizando transações de bens e moedas de todos os tipos como forma de pagamento pelo serviço acordado. (SZABO, 1997)

Esses contratos inteligentes ganharam proeminência com o desenvolvimento do *Etherium*, atualmente a segunda maior criptomoeda em circulação que possui no seu código uma ferramenta que possibilita a criação e execução automática desses contratos entre duas partes que sequer necessitam se conhecer. Essa ferramenta está em pleno crescimento e em uma pesquisa publicada no jornal financeiro americano Bloomberg o mercado dela deve chegar ao valor de aproximadamente 350 milhões de dólares até 2026. (BLOOMBERG. 2021)

O principal empecilho legal dessa ferramenta em ascensão é o da sua irreversibilidade e inflexibilidade que os colocam em conflito direto com muitos, se não todas as legislações cíveis do mundo. Uma vez assinados, esses contratos se auto executam de forma alheia aos controles jurídicos do Estado, dessa forma nem mesmo uma decisão jurídica de uma justiça competente poderia congelar ou reverter tal instrumento. Ainda mais quando o pagamento regido por esse *smart contract* são de quantias em criptomoedas, muitas vezes de transferências irrastreáveis e cuja reversibilidade dependem apenas da boa-fé do recebedor dos valores.

Inadmissível portanto, no ordenamento jurídico brasileiro, cogitar a utilização dessa ferramenta nessa forma original, pois os contratos poderiam ser executados sem que as partes possam utilizar dos seus direitos de arguir nulidade ou anular o negócio. Ferindo então os artigos 147, 166 e 167 do Código Civil, bem como quaisquer outros que discorrerem sobre eventuais causas de nulidade ou anulação contratual, pois por ser cumprido de forma automática o contrato é apenas uma forma pura de *Pacta sunt servanta* ignorando milênios de avanço no direito civil que advém desde o direito romano. (BRASIL, 2002)

Outro pilar do direito brasileiro ao qual essa ferramenta no presente estado encontra-se inaceitável é o direito do consumidor, principalmente no que tange das relações comerciais pela internet, havendo no Brasil o direito a desistência de compras online que perdura até 7 dias

depois do recebimento do produto, podendo até o fim desse prazo o consumidor desistir e ser ressarcido de forma integral aos valores usados para a compra.

Há que se mencionar que os desenvolvedores que almejam pelo aperfeiçoamento e adoçam dá ferramenta para o uso cotidiano já identificaram os vários problemas que essas formas de contratos causam, havendo inclusive uma ideia na comunidade da adoção de uma ferramenta chamada de *Judge as a Service.* Uma espécie de árbitro ou intermediador que teria poderes para sanar vício ou até mesmo reverter as transações realizadas na *Blockchain.*

Existiria, portanto, segundo defendido pelos juristas Pedro Vilela e Rafael Coutinho, uma aproximação desse árbitro do *Judge as a Service* com o mecanismo da Arbitragem Judicial posta em prática pelo novo Código de Processo Civil de 2015 que almeja reduzir os longos tramites jurídicos para uma forma de resolução mais consensual e célere das demandas. (GONÇALVES, CAMARGOS, 2017)

Todavia, resta ainda conhecer se com essa adição à execução dessa nova modalidade contratual haveria forma de controle jurisdicional, pois mesmo com a existência dessa figura arbitral ainda é mister que haja a possibilidade de intermédio do judiciário para garantir os direitos fundamentais dos brasileiros, assim como é preconizado no artigo 5º inciso XXXV da nossa magna carta “A lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito”.

Embora o “Juiz de serviço” dos contratos inteligentes represente um avanço para sanar essas deficiências legais da aplicação do *smart contract* no Brasil, notável que essa ferramenta ainda necessitará de várias adequações para que haja sua inserção como uma modalidade contratual de uso amplo. No momento, sem que haja a observância dos direitos dos contratantes essa forma incipiente de contrato traz consigo uma insegurança jurídica que deve ser sanada para se adequar ao devido processo legal.

3.3 BLOCKCHAIN COMO FORMA DE ARMAZENAMENTO DE DADOS

Existem duas formas principais de utilizar o *Blockchain* para armazenamento de dados, utilizando-o como um Livro de Registro distribuído permitindo que todos os participantes tenham acesso à mesma visão do estado do sistema no mesmo tempo. Podendo ser utilizado

para a contabilidade, principalmente para revisões de contabilidade por múltiplas partes pois o livro pode ser distribuído sem haver o temor de que seja adulterado.

Há também a possibilidade a possibilidade de se usar a ferramenta para a criação de títulos digitais, havendo países como Georgia e Suécia que estão experimentando com a utilização de *Blockchain* como forma de registro de imóvel. Não se limitando, todavia, a esses exemplos, podendo ser utilizado para criar registros de outras coisas, como no Brasil está se criando um registro para diplomas de ensino superior o que potencialmente inviabilizará a venda de diplomas. (MEUNIER, 2018)

Outra forma de armazenamento de dados pelo *Blockchain* pode ser o da prova de validade, pois essa ferramenta permite que informação seja datada, autenticada e armazenada de forma imutável, poderia, portanto, validar informações sem depender de uma terceira parte, com possíveis utilizações se mesclando com as de armazenamento de título. Pois a ferramenta não só armazenaria os títulos e livros de contabilidade de forma muito difícil de ser adulterada como também pode ser utilizado para validar tais documentos.

É mister, relembrar como o *Blockchain* funciona, principalmente no que concerne a adição de novos blocos à comunidade, os blocos quando publicados tem seu histórico comparado com o de toda a comunidade e caso não sejam aprovados são então declarados falsos e descartados, isso é importante pois a cada bloco novo que se é criado esse histórico fica cada vez mais difícil de ser manipulado explicando por fim, como que o sistema validaria eventuais documentos. (NSIT. 2018)

Estando compreendidas essas possibilidades atuais, que provavelmente serão estendidas a outros dados cujo armazenamento seguro sejam de amplo interesse, como nos EUA onde já se discute prontuários ou até mesmo históricos médicos de pacientes que poderiam ser armazenados de forma digital em *Blockchain,* necessário também entender que essa ferramenta e outras nesse viés de formas de armazenamento seguras necessitarão de ampla discussão legal, doutrinária e jurisprudencial no Brasil.

3.4 DIREITO À PRIVACIDADE, LGDP E BLOCKCHAIN COMO FORMA DE ARMAZENAMENTO DE DADOS

A Lei Geral de Proteção de Dados veio para servir de norte jurídico para como os dados dos brasileiros devem ser tratados, armazenados e explorados e em seu texto confere vários direitos aos cidadãos dessa nação, devido aos vários escândalos de violação de privacidade, venda de dados por empresas e até utilização desses dados para influenciar em eleições o legislador conferiu ao brasileiro várias modalidades do direito à privacidade, dentre delas encontra-se o direito ao esquecimento.

O "esquecimento" surge como direito pela primeira na União Europeia, em seu regulamento 2016/679 no artigo 17º que ao tratar da exclusão de dados confere em forma de subtítulo o "direito a ser esquecido", ultrapassando essa menção no considerando 66 desse mesmo regulamento preconiza o "direito a ser esquecido no ambiente por via eletrônica".

Necessário definir que se entende por esquecimento não o sentido literal da palavra, pois dados não são memória para que sejam esquecidos, mas, na realidade, o direito de restringir o acesso à dados que o indivíduo não queira que sejam publicizados ou ainda, requisitar a remoção desses dados de forma que eles não possam mais serem utilizados. Segundo o Supremo Tribunal Federal no seu RE 1.010.606/RJ, o direito ao esquecimento estaria ancorado no direito a proteção do nome, da vida privada, da honra e da dignidade. (STF, RE1.010.606, 2021)

Digno de menção também que o STF, nesse mesmo RE entendeu que o Direito ao esquecimento é incompatível com a Constituição Federal quando utilizado para impedir a divulgação de Fatos verídicos, obtidos de forma lícita e, no caso específico, haviam ocorrido há muito tempo e que caso o direito ao esquecimento fosse aplicado, implicaria em censurar o direito de liberdade de expressão, existindo ressalva explícita na própria lei no artigo 4º, inciso II dá utilização de dados para fins jornalísticos. Não atingindo, portanto, o direito ao esquecimento enquadrado na LGPD, pois os dados digitais obtidos pelas empresas de tecnologia seriam de propriedade do cidadão e, ao obstar da utilização deles, os dados não seriam mais obtidos de forma lícita.

Considerando que as empresas de tecnologia não se enquadram em um uso de liberdade de expressão, o armazenamento de dados pessoais de indivíduos em forma de *Blockchain* apresentaram desafios inéditos ao direito nacional, não apenas cível, há uma crescente

possibilidade da adoção dessa ferramenta para emissão de títulos notariais e para armazenamento seguro de prontuários eletrônicos como proposta pelos autores Thiago Vieira et al. (VIEIRA *et al*. 2016)

Como conciliar então uma ferramenta criada para prevenir alterações com a necessidade de que os dados sejam manuseados caso o cidadão requisite sua deleção, eis o principal desafio que as empresas de tecnologia enfrentarão ao adotar essa ferramenta inovadora com a entrada em vigor da LGPD. Faz-se mister portanto conciliar o direito à privacidade do cidadão, com o direito a exigir que seus dados sejam deletados e a incapacidade da ferramenta de excluir, propriamente dita, os dados.

Danilo Doneda jurista atuante na área de Proteção de Dados discorre que privacidade como entendemos de forma hodierna só adveio com o final do século XIX pois houve uma "mudança na percepção da pessoa humana pelo ordenamento e ao qual se segue a juridificação de vários aspectos de seu cotidiano". Óbvio que a privacidade nesse período não encontrava desafios modernos como o da Internet, porém um produto incontestável da revolução industrial foram as migrações urbanas que ao intensificar a densidade demográfica, trouxe essa preocupação antes inexistente à tona. (DONEDA, 2006)

Não podendo, todavia, confundir privacidade com isolamento e nesse sentido a LGPD atua não para "isolar" o indivíduo, mas para, como argui Márcio Cots, garantir que ele escolha à quem admitir em sua vida privada, assim como as formas dessa admissão. Logo, tornou-se a privacidade direito fundamental da pessoa humana, possível de ser verificado no artigo 12º da Declaração Universal dos direitos Humanos, no inciso X do artigo 5º da Constituição Federal brasileira, cujos efeitos emanaram para outras peças legislativas, como o Código Civil, Marco Civil da internet, dentre outros, como inclusive a LGPD. (COTS, 2019)

Restando fundamentada a motivação principiológica por trás do parágrafo 5º do artigo 8º da LGPD, em seu texto ele preconiza que:

> O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação nos termos do inciso VI do *caput* do artigo 18 desta Lei.

Torna-se bastante clara a procura do legislador pela resguarda do direito à privacidade e da criação de um novo direito, o da Autodeterminação informativa, termo que segundo Bruno Bioni advém de decisão judicial da corte constitucional alemã que em 1983 cunha o termo, construindo que o cidadão deve ter o controle de seus dados pessoais com o viés que ele possa autodeterminar suas informações privadas. (BIONI, 2019)

Ainda mais claro que o esse parágrafo do artigo 8º é encontrado no inciso mencionado em seu texto, o VI do caput do artigo 18º da LGPD que preconiza:

> 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:
> VI – Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta lei;

Márcio Cots defende também que além de poder requisitar acesso e ou restringir o acesso a esses dados ao titular do direito também é devido pelo controlador desses dados que informe o titular do que será realizado com eles, não cabendo, portanto, ao titular o dever de presumir o que acontecerá. (COTS, 2019)

O que fazer, portanto, com dados que não poder ser eliminados de caráter pessoal será a questão que a doutrina e jurisprudência deverá responder com a aplicação da LGPD, há que se compreender que embora a deleção dos dados inclusos numa *Blockchain* seja de fato, impossível, impedir que esses dados sejam acessíveis não o é.

4 CONSIDERAÇÕES FINAIS

Como já dito previamente, a autoderminação dos dados assim como o direito à privacidade assume posições centrais na LGPD, principalmente naquilo que concerne o tratamento de dados pessoais principalmente para que o Brasil atinja o status de “seguro” para o padrão internacional, principalmente para que as empresas brasileiras possam continuar a realizar transações com as europeias, que só é possível com a manutenção desse patamar de proteção aos dados pessoais.

Todavia, existem alguns desafios quando a ferramenta *Blockchain* é utilizada como forma de armazenamento de dados, principalmente os médicos, documentais ou até mesmo como forma de armazenamento de dados que não devem ser manipulados.

O Prontuário Eletrônico Pessoal de um paciente pode ser uni ou multiprofissional a depender do atendimento e do estabelecimento onde o mesmo busca atendimento, e em quaisquer das situações é um documento que armazena dados pessoais e histórico clínico do mesmo, resultado de exames, condutas e planos de cuidado, dentre outros. (FERNANDES, GOLDIM, 2019.)

O *Blockchain* como já estabelecido é uma ótima forma de garantir que tais informações, de suma importância para a preservação da vida no exemplo do PEP, tenham seus dados validados e armazenados de forma segura. Entretanto, como já aqui explanado o cidadão brasileiro possui o direito à autodeterminação dos dados pessoais como uma forma de fazer cumprir seu direito à privacidade, resguardado na Constituição e adquirido exigibilidade pela LGPD.

Como, portanto, sanar essa divergência, principalmente quando é notório que todos as demais formas de utilização dessa tecnologia para armazenamento de dados podem ocasionar nessa mesma consequência. Deduzível que documentos armazenados assim também conteriam dados pessoais, assim como outras informações que assim armazenadas também encontrar-se-iam à mercê da vontade do titular dos dados que pode a qualquer instante requisitar do controlador a eliminação dos dados pessoais.

Ao mesmo tempo, como arguir que direitos, cuja construção histórica aqui detalhados adveio de processo histórico que demonstrou amplamente a capacidade de abuso, e o abuso de

fato que ocorreu em países estrangeiros, trazendo até consequências como monitoramento de presidente da república brasileira de forma irregular. (GREENWALD, BRIDI, 2013)

A situação torna-se ainda mais complexa quando se considera que o caminho da criptologia, principalmente como forma de armazenamento seguro de dados caminha para que cada vez mais os dados sejam de difícil adulteração e até mesmo deleção. Visível aqui que a necessidade de segurança dos dados poderá se confrontar com o controle dele.

Ainda digno de menção é que existe no Congresso Nacional uma preocupação gritante com a proteção de dados pessoais que existe a Proposta de Emenda Constitucional 17/2019 que atua visando a inserção do direito à proteção dos dados pessoais no artigo 5º da Constituição Federal, além de atribuir a competência exclusiva de legislar sobre o Tema para a União, os legisladores ambicionam fazer o acompanhamento do progresso tecnológico.

Postos aqui, portanto, os desafios que virão à tona com a utilização da ferramenta e sua adequação para as conformidades da legislação nacional vigente propõe-se duas possíveis saídas: a primeira seria a utilização de um sistema que, embora faça o armazenamento por meio da ferramenta de *Blockchain*, que o faça de forma que os dados explícitos no livro de registro não sejam os pessoais e meramente as formas de certificar à autenticidade dos dados pessoais, a segunda seria que a *Blockchain* faça uso de outro sistema necessário para que haja o acesso dos dados, e, embora não seja possível a exclusão dos dados incluídos no registro distribuído da ferramenta o acesso à esses dados poderia ser tornado impossível pelo sistema que controla o mesmo.

A primeira proposta, de acordo com a dissertação do cientista da computação Filipy Soares que expressa claramente que os “Repositórios Digitais Confiáveis precisam demonstrar confiabilidade frente ao seu público e essa demonstração passa pela conformidade com itens normativos definidos por documentos de referência para tal”

Essa necessidade de conformidade é proposta no trabalho científico de forma a utilizar o mecanismo de armazenamento de dados confiáveis do livro de registro disperso do *Blockchain* de forma a armazenar apenas os dados não considerados pessoais, ou no caso de documentos, os dados que não podem ser alterados de acordo com nosso ordenamento jurídico nacional. (SOARES, 2021)

A segunda necessita de uma hermenêutica expansiva da legislação, interpretando que quando o legislador no inciso VI do artigo 18º da LGPD determina que os dados sejam

eliminados, ele na realidade almeja que o acesso e a utilização desses dados fiquem impossibilitados, não prevendo, portanto, a legislação a utilização de ferramentas de armazenamento de dados que por sua necessidade de segurança não seriam, portanto, deletáveis.

Caberá, nesse caso, aos juristas e à jurisprudência a determinação do quão literal essa deleção necessita ser, considerando que não é possível conciliar avanços no cerne da documentação digital, que não podem ser de fácil manipulação, quiçá não possam ser manipulados no geral, com o cumprimento *ipsis litteris* do inciso.

O século XXI trouxe inúmeras mudanças para o cotidiano do mundo, os avanços tecnológicos trouxeram graves consequências para direitos abstratos outrora inquestionáveis, como a privacidade. A realidade é que a internet só tem crescido sua influência, principalmente através de redes sociais e dos *smart phones.* Mudanças tecnológicas ocorrem em ritmo frenético no mundo do desenvolvimento de sistemas e embora nosso legislativo tenha dado os primeiros passos necessários para garantir nossos direitos, é necessário também conciliar as exigências com o desenvolvimento tecnológico, evitando restringir no Brasil a utilização de ferramentas amplamente adotar no exterior o que poderia trazer consequências inesperadas para nossa grande indústria de *software.*

Por fim, mister aqui destacar que ao mesmo tempo, não pode o direito aderir a argumentos, como os utilizados por fundadores do *Facebook*, que chegaram a utilizar a máxima da *"era da privacidade acabou"* e o desafio será constante para fazê-lo de forma que concilie a adoção e desenvolvimento de ferramentas novas que tornem conceitos inovadores como documentos digitais, cartórios que operam completamente de forma digital e outras inovações que constantemente veem à tona com o inquestionável dever de resguardar o direito constitucional previsto no artigo 5º da Constituição Federal em seu inciso X que declara inviolável a vida intima e privada dos cidadão da república. (JOHNSON, 2010)

REFERÊNCIAS

ABC. Cambridge Analytica bosses claimed they invented “Crooked Hillary” campaign, won Donald Trump the presidency. Disponível em: https://www.abc.net.au/news/2018-03-21/cambridge-analytica-claimed-it-secured-donald-trump-presidentia/9570690
Acesso em: 20/05/2021

ABREU, Jacqueline De Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. Revista Brasileira de Políticas Públicas, volume 7, número 3 2017.

BIONI, Bruno R. Proteção de dados pessoais a função e os limites do consentimento. Editora Forense 2019.

BLOOMBERG. Smart Contracts Market Size to Reach USD 345.4 Million by 2026 at CAGR 18.1%. 05/03/2021. Disponível em: https://www.bloomberg.com/press-releases/2021-03-05/smart-contracts-market-size-to-reach-usd-345-4-million-by-2026-at-cagr-18-1-valuates-reports
Acesso em: 05/06/2021

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm. Acesso em: 1 jan. 2017.

BRENNAN, Margaret. Kerry Warns Russia on Snowden: “Respect the Relationship”. CBS, 24/06/2013. Disponível em: https://www.cbsnews.com/news/kerry-warns-russia-on-snowden-respect-the-relationship/
Acesso em: 20/05/2021.

CADWALLADR, Carole, Graham-Harrison, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17/03/2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
Acesso em: 20/05/2021.

CASADO, Letícia. “Medir impacto de fake news nas eleições é difícil”, diz chefe da missão da OEA. Folha de São Paulo, 29/10/2018. Disponível em: https://www1.folha.uol.com.br/poder/2018/10/medir-impacto-de-fake-news-nas-eleicoes-e-dificil-diz-chefe-de-missao-da-oea.shtml
Acesso em: 25/05/2021

CAPPELLI, Paulo. Mudança na Lei de Segurança Nacional prevê criminalização de fake News e disparos em massa nas eleições. Extra, 08/04/2021. Disponível em: https://extra.globo.com/noticias/brasil/mudanca-na-lei-de-seguranca-nacional-preve-criminalizacao-de-fake-news-disparos-em-massa-nas-eleicoes-24961601.html. Acesso em: 12/05/2021.

CHAUM, David. Blind Signatures for Untraceable Payments. Advances in Crytpology, 1983. Disponível em:
https://link.springer.com/chapter/10.1007/978-1-4757-0602-418
Acesso em: 02/06/2021

CHOHAN, Usman W. A History of Bitcoin. University of New South Wales, 30/09/2017.

COTS, MÁRCIO, OLIVEIRA, RICARDO. Lei Geral de Proteção de Dados Pessoais Comentada. 2ª Edição. Thomson Reuters 2019.

DOLMETSCH, CHRIS. OneCoin Leaders Charged in Multibillion-Dollar Pyramid Scam. Bloomberg, 2019. Disponível em:
https://www.bloomberg.com/news/articles/2019-03-08/onecoin-leaders-charged-in-u-s-with-operating-pyramid-scheme?utm_source=google&utm_medium=cpc&utm_campaign=dsa&utm_term=&gclid=Cj0KCQjwnueFBhChARIsAPu3YkSBNVJXdPBecH0R99UF8KROfIijE4NS45i0hwiDUdxjjj64G_Q3PREaAtjkEALw_wcB
Acesso em: 04/06/2021

DONEDA, Danilo. Da privacidade à proteção de dados. São Paulo: Renovar. 2006.

EPOCA NEGOCIOS. Há oito anos duas pizzas foram vendidas com bitcoins. Hoje, valem R$ 300 milhões. Disponível em: https://epocanegocios.globo.com/Dinheiro/noticia/2018/05/ha-oito-anos-duas-pizzas-foram-vendidas-com-bitcoin-hoje-elas-valem-r-300-milhoes.html
Acesso em: 01/06/2021

FERNANDES, M. S., GOLDIM, J. R. A sistematização de dados e informações em saúde em um contexto de big data e blockchain, in Lucca, N.; Pereira de Lima, C. R.; Simão, A.; Maciel, R. M. (Org). Direito e Internet IV. São Paulo: Quartier Latin, 2019.

GREENWALD, Glenn; e BRIDI, Sônia. Documentos revelam esquema de agência dos EUA para espionar em Dilma. O Globo, 01/09/2013. Disponível em:
http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html
Acesso em: 20/05/2021.

GREENWALD, Glenn; e BRIDI, Sônia. NSA Documents Show United States Spied Brazilian Oil Giant. O Globo, 09/09/2013. Disponível em:
http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html
Acesso em: 20/05/2021.

JOHNSON, Bobby. Privacy no longer a social norm, says Facebook founder. The Guardian, 11/01/2010. Disponível em:
https://www.theguardian.com/technology/2010/jan/11/facebook-privacy
Acesso em: 24/06/2021

KEBIE, Nicole. The complicated truth about China's social credit system. Wired, 07/06/2019. Disponível em:

https://www.wired.co.uk/article/china-social-credit-system-explained . Acesso em: 12/05/2021.

LEMOS, Ronaldo. A Lei de Proteção de Dados e as eleições. Folha de São Paulo, 22/09/2020. Disponível em: https://itsrio.org/pt/artigos/a-lei-de-protecao-dados-e-as-eleicoes/ Acesso em: 30/05/2021

LIND, Dara. Everyone's heard of the Patriot Act. Here's what it actually does. Vox, 02/06/2015. Disponível em: https://www.vox.com/2015/6/2/8701499/patriot-act-explain. Acesso em: 12/05/2021.

MELIK, James. Digital Currency: Brave new world or criminal haven? BBC Business, 2012. Disponível em: https://www.bbc.com/news/business-19785935 Acesso em: 04/06/2021

MEUNIER, Sebastien. Blockchain 101: What is Blockchain and How Does this Revolutionary Technology Work? Transforming Climate Finance and Green Investment with Blockchains, p 23-24, 2018.

POPPER, Nathaniel. Digital Gold. Harper Collins publisher edição de 2015.

UNITED STATES DEPARTMENT OF COMMERCE. NSIT 2018. Disponível em: https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf . Acesso em: 01/06/2021

SAINT-PIERRE, Héctor L., 11 de Setembro: do Terror à injustificada arbitrariedade e terrorismo de Estado. Revista de Sociológia e Política, volume 23 número 53, Março de 2015. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-44782015000100009. Acesso em: 12/05/2021

PECK, Patricia Pinheiro. Proteção de Dados Pessoais: comentários à Lei N. 13.709/2018(LGPD). 3ª edição Saraiva 2021

PONZEN, David. Edward Snowden, National Security Whistleblowing and Civil Disobendience. Lawfare, 26/03/2019. Disponível em: https://www.lawfareblog.com/edward-snowden-national-security-whistleblowing-and-civil-disobedience Acesso em: 20/05/2021

SARMAH, Simanta. Understanding Blockchain Technology. Computer Sciences and Engineering, 2018 pp 23-29.

SODRÉ, Paulo Cesar Alves. As Fake News e a propaganda eleitoral: da liberdade de expressão à legitimidade do processo eleitoral. Direito Eleitoral: Temas Relevantes, 2018.

STEUART, JADA. Netflix's "The Great Hack" highlights Cambridge Analytica's role in Trinidad & Tobago elections. Global Voices, 06/08/2019.

Disponível em: https://advox.globalvoices.org/2019/08/06/netflixs-the-great-hack-highlights-cambridge-analyticas-role-in-trinidad-tobago-elections/
Acesso em: 20/05/2021

SZABO, NICK. The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials, n.c, p. 1-2, 1997.

TRE. Eleições de 2018 e o impacto das Fake News. 15/06/2018. Disponível em: https://www.tre-pa.jus.br/imprensa/noticias-tre-pa/2018/Junho/eleicoes-2018-e-o-impacto-das-fake-news-1
Acesso em: 25/05/2021

VIEIRA, Thiago; AZARIA, Asaph; EKBLAW, Ariel; LIPPMAN, Andrew. MedRec: Using Blockchain for Medical Data Access and Permission Management. IEEE, 22/09/2016. Disponível em:
https://ieeexplore.ieee.org/abstract/document/7573685
Acesso em: 08/06/2021

WHITFIELD, Diffie e HELLMAN, Martin E. New Directions in Cryptography. IEEE Transactions on Information Theory, 06/11/1976. Disponível em:
https://ee.stanford.edu/~hellman/publications/24.pdf.
Acesso em: 01/06/2021